Informe sobre Amenazas para la Seguridad en Internet

ISTR

Abril 2017

Volumen

22

Índice

Introducción

Sumario ejecutivo

Grandes números

Ataques dirigidos: Espionaje, subversión y sabotaje

Correo Electrónico: Malware, spam y phishing

Ataques web, toolkits y explotación de vulnerabilidades online

Cibercrimen y la economía clandestina

Ransomware: Extorsionando a consumidores y empresas

Nuevas fronteras: IoT, dispositivos móviles y amenazas en la nube

Informe sobre Amenazas para la Seguridad en Internet

Índice

4 **Introducción**

6 **Sumario ejecutivo**

10 **Grandes números**

14 **Ataques dirigidos: Espionaje, subversión y sabotaje**

15 Introducción
15 Principales conclusiones
17 El panorama de los ataques dirigidos en 2016
18 Tendencias y análisis
18 Subversión surge como un nuevo motivo para ataques dirigidos
19 Retornan los ataques de sabotaje
19 Uso de herramientas del día a día
20 *Como los atacantes de Shamoon emplearon tácticas con "herramientas del día a día"*
21 Espionaje económico
22 Surgen nuevas amenazas
22 Lectura adicional
23 Mejores prácticas

24 **Correo Electrónico: Malware, spam y phishing**

25 Introducción
25 Principales conclusiones
25 Tendencias y análisis
25 Amenaza de Malware
26 Phishing
27 Fraudes BEC
28 Spam permanece estable
29 Investigaciones/Estudios de casos
29 Cambio de táctica
29 *Ice-cold: Técnicas snowshoe y hailstorm*
30 Ingeniería social experimentada y comprobada
31 Ingeniería social y nuevas plataformas de mensajería
31 Lectura adicional
32 Mejores prácticas

33 **Ataques web, toolkits y explotación de vulnerabilidades online**

34 Introducción
34 Principales conclusiones
34 Tendencias y análisis
34 Evaluación de vulnerabilidades
35 Kits de Exploit
36 Ataques web
36 Vulnerabilidades del navegador
37 Estudio de caso
37 *Angler: La ascensión y caída de un kit de exploit*
37 Lectura adicional
37 Mejores prácticas

38 **Cibercrimen y la economía clandestina**

39 Introducción
39 Principales conclusiones
39 Malware
40 Uso de herramientas del día a día: PowerShell, macros y ingeniería social
43 Estudio de caso de Botnet: Necurs
43 Todo está relacionado al dinero: Malware financiero
44 Incluso Mac
45 Odinaff y Banswift: El año del asalto financiero dirigido
45 Banswift
46 Odinaff
46 Violaciones de datos y la economía clandestina
46 Violaciones de datos
47 *Retrospectiva del año*
48 Causas de violaciones de datos
49 Sectores expuestos
51 Datos por país
52 Economía Clandestina
54 Interferencias y interrupciones
54 Avalanche
54 Bayrob
54 Lurk/Angler
55 Dyre
55 Lectura adicional
55 Mejores prácticas

56 **Ransomware: Extorsionando a consumidores y empresas**

57 Introducción
57 Principales conclusiones
57 Tendencias y análisis
59 Investigaciones/Estudios de casos
59 Cómo ransomware puede afectar a los consumidores
59 Cómo ransomware puede afectar a las empresas
60 Aumentan los pedidos de rescate
60 Vectores de infección
62 Llega el ransomware como servicio
62 Nuevas técnicas: ataques dirigidos y "uso de herramientas del día a día"
63 Otras plataformas ahora vulnerables
63 Operaciones de autoridades legales
63 Lectura adicional
63 Mejores prácticas

64 **Nuevas fronteras: El Internet de las Cosas, dispositivos móviles y amenazas en la nube**

65 El Internet de las Cosas
65 Principales conclusiones
65 Tendencias y análisis
67 Datos por país
67 Contrseñas
67 La botnet Mirai
68 Una historia en evolución
68 Visión futura
69 Mejores prácticas
69 Dispositivos Móviles
69 Principales conclusiones
69 Tendencias de malware de dispositivos móviles
70 Motivos y técnicas
71 Tasas de malware y grayware
71 Aumento de empaquetadores en tiempo real
72 Vulnerabilidades en dispositivos móviles
72 Mejoras en la arquitectura Android
73 Un sabor amargo para Apple
73 Mejores prácticas
74 Nube
74 Principales conclusiones
74 Tendencias y análisis
75 Negocios de riesgo
75 El pelirgro del ransomware
75 IoT y nube: potenciales aliados en el cibercrimen
76 Uso de herramientas del día a día
76 Lectura adicional
76 Mejores prácticas
77 Créditos
78 Acerca de Symantec
78 Más información

Symantec

Informe sobre Amenazas para la Seguridad en Internet

Índice

GRÁFICOS & TABLAS

10 Grandes números

14 Ataques direcionados: Espionaje, subversión e sabotaje

15 Línea del tiempo de incidentes de ataque dirigidos notables en 2016

16 Grupos de ataques dirigidos notables

17 Total anual de vulnerabilidades de día cero

17 Elección presidencial de EE.UU.: Línea del tiempo de los ataques en 2016

18 Vulnerabilidades divulgadas en sistemas de control industrial

20 Las herramientas más frecuentes que los atacantes pueden usar de forma indebida

21 Correo electrónico de spear phishing usado en los ataques al DNC

24 Correo Electrónico: Malware, spam y phishing

25 Tasa General de Malware de Correo Electrónico

26 Tasa Mensual de Malware de Correo Electrónico

26 Tasa de Malware de Correo Electrónico por Sector

26 Tasa de Malware de Correo Electrónico por Tamaño de Empresa

26 Tasa General de Phishing

27 Tasa Mensual de Phishing

27 Tasa de Phishing por Sector

27 Tasa de Phishing por Tamaño de Empresa

28 Fraudes BEC: Líneas frecuentes de asunto

28 Tasa General de Spam

28 Tasa Mensual de Spam

29 Tasa de Spam por Tamaño de Empresa

29 Tasa de Spam por Sector

29 Detecciones de archivos ejecutables por mes

30 Correos electrónicos bloqueados con adjuntos WSF

30 Proceso típico de infección por malware enviado por correo electrónico

31 Palabras clave usadas en campañas de spam de malware

31 Idiomas preferidos usados en campañas de spam

33 Ataques web, toolkits y explotación de vulnerabilidades online

34 Sitios web escaneados con vulnerabilidades

34 Porcentaje de vulnerabilidades que eran críticas

35 Los 10 principales kits de exploit

36 Ataques web bloqueados por mes

36 Clasificación de los sitios web explotados con más frecuencia

37 Vulnerabilidades del navegador

38 Cibercrimen y la economía clandestina

39 Variantes únicas de malware detectadas por primera vez

39 Cálculo mensual de variantes únicas de malware vistas por primera vez en 2016

40 Variantes únicas de malware detectadas

40 Cálculo mensual de variantes únicas de malware en 2016

41 Incidencia y tendencias de malware

41 Panorama de ataque típico en 2016 tuvo las siguientes etapas

42 Detecciones de archivos ejecutables de JavaScript por mes

42 Detecciones de archivos ejecutables de macros de Office por mes

42 Cifra de actividad de Bots

43 Archivos ejecutables entregados por la botnet de spam Necurs

43 Los 10 principales troyanos financieros

44 Actividades de troyanos financieros por mes

44 Distribución de malware para Mac por mes, 2014-2016

45 Las 10 principales instancias de malware bloqueadas en los endpoints del OS X en porcentaje de las infecciones totales

46 Violaciones de datos, 2014-2016

47 Violaciones de datos por mes, 2014-2016

47 Identidades robadas por mes, 2014-2016

47 Tipos de datos perdidos en violaciones en 2016

48 Las 10 principales causas de violaciones de datos en 2016

48 Las 10 principales causas de violaciones de datos por identidades robadas en 2016

49 Los 10 principales sectores que sufrieron violaciones por cifra de incidentes

49 Los 10 principales subsectores que sufrieron violaciones por cifra de incidentes

50 Los 10 principales sectores que sufrieron violaciones por cifra de identidades robadas

50 Los 10 principales subsectores que sufrieron violaciones por cifra de identidades robadas

51 Los 10 principales países por cifra de violaciones de datos

51 Los 10 principales países por cifra de identidades robadas

52 Lista de precios de mercados clandestinos

53 El mercado clandestino

56 Ransomware: Extorsionando a consumidores y empresas

57 Promedio de detecciones globales de ransomware por día

58 Detecciones globales de ransomware por mes

58 Detecciones de ransomware por país

58 Nuevas familias de ransomware

58 Nuevas variantes de ransomware

59 Variantes de ransomware por mes

59 Infecciones de consumidores x corporativas

59 Infecciones de consumidores x corporativas por mes

60 Promedio de Pedido de rescate

61 Principales amenazas de ransomware

64 Nuevas fronteras: El Internet de las Cosas, dispositivos móviles y amenazas en la nube

66 Ataques a cada hora al honeypot de IoT por mes

66 Los 10 principales países donde se iniciaron los ataques al honeypot IoT de Symantec

67 Las 10 contraseñas más utilizadas para intentar ingresar en el honeypot IoT de Symantec

68 El rastro de interrupciones de Mirai en 2016

70 Cifra total de detecciones por año de malware

70 Número acumulativo de familias de malware por año

70 Variantes de dispositivos móviles por familia

70 Variantes de malware para dispositivos móviles por año

71 Principales amenazas para dispositivos móviles en 2016

71 Tasas de malware y grayware, 2014-2016

72 Vulnerabilidades relatadas en dispositivos móviles por sistema operativo

72 Porcentaje de malware para dispositivos móviles en el campo que es empaquetado

73 Participación de mercado de diferentes versiones de Android, enero de 2017

74 Aplicaciones en la nube más utilizadas en las compañías

Symantec

Introducción

Sección

00

Symantec

Symantec creó la red global de recopilación de amenazas civiles más grande del mundo y una de las más completas colecciones de inteligencia sobre amenazas a la ciberseguridad a través de Symantec Global Intelligence Network™. La Red de Inteligencia Global de Symantec rastrea más de 700.000 adversarios globales y registra eventos de 98 millones de sensores de ataque en todo el mundo.

Esta red monitorea actividades de amenazas en más de 157 países y territorios a través de una combinación de productos, tecnologías y servicios de Symantec, incluyendo Symantec Endpoint Protection™, Symantec DeepSight™ Intelligence, Symantec Managed Security Services™, los productos Norton™ para consumidores y otras fuentes de datos de terceros, con la generación de más de nueve trillones de líneas de datos de seguridad.

Asimismo, Symantec mantiene una de las bases de datos de vulnerabilidades más amplia del mundo, actualmente compuesta por más de 88.900 vulnerabilidades registradas (que abarcan más de dos décadas) de 24.560 proveedores que representan más de 78.900 productos.

El análisis de tendencias de malware de spam, phishing y correo electrónico es recopilado de una gama de tecnologías de seguridad de Symantec que procesan más de 2.000 millones de correos electrónicos todos los días, incluyendo: Skeptic™, Symantec Messaging Gateway para Proveedores de Servicios, Symantec CloudSOC y Symantec Probe Network.

Skeptic™ es la tecnología heurística propietaria de Symantec, incluida en el producto Symantec Email and Web Security. cloud™, que filtra más de 336 millones de correos electrónicos y más de 2.400 millones de solicitudes en la web todos los días. Symantec también reúne información sobre phishing a través de una amplia comunidad antifraude, compuesta por empresas, proveedores de seguridad y aliados.

Symantec Cloud Threat Labs proporciona el análisis detallado de amenazas y riesgos con base en la nube, desarrollado usando datos de la tecnología de seguridad de Symantec CloudSOC, que en 2016 protegió más de 20.000 aplicaciones en la nube, 176 millones de documentos en la nube y 1.300 millones de correos electrónicos. Symantec CloudSOC es la solución de CASB (Cloud Access Security Broker) de la empresa y fue desarrollada para brindar visibilidad, control y protección a aplicaciones y datos basados en la nube.

Symantec Web Application Firewall & Reverse Proxy realiza el escaneo diario de 1.000 millones de solicitudes Web que no habían sido vistas anteriormente.

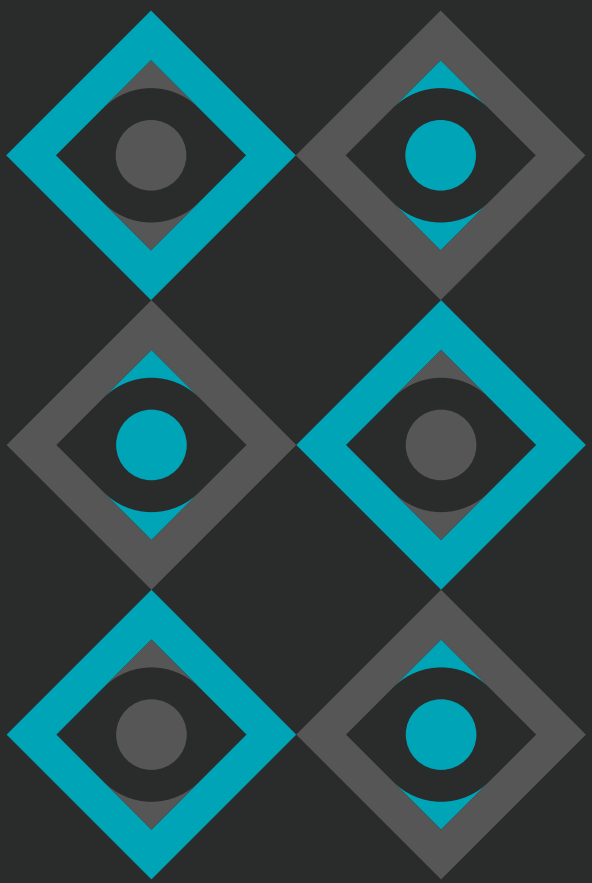
Symantec Website Security protege desde 2004, 1,4 millones de servidores web en todo el mundo con 100% de disponibilidad. La infraestructura de validación procesa más de 15.7000 millones de consultas OCSP (Protocolo Online de Status de Certificados) por día, usadas para obtener el status de revocación de certificados digitales X.509 en todo el mundo.

Esos recursos brindan a los analistas de Symantec fuentes inigualables de datos para identificar, analizar y proporcionar comentarios actualizados sobre las amenazas emergentes de ataques, actividades de códigos maliciosos, phishing y spam. El resultado es el Informe Anual sobre Amenazas para la Seguridad en Internet Symantec™, que ofrece a las organizaciones, pequeñas empresas y consumidores, información fundamental para proteger sus sistemas de forma eficaz tanto ahora como en el futuro.

Sumario ejecutivo

Sección

01



Symantec

Los grupos de ataque revelaron nuevos niveles de ambición en 2016, un año marcado por ataques increíbles, incluyendo asaltos virtuales de varios millones de dólares a bancos, intentos explícitos de interrumpir el proceso electoral de EE.UU a través de grupos patrocinados por naciones y algunos de los mayores ataques distribuidos de denegación de servicio (DDoS) ya registrados, conducidos por una botnet de dispositivos del Internet de las Cosas (IoT).

Si bien los ciberataques lograron causar niveles sin precedentes de interrupción de servicios, los atacantes frecuentemente usaron herramientas y tácticas muy simples para ocasionar un gran impacto. Vulnerabilidades de día cero y malware sofisticado ahora tienden a ser usados con moderación y los delincuentes cada vez más buscan esconderse en áreas abiertas. Usan abordajes simples, como correo electrónico de spear phishing y "herramientas del día a día", empleando cualquier herramienta que consigan acceder, como software legítimo de administración de red y recursos del sistema operativo.

Mirai, la botnet responsable de una ola de ataques DDoS, fue compuesta principalmente por ruteadores y cámaras de seguridad infectadas, dispositivos de baja potencia y mal protegidos. En manos equivocadas, incluso los dispositivos y software relativamente benignos pueden emplearse para causar un efecto devastador.

Ataques dirigidos: Subversión y sabotaje toman cuenta de las principales noticias

El mundo del ciberespionaje pasó por un cambio importante hacia actividades más explícitas, destinadas a desestabilizar y desorganizar las organizaciones y los países blanco de ataque. Los ciberataques contra el Partido Demócrata de E.EUU. y la subsiguiente filtración de información robada fueron uno de los principales puntos de discusión de las elecciones presidenciales en EE.UU. Con la Comunidad de Inteligencia de EE.UU. atribuyendo los ataques a Rusia y concluyendo que la campaña habría sido juzgada un éxito, es posible que esas tácticas se utilicen nuevamente en esfuerzos para influir la política y sembrar el caos en otros países.

Los ciberataques que involucran sabotaje han sido tradicionalmente raros, sin embargo 2016 vio dos olas separadas de ataques que contenían malware destructivo. En enero y nuevamente en diciembre se usó en Ucrania el malware contra objetivos determinados, un malware que borra el contenido de discos, tales ataques ocasionaron también cortes de energía. Mientras tanto, el troyano Shamoon, que también borra el contenido de discos, resurgió tras cuatro años de ausencia y fue usado contra varias organizaciones en Arabia Saudita.

El aumento de los ataques disruptivos coincidió con el descenso de algunas actividades secretas, específicamente el espionaje económico, robo de propiedad intelectual y secretos comerciales. Tras un acuerdo en 2015 entre EE.UU. y China, en el que los dos países prometierom no realizar espionaje económico en el ciberespacio, las detecciones de malware vinculadas a grupos chinos sospechosos de espionaje disminuyeron considerablemente. Sin embargo, eso no significa que el espionaje económico haya desaparecido completamente y llega en un momento en el que otras formas de ataques dirigidos, como subversión o ataques financieros de alto nivel han aumentado.

Asaltos financieros: Los delincuentes centran la atención en objetivos más grandes

Hasta hace poco tiempo, los cibercriminales centraban sus esfuerzos principalmente en clientes bancarios, invadiendo cuentas o robando tarjetas de crédito. No obstante, un nuevo tipo de delincuentes tiene mayores ambiciones y puso como objetivo los propios bancos, algunas veces intentando robar millones de dólares en un único ataque. Grupos como Carbanak han liderado el camino, demostrando el potencial de este abordaje al realizar una serie de ataques contra bancos en EE.UU.

En 2016, otros dos grupos apostaron más alto lanzando ataques mucho más ambiciosos. El grupo Banswift logró robar US$ 81 millones del Banco Central de Bangladesh, explotando las debilidades en la seguridad del banco para infiltrarse en su red y robar sus credenciales SWIFT, permitiéndole efectuar transacciones fraudulentas.

Otro grupo, conocido como Odinaff, también fue descubierto al ejecutar ataques sofisticados contra bancos y otras instituciones financieras. El grupo también parecía usar malware para ocultar los registros de mensajes SWIFT de clientes, relacionados a transacciones fraudulentas realizadas por el grupo.

Mientras que Banswift y Odinaff demostraron poseer competencia técnica y emplearon tácticas asociadas con grupos avanzados, grupos mucho menos sofisticados también robaron grandes sumas de dinero. Los fraudes BEC (Business Email Compromise), que usan básicamente correos electrónicos spear-phishing cuidadosamente compuestos, continúan causando grandes pérdidas; más de US$ 3.000 millones robados en los últimos tres años.

Uso de herramientas del día a día

Atacantes que van desde cibercriminales a grupos patrocinados por naciones han comenzado a cambiar sus tácticas, al aplicar un mayor uso de recursos del sistema operativo, herramientas listas para uso y servicios en la nube para invadir a sus víctimas. El caso más marcante que utiliza herramientas del día a día se produjo durante las elecciones de EE.UU. Un simple correo electrónico de spear phishing proporcionó el acceso a la cuenta de Gmail del presidente de la campaña de Hillary Clinton, John Podesta, sin usar cualquier malware o vulnerabilidades.

La táctica de “uso de herramientas del día a día” utiliza los recursos disponibles en vez de malware y exploits, y ofrece muchas ventajas a los atacantes. Identificar y explotar vulnerabilidades de día cero se ha vuelto más difícil, debido a las mejoras en desarrollo seguro y a los programas de recompensas. Los toolkits de ataques Web han perdido popularidad, posiblemente gracias al esfuerzo necesario para mantener los exploits actualizados y una infraestructura de backend.

Las poderosas herramientas de script, como PowerShell y macros, son recursos estándar del Windows y del Microsoft Office que pueden facilitar el acceso remoto y descargas de malware sin usar vulnerabilidades o herramientas maliciosas. Aunque existen desde hace casi 20 años, los macros de Office resurgieron en el panorama de amenazas, ya que los atacantes emplean técnicas de ingeniería social y logran fácilmente violar las medidas de seguridad que fueron implementadas para resolver el antiguo problema de los virus de macros.

Cuando se ejecutan correctamente los abordajes que utilizan herramientas del día a día pueden ocasionar infecciones casi asintomáticas, lo que permite que los atacantes se escondan fácilmente.

El correo electrónico resurge como canal de ataque preferido

En 2016, los correos electrónicos maliciosos fueron el arma principal de varios ciberataques usados por todos, desde grupos de ciberespionaje patrocinados por naciones hasta pandillas de ransomware que envían masivos correos electrónicos. De cada 131 correos electrónicos enviados uno era malicioso, la tasa más alta en cinco años.

La popularidad renovada del correo electrónico se debe a varios factores. Es un comprobado canal de ataque. No se basa en vulnerabilidades, sino que usa un artificio sencillo para atraer a las víctimas a abrir archivos adjuntos, seguir enlaces o revelar sus credenciales. Los correos electrónicos de spear phishing, tales como correos electrónicos falsificados que instruyen a la víctima a redefinir su contraseña del Gmail, se usaron en los ataques electorales de EE.UU.

Los correos electrónicos camuflados como correspondencia de rutina, de facturas o notificaciones de entrega, fueron el medio preferido para propagar el ransomware. La disponibilidad de botnets de spam de fácil contratación, como Necurs, permitió que los grupos de ransomware elaborasen campañas de correo electrónico masivo en 2016, distribuyendo a diario cientos de miles de correos electrónicos maliciosos.

Ransomware presiona a las víctimas con crecientes exigencias

El ransomware continúa preocupando a las empresas y a los consumidores, con campañas indiscriminadas que distribuyen grandes volúmenes de correos electrónicos maliciosos. En algunos casos, las empresas pueden quedar sobrecargadas por el gran volumen de correos electrónicos que reciben con ransomware. Los delincuentes exigen cada vez más de las víctimas con el aumento del pedido promedio de rescate en 2016 para US$ 1.077, en comparación con US$ 294 del año anterior.

Los atacantes perfeccionaron un modelo de negocios que generalmente utiliza malware escondido en correos electrónicos inofensivos, cifrado irrompible y pago de rescate anónimo empleando criptomonedas. El éxito de este modelo de negocio ha visto un creciente número de delincuentes que aprovechan esta oportunidad. El número de nuevas familias descubiertas de ransomware en 2016 más que triplicó para 101 y Symantec registró un aumento del 36% en infecciones por ransomware.

Nuevas fronteras: IoT y servicios en la nube en destaque

Si bien los grupos de fraudes financieros y de ransomware continúan representando la principal amenaza para los usuarios finales, comienzan a surgir otras amenazas. Era apenas una cuestión de tiempo hasta que los ataques a los dispositivos del internet de las cosas comenzaran a ganar popularidad, y 2016 tuvo el primer gran incidente con el surgimiento de Mirai, una botnet compuesta por dispositivos del internet de las cosas, como ruteadores y cámaras de seguridad. La débil seguridad tornó a esos dispositivos víctimas fáciles para los delincuentes, que construyeron una botnet grande lo suficiente para realizar el mayor ataque DDoS ya visto. Symantec verificó un gran incremento, con el doble de intentos de ataques contra dispositivos del internet de las cosas en el transcurso de 2016 y, en momentos de pico de actividad, los dispositivos del internet de las cosas fueron atacados una vez a cada dos minutos.

Varios blancos de ataque de Mirai eran los servicios relacionados a la nube, como el proveedor DNS Dyn. Esto, juntamente con la invasión de millones de bases de datos de MongoDB alojadas en la nube, muestra como los ataques en la nube se han vuelto realidad y tienden a aumentar

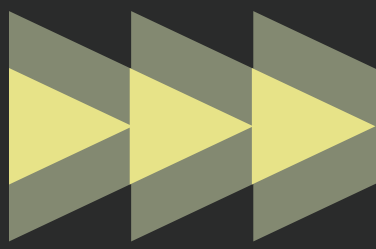
en 2017. La creciente dependencia de los servicios en la nube debe ser un tema preocupante para las empresas, pues representan un punto ciego de seguridad. Symantec descubrió que una organización común usaba 928 aplicaciones en la nube, un aumento en relación a las 841 en el inicio del año. Sin embargo, la mayoría de los CIOs cree que sus organizaciones usan apenas alrededor de 30 o 40 aplicaciones en la nube, lo que demuestra que puede subestimarse el nivel de riesgo, dejándolos vulnerables al ataque de amenazas emergentes.

Grandes números

352

Sección

02



Symantec

Violaciones

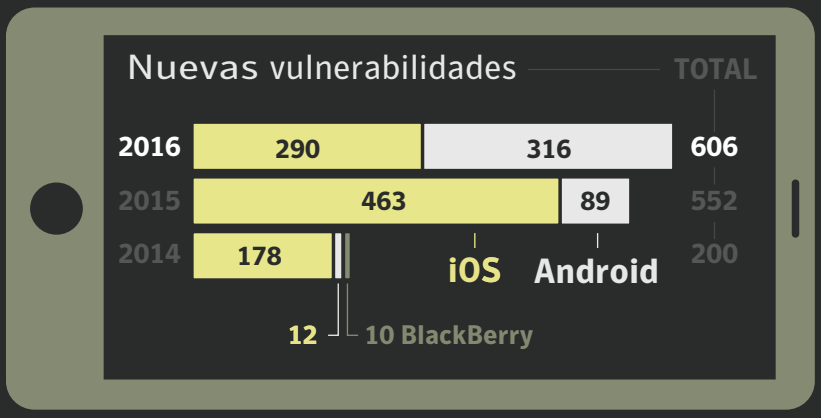
	2014	2015	2016
Total de violaciones	1.523	1.211	1.209
Violaciones con más de 10 millones de identidades expuestas	11	13	15
Total de identidades expuestas	1,2B	564M	1,1B
Promedio de identidades expuestas por violación	805K	466K	927K

En los últimos **8** años, más de **7,1 bilhões** milones de identidades fueron expuestas en violaciones de datos

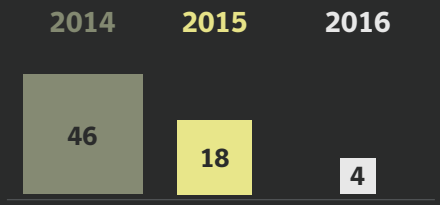
Amenazas de correo electrónico, malware y bots

	2014	2015	2016
Tasa de spam %	60%	53%	53%
Tasa de phishing	1 de cada 965	1 de cada 1.846	1 de cada 2.596
Tasa de Malware de correo electrónico	1 de cada 244	1 de cada 220	1 de cada 131
Nuevas variantes de malware	275M	355M	357M
Número de bots		91,9M	98,6M

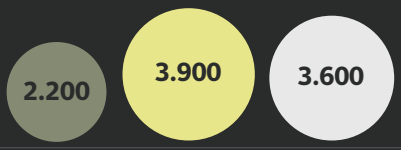
Dispositivos Móviles



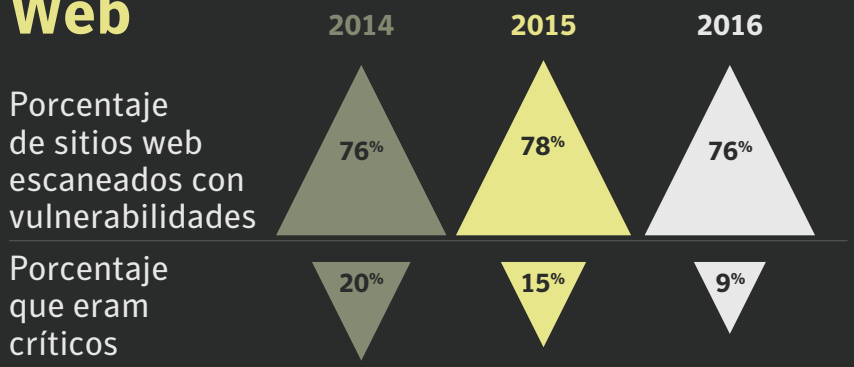
Nuevas Familias de Malware para Dispositivos Móviles Android



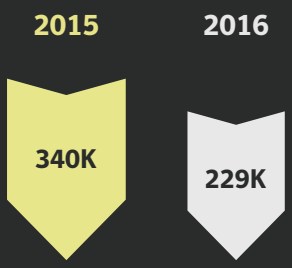
Nuevas Variantes de Malware para Dispositivos Móviles Android



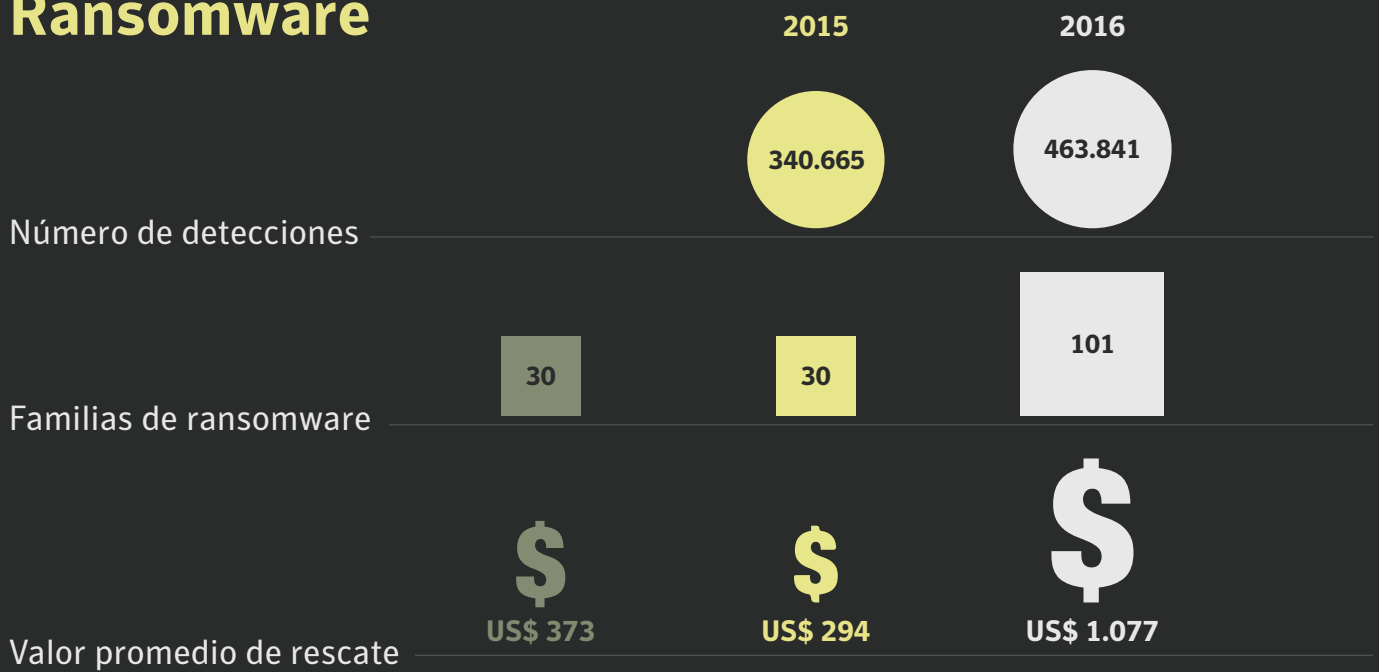
Web



Promedio de ataques web bloqueados por día



Ransomware



Nube

	JUL-DIC 2015	ENE-JUN 2016	JUL-DIC 2016
Número promedio de aplicaciones en la nube usadas por organización	774	841	928
Porcentaje de datos ampliamente compartidos	25%	23%	25%

El Internet de las Cosas

2 minutos: tiempo necesario para atacar a un dispositivo IoT

Velocidad de ataque

Número de ataques contra el honeypot de Symantec **por hora**

ENE | **2016** DIC | **2016**

Ataques dirigidos: Espionaje, subversión y sabotaje

Sección

03

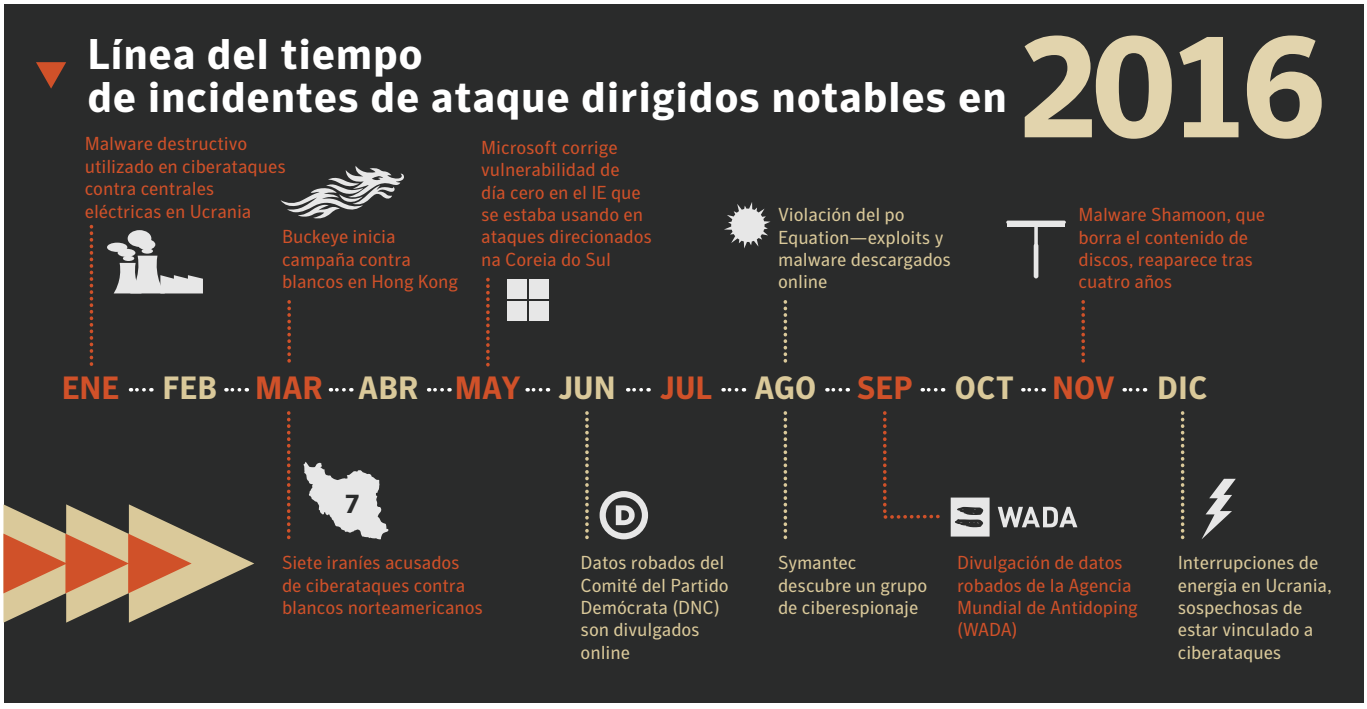
Symantec

Introducción

El panorama de ataques dirigidos cambió considerablemente en 2016, con varios grupos emergiendo de las sombras, participando en más actividades públicas y políticamente subversivas. El conflicto continuo en Ucrania, las elecciones en EE.UU y las Olimpiadas se vieron afectados por campañas destinadas al robo y filtración de datos para influir la opinión pública, creando un ambiente de desconfianza y posiblemente influenciando los resultados políticos. Debido a estos recientes sucesos y con elecciones importantes en 2017 en varios países es probable que este tipo de actividades continúe. Durante este período, los delincuentes perfeccionarán constantemente sus tácticas, con varios grupos distanciándose del malware personalizado y centrando cada vez más su atención en legítimas herramientas de software para afectar a sus objetivos, las redes.

Principales conclusiones

- Ataques con fines subversivos, en particular los que se produjeron durante las elecciones en EE.UU., salieron a la luz y representaron una nueva forma de ataque de gran importancia.
- Los ataques dirigidos que involucran malware destructivo aumentaron en algunas regiones, como el resurgimiento del malware Shamoon en Medio Oriente y los ataques contra objetivos en Ucrania que implicaban al troyano KillDisk.
- En algunos casos, ha disminuido el espionaje económico, como el robo de secretos de negocios o comerciales, una de las formas tradicionales de ataques dirigidos. Las detecciones de malware de espionaje chino han caído considerablemente, tras un acuerdo mútuo con EE.UU. para no poner la propiedad intelectual en la mira. Sin embargo, el espionaje económico no ha desaparecido definitivamente y la caída de volumen ocurre en un momento en el que han crecido otros tipos de ataques dirigidos, como sabotaje y subversión.
- Las vulnerabilidades de día cero se han vuelto menos importantes y algunos adversarios no dependen más de malware, con el uso cada vez mayor de "herramientas del día a día" – al emplear recursos disponibles, que incluyen legítimas herramientas administrativas y de prueba de penetración para llevar a cabo los ataques.



Ataques dirigidos notables

Sandworm

est. 2014

Posible región de origen: **Rusia**

Pseudónimos / *Quedagh, BE2 APT*

Herramientas, tácticas y procedimientos (TTP)
Spear phishing, vulnerabilidades, ataques de día cero, programas backdoor personalizados, cargas útiles destrutcivas

Motivos
Espionaje, sabotaje

Actividades recientes
Vinculadas a ataques destructivos contra medios de comunicación y objetivos en el sector de energía en Ucrania

Categorías y regiones objetivo
Gobiernos, organismos internacionales, sector de energía, Europa, EEUU

Housefly

est. 2001

Posible región de origen: **EEUU**

Pseudónimos / *Equation*

Herramientas, tácticas y procedimientos (TTP)
Watering holes, CD-ROMs infectados, claves USB infectadas, vulnerabilidades, ataques de día cero, programas de robo de información y backdoor personalizados, programas gusano

Motivos
Espionaje

Actividades recientes
Sufrió violación en 2016, con herramientas y exploits que vazaram

Categorías y regiones objetivo
Blancos de interés para atacantes patrocinados por naciones

Fritillary

est. 2010

Posible región de origen: **Rusia**

Pseudónimos / *Cozy Bear, Office Monkeys, EuroAPT, Cozyduke, APT29*

Herramientas, tácticas y procedimientos (TTP)
Spear phishing, programas backdoor personalizados

Motives
Espionaje, subversión

Actividades recientes
Vinculado a los ataques al Comité Nacional del Partido Demócrata (DNC)

Categorías y regiones objetivo
Gobiernos, grupos de investigación, medios de comunicación, Europa, EEUU

Strider

est. 2011

Posible región de origen: **Occidental**

Pseudónimos / *Remsec*

Herramientas, tácticas y procedimientos (TTP)
Herramienta de vigilancia avanzada

Motivos
Espionaje

Actividades recientes
Descubierto por Symantec en 2016

Categorías y regiones objetivo
Embajadas, compañías aéreas, Rusia, China, Suecia, Bélgica

Swallowtail

est. 2007

Possible region of origin: **Rusia**

Pseudónimos / *Fancy Bear, APT28, Tsar Team, Sednit*

Ferramentas, táticas e procedimentos (TTP)
Spear phishing, watering holes, dispositivos de almacenamiento infectados, vulnerabilidades, ataques de día cero, programas de robo de información y backdoor personalizados

Motivos
Espionaje, subversión

Actividades recientes
Vinculado a los ataques a WADA y DNC

Categorías y regiones objetivo
Governos, Europa, EEUU

Suckfly

est. 2014

Possible region of origin: **China**

Pseudónimos / *Ninguno*

Herramientas, tácticas y procedimientos (TTP)
Programas backdoor personalizados que usan firma con certificados robados

Motivos
Espionaje

Actividades recientes
Ataques dirigidos con múltiples certificados de firma robados

Categorías y regiones objetivo
E-commerce, gobiernos, sectores de tecnología, salud, financiero, transporte

Cadelle

est. 2012

Posible región de origen: **Irán**

Pseudónimos / *Ninguno*

Herramientas, tácticas y procedimientos (TTP)
Programas backdoor personalizados

Motivos
Espionaje

Actividades recientes
Vigilancia en blancos de ataque nacionales en Irán y organizaciones en Medio Oriente

Categorías y regiones objetivo
Compañías aéreas, empresas de telecomunicaciones, ciudadanos iraníes, gobiernos, ONGs

Buckeye

est. 2009

Posible región de origen: **China**

Pseudónimos / *APT3, UPS, Gothic Panda, TG-0110*

Herramientas, tácticas y procedimientos (TTP)
Spear phishing, ataques de día cero, programas backdoor personalizados

Motivos
Espionaje

Actividades recientes
Cambió la atenciónde blancos de ataque occidentales hacia Hong Kong

Categorías y regiones objetivo
Sectores de defensa, militar, medios de comunicación y educación, EE UU, Reino Unido, Hong Kong

Appleworm

est. 2012

Posible región de origen: **Corea del Norte**

Pseudónimos / *Lazarus*

Herramientas, tácticas y procedimientos (TTP)
Spear phishing, ataques DDoS, borrar contenido de discos, ataques de día cero, programas de robo de información y backdoor personalizados, cargas útiles destructivas

Motivos
Espionaje, sabotaje, subversión

Actividades recientes
Responsable de operaciones de interrupción de servicios en el inicio de 2016. Relacionado con el grupo de ataque del Banco de Bangladesh

Categorías y regiones objetivo
Sector financiero, militar, gobiernos, entretenimiento, electrónicos

Tick

est. 2006

Posible región de origen: **China**

Pseudónimos / *Ninguno*

Herramientas, tácticas y procedimientos (TTP)
Spear phishing, watering holes, programas backdoor personalizados

Motivos
Espionaje

Actividades recientes
Campañas de larga duración contra blancos de ataque en Japón

Categorías y regiones objetivo
Tecnología, transmisión, ingeniería acuática, Japón

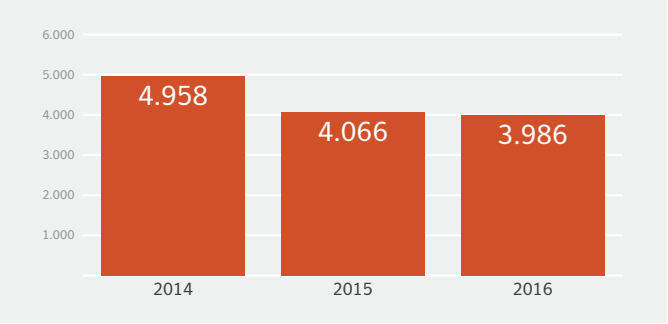
El panorama de los ataques dirigidos en 2016

2016 fue un año excepcionalmente activo para los ataques dirigidos, con increíbles incidentes ocurriendo en Europa, EE.UU., Asia y Medio Oriente. A medida que el año avanzaba, aumentaba el nivel de actividades de gran importancia, con incidentes políticamente subversivos dirigidos a Estados Unidos y malware destructivo centrado en Arabia Saudita y Ucrania.

Hoy en día, una amplia gama de grupos de ataque dirigidos está en operación. Si bien las potencias globales tienen una capacidad de larga data para llevar a cabo una variedad de ciberoperaciones, las potencias regionales también migraron al ciberespacio con sus propias operaciones de ciberespionaje dirigidas a los países rivales y a los grupos internos de oposición. El gráfico de grupos de ataques dirigidos importantes lista los 10 grupos más significativos y activos en 2016 y que están públicamente vinculados a naciones.

Total anual de vulnerabilidades de día cero

Las vulnerabilidades de día cero (vulnerabilidades no descubiertas por el proveedor del software) disminuyeron marginalmente de 4.066 en 2015 para 3.986 en 2016.



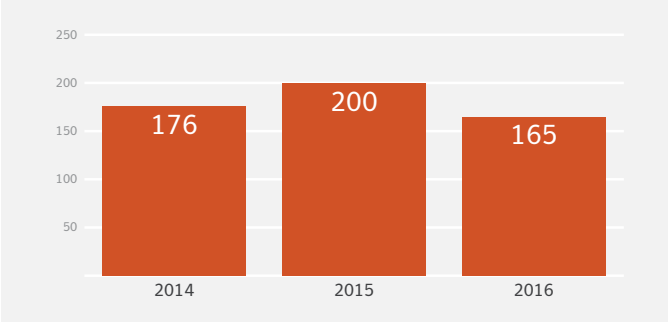
Ediciones anteriores del Informe sobre Amenazas para la Seguridad en Internet se centraron en el número de explotaciones de vulnerabilidades de día cero. Este año, optamos por analizar la cifra total de vulnerabilidades de día cero, es decir, las vulnerabilidades no descubiertas por el proveedor del software. Bajo esta métrica, las vulnerabilidades de día cero encontradas en 2016 cayeron más una vez, disminuyendo marginalmente de 4.066 para 3.986. Esta estancamiento sugiere que la creciente popularidad de los programas "bug bounty" y una mayor atención en la seguridad como parte del proceso de desarrollo de productos pueden reflejar que las vulnerabilidades de día cero se están volviendo más difíciles de encontrar para los delincuentes, forzándolos a alejarse de su uso y ampliar su gama de tácticas (vea "uso de uso de herramientas del día a día" abajo).

El declive en el descubrimiento de ataques de día cero se produce después que el mercado clandestino de vulnerabilidades tuvo destaque en 2015, seguido de la violación de Hacking Team. Hubo filtración de múltiples explotaciones de día cero como parte de la violación, además de información sobre cuanto dinero esos exploits estaban generando.

Sin embargo, se produjeron varios casos de vulnerabilidades de día cero explotadas en ataques dirigidos en 2016. Por ejemplo, tras descubrir que una vulnerabilidad de día cero estaba siendo explotada de forma activa, Adobe lanzó en octubre un parche para Flash Player. Tres vulnerabilidades en el iOS de Apple, conocidas colectivamente como Trident, fueron divulgadas y corregidas en agosto, luego de descubrirse que habían sido usadas en un ciberataque contra un activista de los derechos humanos en los Emiratos Árabes Unidos. En mayo, Microsoft corrigió una vulnerabilidad de día cero del Internet Explorer, que fue explotado en ataques dirigidos en Corea del Sur.

Vulnerabilidades divulgadas en sistemas de control industrial

El número de vulnerabilidades descubiertas en sistemas de control industrial (ICS) cayó en relación a 2015.



Del mismo modo, el número de vulnerabilidades en sistemas de control industrial (ICS) descubiertas durante 2016 cayó en relación a 2015, y eso brinda más evidencias que sugieren que las vulnerabilidades se han vuelto más difíciles de encontrar para los atacantes.

Tendencias y análisis

La subversión surge como un nuevo motivo para los ataques dirigidos.

Una de las tendencias que más llamaron la atención en 2016 fue el destaque de operaciones que intentan influir en eventos políticos en países blanco de ataque. Tradicionalmente, los grupos de ataques dirigidos se concentraban en el espionaje y mantuvieron un perfil discreto para evitar que fuesen detectados, sin embargo varios grupos añadieron operaciones más explícitas a su lista en 2016.

En agosto de 2016, se divulgaron de forma online datos valiosos vinculados al grupo de ciberespionaje Equation, por un grupo llamado "Shadow Brokers". La fuga de datos contenía herramientas y exploits usados por Equation, y el grupo Shadow Brokers alegó que era una fracción de lo que se había obtenido, ofreciendo subastar el resto al mejor postor.

La mayoría de los archivos difundidos parece tener varios años, con fechas entre 2010 y 2013. Cómo llegaron a manos del grupo que divulgó la información, nadie lo sabe. El grupo Shadow Brokers era desconocido antes de este incidente, sin embargo, es posible también que sea un pseudónimo de otro grupo.

Debido a que los intentos de Shadow Brokers de vender los datos robados parecían sin convicción, es probable que difamar al grupo Equation en vez de ganancia monetaria fue el principal motivo de la filtración de datos.

El incidente subversivo más marcante del año fue una serie de invasiones contra el Partido Demócrata, que se produjo en el período que antecedió a la elección presidencial de 2016 en EE.UU. Una investigación conjunta de la Comunidad de Inteligencia de EE.UU. concluyó que dos grupos vinculados a los servicios de inteligencia rusos fueron responsables de la campaña.

Los dos grupos eran previamente conocidos por Symantec y están activos desde hace varios años, participando en espionaje contra una serie de blancos en EE.UU. y en Europa. Fritillary (aka APT29 y Cozy Bear) está activo al menos desde 2010 y era conocido por usar la familia de troyanos Duke contra sus víctimas, como por ejemplo Cozyduke (Trojan.Cozer) y Seaduke (Trojan.Seaduke). Swallowtail (también conocido como APT28 y Fancy Bear) está activo desde hace por lo menos 10 años y generalmente usa el troyano Sofacy (Infostealer. Sofacy) como una de sus principales herramientas de malware. Fritillary es conocido por tener como blanco de ataque a individuos y compañías de alto nivel en el gobierno, en la política internacional y en las entidades de investigación en la Unión Europea y Estados Unidos, mientras que Swallowtail se dirige principalmente a militares, gobiernos, embajadas y a los equipos de empresas contratadas para la defensa en países de Europa Oriental.

En septiembre, Swallowtail también estuvo involucrado en la filtración de registros médicos robados de la Agencia Mundial de Antidoping (WADA). Tras una invasión, se divulgaron los datos relacionados a los atletas olímpicos estadounidenses, ciclistas británicos y de otros países.

De acuerdo con WADA, Swallowtail fue responsable de la invasión. El grupo adoptó la estrategia inusual de crear su propio sitio web (usando el apodo Fancy Bear) para publicar los datos robados junto con reivindicaciones que contenían pruebas de atletas que habían infringido reglas de antidoping.

Las invasiones a DNC y a WADA constituyeron un gran cambio en la táctica de estos grupos, que no se habían involucrado anteriormente en ese tipo de actividad subversiva. El informe de la comunidad de inteligencia de EE.UU. sobre el robo de datos de DNC y subsiguientes divulgaciones públicas, reveló que formaban parte de una campaña de influencia conducida por el gobierno ruso teniendo como objetivo la elección presidencial de EE.UU en 2016. También concluyó que la campaña habría sido vista como un éxito en Rusia y que esas actividades posiblemente se usarán para informar futuras operaciones de influencia.

Dado el comprobado potencial para sembrar el caos y confusión, existe una fuerte probabilidad de que esas tácticas puedan emplearse nuevamente en un intento de desestabilizar a otros países. Francia y Alemania tienen elecciones este año y Bruno Kahl, jefe del servicio de inteligencia extranjera en Alemania, dijo que el mismo tipo de ataques ya ha empezado contra Alemania. "Existen evidencias de ciberataques que no tienen otra finalidad sino desencadenar la incertidumbre política", dijo Bruno Kahl. "Los delincuentes están interesados en deslegitimar el proceso democrático, no importa a quien ayude eso posteriormente."

Retornan los ataques de sabotaje

Los ataques de sabotaje resurgieron en 2016, empezando con una serie de ataques contra Ucrania que involucraba el uso de malware que borra el contenido de discos. Los ataques se vincularon a otro grupo, posiblemente ruso, de ciberespionaje conocido como Sandworm y contenía un troyano altamente destructivo (Trojan. Disakil). Ataques en el fin de 2015 e inicios de 2016 afectaron a organizaciones de medios de comunicación y al sector de energía en Ucrania, siendo que este último fue asociado a cortes de energía en el país.

Disakil retornó a fines de 2016, cuando una nueva versión circuló camuflada de ransomware. Se supone que el malware fue utilizado en una serie de intentos de ataques contra el sector financiero en Ucrania.

La variante fue proyectada para ejecutarse en computadoras Linux y, al ejecutarse, las tornaba inutilizables al cifrar archivos esenciales del sistema operativo. Una vez que el cifrado termina, se exhibe un mensaje solicitando un rescate de 222 Bitcoin (aproximadamente US$ 210.000 en el momento de los ataques). El pago del rescate no descodificaba los archivos afectados, siendo que las claves de cifrado generadas en la computadora infectada no eran guardadas localmente ni en un servidor de comando y control (C&C). El malware posiblemente fue disfrazado como ransomware, para engañar a las víctimas y que no investigasen completamente los ataques.

También se produjeron ataques de sabotaje en otras regiones, uno de los más notables fue el retorno del malware de Shamoon (W32.Disttrack), que borra el contenido de discos, luego de una ausencia de cinco años. Usado por primera vez en ataques contra el sector de energía en Arabia Saudita en 2012, una nueva variante (W32.Disttrack.B) fue usada contra blancos de ataque en Arabia Saudita en noviembre de 2016 y en enero de 2017.

En la primera ola de nuevos ataques, el malware fue configurado para lanzar su carga útil y borrar el contenido de los discos el jueves, 17 de noviembre a las 20:45, horario local. La semana laboral en Arabia Saudita es de domingo a jueves. De ese modo, el ataque fue coordinado para que se produjese después de que la mayoría del equipo hubiese regresado a sus casas para el fin de semana, en la esperanza de reducir la posibilidad de descubrirse antes que el daño máximo pudiese ser causado.

El malware Shamoon fue configurado con contraseñas que parecían haber sido robadas de las empresas víctimas. Esas contraseñas probablemente se utilizaron para permitir que el malware se propagase por la red de una empresa.

Es posible que los ataques tuvieran intereses políticos. En los ataques de 2012, las computadoras infectadas tuvieron su registro maestro de inicialización borrado y sustituido por una imagen de una bandera en llamas de EE.UU. Los últimos ataques usaron una foto del cuerpo de Alan Kurdi, el refugiado sirio de tres años que se ahogó en el Mediterráneo en 2015.

Los ataques de noviembre eran vinculados a un grupo conocido como "Greenbug", que fue descubierto por Symantec durante su investigación sobre los ataques Shamoon. Greenbug tiene como víctimas una serie de empresas en Medio Oriente, que incluyen empresas en los sectores de aviación, energía, gobierno, finanzas y educación. Symantec descubrió que Greenbug infectó al menos una computadora administradora perteneciente a una empresa que fue posteriormente afectada por Shamoon.

Los ataques de enero se perpetraron por un grupo conocido como "Timberworm" (vea el panel Cómo los grupos de ataque de Shamoon usaron tácticas con "herramientas del día a día"). Aunque Greenbug y Timberworm parecían ser grupos distintos, si ambos están distribuyendo Shamoon, es probable que sea hacia una única entidad.

Uso de herramientas del día a día

Los grupos de ataque comenzaron a alterar sus tácticas, ampliando su gama de herramientas y muchos grupos ya no dependen más del tradicional toolkit de malware para ataque y vulnerabilidades de día cero. A pesar de que no sea una nueva técnica, los delincuentes están usando cada vez más "herramientas del día a día", recursos del sistema operativo, legítimas herramientas y servicios en la nube para afectar las redes. Esa táctica puede dificultar la detección de ataques, una vez que es más difícil detectar el uso malicioso de herramientas legítimas que la presencia de malware.

Como los atacantes de Shamoon emplearon tácticas con "herramientas del día a día"

Un exponente notable del uso de "herramientas del día a día" en 2016 fue Timberworm, un grupo de ciberespionaje vinculado a la retomada de ataques involucrando el malware destructivo Shamoon (W32. Disttrack.B). Tras una ausencia de cuatro años, Shamoon resurgió en noviembre de 2016 con una serie de ataques contra víctimas en Arabia Saudita. Dos olas más de ataques se llevaron a cabo en noviembre de 2016 y nuevamente en enero de 2017.

Mientras que los ataques de noviembre estaban vinculados a un grupo conocido como "Greenbug", los ataques de enero se lanzaron por Timberworm, un grupo de ciberespionaje responsable de una serie de ataques en todo Medio Oriente.

Para distribuir Shamoon, Timberworm primero envió correos electrónicos de spear phishing a individuos en empresas blanco de ataque. En algunos casos, los correos electrónicos contenían archivos del Microsoft Word o Excel como adjuntos. En otros, los correos electrónicos contenían enlaces maliciosos, que al hacer clic, bajaban los archivos similares del Word o del Excel.

Si el archivo fuese abierto, una macro ejecutaba un script del PowerShell que proveía el acceso remoto y realizaba reconocimiento básico de la computadora afectada. Si una computadora era de interés, entonces instalaban el malware (Backdoor.Retriever).

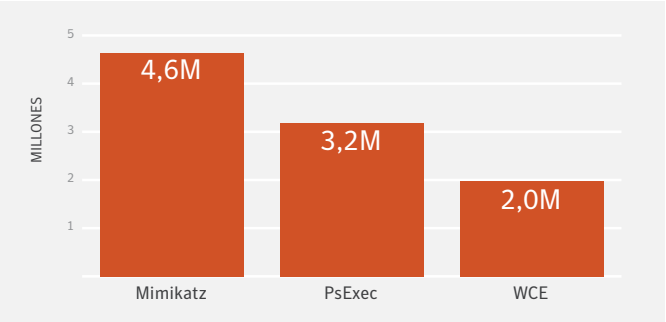
A partir de ahí, los grupos de ataque usaron muchas herramientas legítimas administrativas y de prueba de penetración para recorrer la red de la víctima e identificar las computadoras que serían infectadas. Estas incluían:

- PsExec, una herramienta para ejecutar los procesos en otros sistemas a partir del Microsoft Sysinternals.
- PAExec, una reimplantación gratuita de PsExec de PowerAdmin
- Netscan, un escáner de red IPv4/IPv6 multifuncional
- Samdump, una herramienta de hacking que descarga hash de la contraseña del Windows
- Mimikatz (Hacktool.Mimikatz), una herramienta de hackeo usada para recopilar credenciales
- TightVNC, una aplicación de acceso remoto al escritorio de trabajo de código abierto
- Plink, una herramienta de conexión de red de líneas de comando que soporta comunicaciones cifradas
- Rar, utilitario de archivado para compactar archivos antes de la exfiltración

Una vez concluida la operación de reconocimiento, Shamoon (W32. Disttrack.B) se instalaba en las computadoras preseleccionadas. El malware fue configurado para disparar su carga útil que borraba el contenido de los discos en un horario programado, en todas las computadoras invadidas, maximizando el impacto de los ataques.

Las herramientas más frecuentes que los atacantes pueden usar de forma indebida

De acuerdo con la telemetría de reputación de archivos de Symantec, las herramientas legítimas más vistas que podrían haber sido usadas indebidamente por delincuentes en 2016 fueron Mimikatz, PsExec y WCE.



Según la telemetría de reputación de archivos de Symantec, la herramienta legítima más ampliamente vista que podría haber sido usada indebidamente por delincuentes durante 2016 fue Mimikatz (Hacktool.Mimikatz) - una herramienta capaz de alterar privilegios, exportar certificados de seguridad y recuperar contraseñas del Windows en texto simple - seguido de la Herramienta PsExec de Microsoft Sysinternals y Editor de Credenciales del Windows. Dado el gran número de casos y el hecho de que todas las tres herramientas tienen usos legítimos (incluso Mimikatz puede usarse para pruebas de penetración), es fácil ver el apelo de esas herramientas para los cibercriminales, debido a que su uso puede pasar desapercibido.

Los scripts maliciosos del PowerShell también han sido ampliamente utilizados en ataques dirigidos, con delincuentes explotando la flexibilidad de la estructura para bajar cargas útiles, atravesar redes afectadas y realizar reconocimiento. Investigaciones recientes de Symantec han demostrado la popularidad de PowerShell como una herramienta de ataque. De todos los scripts del PowerShell analizados por sandbox Blue Coat Malware Analysis de Symantec, el 95,4% eran maliciosos.

Esta práctica recientemente ha sido usada de forma extensiva por una serie de grupos. Un caso marcante fue la invasión antes mencionada al DNC en la preparación para las elecciones presidenciales de EE.UU. Uno de los principales puntos de infección, de acuerdo con el FBI fue un correo electrónico de spear phishing enviado a la cuenta de correo electrónico del presidente de la campaña, John Podesta, el 19 de marzo de 2016. El correo electrónico fue creado para simular que había sido enviado de una cuenta administrativa oficial de Gmail, sugiriendo que su correo electrónico había sido invadido y orientándolo a redefinir su contraseña. Incluía una URL acortada que ocultaba una URL maliciosa.

Al hacer clic, la víctima era direccionada hacia una página falsa de redefinición de contraseña, encubierta para parecer una página legítima de redefinición de cuentas del Gmail. No se necesitaron ningún malware o exploits para ejecutar el ataque. En lugar de ello, se utilizó simple ingeniería social para obtener la contraseña.

Correo electrónico de spear phishing usado en los ataques al DNC

El texto del correo electrónico de spear phishing enviado a John Podesta, el presidente de la campaña presidencial Clinton 2016.

"From:" Google <no-reply@accounts.googlemail.com>
"Date:" March 19, 2016 at 4:34:30 AM EDT
"To:" [redacted]@gmail.com
"Subject:" "Someone has your password"

Someone has your password
Hi John

Someone just used your password to try to sign in to your Google Account [redacted]@gmail.com.

Details:
Saturday, 19 March, 8:34:30 UTC
IP Address: 134.249.139.239
Location: Ukraine

Google stopped this sign-in attempt. You should change your password immediately.

CHANGE PASSWORD <https://bit.ly/1PibSU0>

Best,
The Gmail Team
You received this mandatory email service announcement to update you about important changes to your Google product or account.

Otro ejemplo de "uso de herramientas del día a día" es proporcionado por el grupo de ciberespionaje Chafer, que parece tener base en Irán. Uno de sus vectores de ataque es invadir los servidores web, explotando vulnerabilidades identificadas a través de herramientas de verificación web. En una reciente invasión contra un blanco en Turquía, Symantec descubrió que Chafer utilizó una herramienta de software llamada JexBoss para identificar una versión comunitaria más antigua, sin parches de corrección, de JBoss Application Server perteneciente a la víctima. De ese modo, el grupo implantó un web shell en el servidor, un script que permite la administración remota, así como una copia de la herramienta de software Mimikatz.

De ahí, fueron capaces de usar herramientas nativas del sistema operativo como Qwinsta y Whoami para extraer información sobre el servidor invadido. Tras 20 minutos de invasión inicial, el grupo usó la herramienta PsExec de Microsoft Sysinternals para propagarse hacia otras dos computadoras en la red de la víctima.

Recientemente otra organización hizo uso de esta táctica, el grupo con base en China llamado Tick, que ha enfocado principalmente en empresas japonesas desde hace por lo menos 10 años. Campañas recientes del grupo usan correos electrónicos de spear phishing e invaden sitios web japoneses para infectar a sus víctimas.

Una de las principales herramientas del Tick es su propio malware personalizado (Backdoor.Daserf), pero el grupo también usa una variedad de herramientas como Mimikatz, Windows Credential Editor y GSecdump (Gsecdump), una herramienta de hackeo que puede usarse para robar hash del Gerenciador de cuentas de seguridad (SAM), Active Directory y sesiones activas.

Existen también instancias de grupos de ataque que utilizan servicios básicos en la nube, en vez de servidores de comando y control para exfiltración de datos. Por ejemplo, se descubrió que Fritillary, uno de los grupos que atacó el DNC, usó alrededor de 200 cuentas Microsoft OneDrive para exfiltrar los datos robados. El objetivo parecía esconderse en lugares visibles y los grupos de ataque pueden haber decidido que los datos movidos hacia OneDrive podrían confundirse con una actividad legítima.

Espionaje económico

En septiembre de 2015, EE.UU. y China llegaron a un acuerdo en el que ninguno de ellos conduciría espionaje económico en el ciberespacio. Según los términos del acuerdo, los dos países concordaron que ningún gobierno "conduciría o apoyaría conscientemente el robo con ciberherramientas de propiedad intelectual, incluyendo secretos comerciales u otra información comercial confidencial, con la intención de ofrecer ventajas competitivas a empresas o sectores comerciales".

Dada la naturaleza de tales operaciones de espionaje, puede ser difícil establecer si este acuerdo está funcionando. Sin embargo, el análisis de Symantec encontró fuertes evidencias de que hubo una reducción acentuada en la actividad de grupos probablemente asociados a China desde que el acuerdo fue firmado.

El análisis de las detecciones de familias de malware usadas por grupos de ciberespionaje, que Symantec cree que tiene bases en China, brindó una visión sobre los niveles de actividad en el transcurso del tiempo. Casi inmediatamente después de la firma del acuerdo, el número de invasiones disminuyó considerablemente. Los índices de invasión continuaron disminuyendo en los siguientes meses y permanecieron bajos en el fin del año.

Asociada a esa tendencia, algunos específicos grupos chinos también exhibieron cambios en los modelos de sus actividades. Por ejemplo, el grupo Buckeye (aka APT 3 o Gothic Panda) condujo operaciones de ciberespionaje contra compañías en EE.UU., Reino Unido y otros países durante por lo menos cinco años. Sin embargo, el interés del grupo empezó a cambiar durante la preparación del acuerdo entre EE.UU. y China.

A partir de junio de 2015, el grupo comenzó a invadir entidades políticas en Hong Kong. En marzo de 2016, Buckeye migró prácticamente todo su interés hacia organizaciones en Hong Kong. Si bien no existe ninguna prueba definitiva de que el cambio de interés fue motivado por el acuerdo, fue consistente con la tendencia general de una reducción en la actividad de ciberespionaje contra víctimas en otros países. A pesar de que el acuerdo entre EE.UU. y China haya causado un cambio de enfoque para algunos grupos de ciberataques, eso no significa necesariamente que las operaciones hayan parado completamente.

Surgen nuevas amenazas

Además de la actividad constante de los grupos de ataque conocidos, otras amenazas emergieron de las sombras durante 2016. En agosto, Symantec destacó un grupo previamente desconocido llamado Strider, que ha arquitectado ataques contra blancos de ataque seleccionados en Rusia, China, Suecia y Bélgica.

La principal herramienta del Strider es un troyano furtivo conocido como Remsec (Backdoor.Remsec), que parece ser tan sofisticada, que evaluamos que puede haber sido desarrollada principalmente para fines de espionaje. Activa desde por lo menos de 2011, Strider mantuvo un perfil discreto, en parte porque era altamente selectiva en la elección de víctimas, siendo que Symantec encontró evidencias de infecciones en 36 computadoras, en siete diferentes organizaciones.

Remsec presentó un alto nivel de competencia técnica, que contenía una serie de recursos avanzados proyectados para ayudar a evitar la detección. Varios componentes eran en forma de blobs ejecutables (Binary Large Objects), que son más difíciles de detectarse por un software antivirus tradicional basado en firma. Asimismo, gran parte de la funcionalidad del malware es implantada en la red, lo que significa que reside apenas en la memoria de una computadora y nunca se almacena en el disco, tornándola más difícil de detectarse.

Remsec ilustra los niveles de competencia y recursos que los grupos patrocinados por naciones pueden aplicar actualmente para afectar a sus víctimas. A medida que los proveedores se vuelven más eficaces en descubrir los grupos de ataques dirigidos, lo que llevó a algunos delincuentes a alejarse de las herramientas sofisticadas, todavía existen algunas operaciones que están en un nivel extremadamente avanzado.

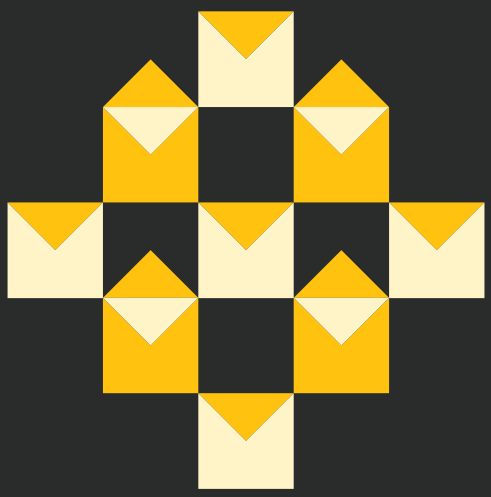
Lectura adicional

- Grupo de ciberespionaje Buckeye cambia su atención de EE.UU. hacia Hong Kong
- Equation: ¿El grupo secreto de ciberespionaje fue violado?
- Strider: El grupo de ciberespionaje usa Sauron contra las víctimas
- Grupo de ciberespionaje Patchwork expande sus blancos de ataque de gobiernos hacia una amplia gama de segmentos
- Grupo de ciberespionaje Tick enfoca esfuerzos en Japón
- Taiwán es víctima del nuevo troyano backdoor de ciberespionaje
- Suckfly: Revelando la vida secreta de sus certificados de firma de código
- La Operación Colaborativa Blockbuster pretende nuevamente eliminar Lazarus
- Malware destructivo Disakil vinculado a la interrupción de energía en Ucrania también fue usado contra organizaciones de medios de comunicación
- Shamoon: Reaparece y está más destructivo que antes
- Grupo de ciberespionaje Greenbug enfocado en Medio Oriente, posiblemente relacionado a Shamoon
- Shamoon: Ataques destructivos de múltiples etapas limitados a blancos de ataque específicos

Mejores prácticas

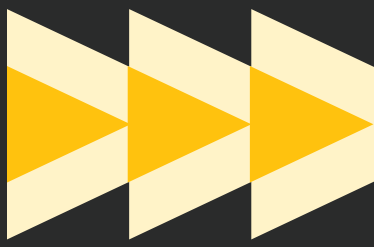
- Céntrese en múltiples sistemas de defensa, sobrepuestos y que tengan sinergia para proteger contra fallas en puntos únicos en cualquier tecnología o método de protección. Esto debe incluir la implantación de firewalls actualizados regularmente, así como antivirus para gateway, sistemas de detección o protección de invasiones (IPS), identificación de vulnerabilidades de sitios web con protección contra malware y soluciones de seguridad web para gateway en toda la red.
- La explotación de vulnerabilidades es una táctica frecuentemente usada por grupos de ataques dirigidos. Reciba alertas para nuevas vulnerabilidades y amenazas en plataformas de proveedores y aplique las correcciones para vulnerabilidades conocidas lo más rápido posible.
- Implemente y aplique una política de seguridad a través de la cual los datos confidenciales son cifrados cuando se almacenan o se transmiten. Garantice que los datos del cliente también sean cifrados. Eso puede ayudar a mitigar los daños de potenciales pérdidas internas de datos de una organización.
- Los grupos de ataque frecuentemente usan credenciales robadas o estándar para invadir una red. Garantice que las contraseñas sean fuertes.
  Las contraseñas importantes, como las que poseen altos privilegios, deben contener por lo menos 8-10 caracteres e incluir una combinación de letras y números.
  Incentive a los usuarios a evitar la reutilización de las mismas contraseñas en varios sitios y debe estar prohibido compartirlas con otras personas. Excluya credenciales y perfiles no utilizados y limite el número de perfiles creados de nivel administrativo.
- Instruya a los funcionarios acerca de los peligros de correos electrónicos de spear phishing, que incluyen la cautela necesaria para los correos electrónicos de fuentes desconocidas y abrir archivos adjuntos que no fueron solicitados. Una solución completa de protección ayuda en la defensa contra las amenazas enviadas por correo electrónico, incluyendo Symantec Email Security.cloud que puede bloquear las amenazas transmitidas por correo electrónico y Symantec Endpoint Protection, que puede bloquear malware en los endpoints. La tecnología Symantec Messaging Gateway Disarm también puede proteger a las computadoras de amenazas, removiendo el contenido malicioso de documentos adjuntos incluso antes de llegar al usuario.

Correo Electrónico: Malware, spam y phishing



Sección

04



Symantec

Introducción

Si bien el correo electrónico es una herramienta esencial de comunicación, también es una de las principales fuentes de interrupción de las actividades, para los usuarios finales y las organizaciones. Esa interrupción puede ser causada por correos electrónicos indeseados en la forma de spam hasta amenazas más peligrosas, como la propagación de ransomware o campañas de spear phishing segmentadas.

Debido a que poco más de la mitad de todos los correos electrónicos (53%) son spam, un porcentaje creciente de ese spam contiene malware. Ese aumento en malware transmitido por correo electrónico es motivado en gran parte por una profesionalización de las operaciones de spam con malware. Los desarrolladores de malware pueden tercerizar sus campañas de spam para grupos especializados que realizan campañas de spam en gran volumen. La gran escala de las operaciones de malware de correo electrónico indica que los grupos de ataque están teniendo considerables lucros con esos tipos de ataques y el correo electrónico posiblemente continuará siendo uno de los principales medios de ataque en 2017.

Principales conclusiones

- La tasa de malware en correo electrónico aumentó considerablemente en 2016. 1 de cada 220 correos electrónicos enviados contenía malware en 2015, para 1 de cada 131 correos electrónicos en 2016. Este aumento fue causado principalmente por botnets, que se emplean para entregar enormes campañas de spam relacionadas a amenazas como Locky (Ransom.Locky), Dridex (W32.Cridex) y TeslaCrypt (Ransom.TeslaCrypt).
- Campañas de spear phishing dirigidas, especialmente campañas BEC (Business Email Compromise), en lugar de campañas de phishing de envío masivo de correos electrónicos, son actualmente las favoritas de los delincuentes. Eso se refleja en la disminución en la tasa de phishing, que cayó de 1 de cada 1.846 correos electrónicos para 1 de cada 2.596 correos electrónicos.
- Grandes grupos de amenazas vía correo electrónico dependen principalmente del uso de archivos ejecutables en la primera fase del ataque para instalar su carga útil, normalmente ransomware. A inicios de 2016, los documentos del Office que contenían macros maliciosos era la forma más común de usar el archivo ejecutable en las campañas de spam. Sin embargo, en marzo se produjo un cambio y, desde entonces, JavaScript downloaders ha dominado este panorama.

Tendencias y análisis

Los datos recopilados de correo electrónico durante 2016 demuestran que el correo electrónico se volvió el principal vector para la propagación de malware.

Amenaza de Malware

La tendencia más notable observada hasta 2016 fue el aumento de la tasa de malware por correo electrónico. La tasa aumentó drásticamente, de 1 de cada 220 correos electrónicos en 2015 para 1 de cada 131 correos electrónicos en 2016.

Tasa General de Malware de Correo Electrónico

2014	2015	2016
1 de cada 244	1 de cada 220	1 de cada 131

Ese aumento en el malware vía correo electrónico posiblemente puede estar relacionado a la actividad continua durante 2016 de grupos enfocados en el envío de malware a través de correos electrónicos masivos, distribuyendo principalmente Locky, Dridex y TeslaCrypt. Uno de los principales distribuidores de malware es una botnet conocida como Necurs (Backdoor.Necurs). Necurs es responsable de campañas masivas que propagan malware a través de archivos adjuntos de macros JavaScript y Office. Esos archivos ejecutables posteriormente instalan la carga útil final, que en 2016 eran típicamente amenazas de ransomware, como Locky.

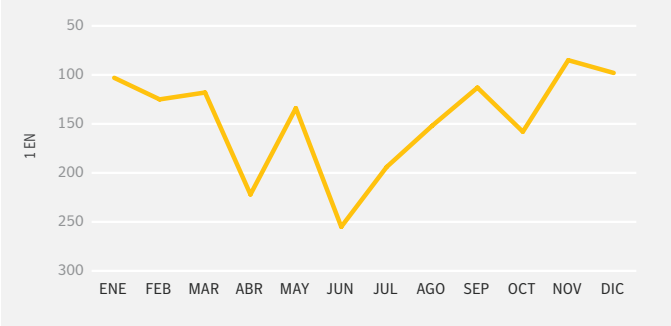
Necurs estuvo inactiva entre el 24 de diciembre de 2016 y el 20 de marzo de 2017, reflejando que hubo un descenso significativo en la tasa de malware de correo electrónico en enero y febrero de 2017. Si bien no es inusual para los grupos de malware hacer una pausa durante la Navidad, esas pausas generalmente solamente duran aproximadamente una semana. El motivo para la suspensión de las operaciones de Necurs permanece un misterio, pero el grupo fue capaz de retomar inmediatamente las campañas de envío masivo a su regreso. El 20 de marzo, el día de su retorno, Symantec bloqueó casi dos millones de correos electrónicos maliciosos.

Dridex es un troyano financiero usado para robar las credenciales bancarias de usuarios finales. Los grupos de ataque responsables de Dridex son profesionales que dedican un gran esfuerzo para refinar continuamente el malware y hacer que los correos electrónicos empleados para distribuirlo parezcan legítimos. TeslaCrypt y Locky son instancias de ransomware, siendo que Locky surgió en febrero de 2016. El ransomware fue uno de los principales temas de ciberseguridad en 2016.

La telemetría mensual recopilada por Symantec mostró un fuerte inicio de año para el malware enviado vía correo electrónico, con caídas acentuadas en abril y junio, momentos en los que se relataron un descenso en las actividades de los grupos responsables de Locky, Dridex y otros.

Tasa Mensual de Malware por Correo Electrónico

La tasa mensual de malware por correo electrónico muestra caídas acentuadas en abril y junio, que pueden relacionarse a la actividad de autoridades legales contra varios grupos de cibercriminales.



Symantec cree que esa caída en las actividades puede estar asociada a la actividad de autoridades legales, siendo que la disminución de las actividades en junio se produjo a seguir del arresto de 50 personas en Rusia, supuestamente vinculadas al grupo de fraude bancario Lurk.

Sin embargo, esa caída de las actividades fue apenas temporal y las campañas de spam de malware retornaron rápidamente en gran volumen. Campañas que involucraban Dridex y Locky recomenzaron, al tiempo que los incidentes de la familia de amenazas Kovter (Trojan.Kovter) empezaron a aumentar en agosto y mantuvieron ese crecimiento por el resto del año. Para obtener más información acerca de las campañas de ransomware enviadas masivamente vía correo electrónico, consulte nuestro capítulo sobre Ransomware.

Tasa de Malware de Correo Electrónico por Sector

Las Ventas al por Mayor y la Agricultura fueron los sectores de la industria clasificados como los más afectad.

Sector	Tasa de Malware de Correo Electrónico (1 de cada)
Establecimientos No Clasificables	103
Agricultura, Forestal y Pesca	111
Comercio Mayorista	111
Servicios	121
Manufactura	130
Comercio Minorista	135
Minería	139
Administración Pública	141
Transporte & Servicios Públicos	176
Construcción	179
Finanzas, Seguros y Mercado Inmobiliario	182

Con excepción de las ventas al por menor, que vio una disminución en su tasa de malware de correo electrónico (1 de cada 74 correos electrónicos en 2015 para 1 de cada 135 correos electrónicos en 2016), cada sector vio un aumento en el volumen de malware vía correo electrónico en 2016. Los aumentos más considerables fueron en los sectores de Transportes (1 de cada 338 correos electrónicos para 1 de cada 176), Finanzas (1 de cada 310 para 1 de cada 182), y Minería (de 1 de cada 304 para 1 de cada 139). El segmento de salud vio un aumento de 1 de cada 396 correos electrónicos para 1 de cada 204.

En 2016, el malware de correo electrónico afectó a las compañías de todos los tamaños. Sin embargo, las pequeñas y medianas empresas (con 251 a 500 funcionarios) fueron las más afectadas, de acuerdo con nuestros números.

Tasa de Malware de Correo Electrónico por Tamaño de Empresa

La tasa más grande de malware en el tráfico de correo electrónico fue en el grupo de empresas de tamaño de 251 a 500, con 1 de cada 95 correos electrónicos recibidos que contenía malware.

Tamaño de la Empresa	Tasa de Malware de Correo Electrónico (1 de cada)
1-250	127
250-500	95
501-1000	139
1001-1500	224
1501-2500	104
+2501	170

Phishing

En los últimos años las tasas de phishing están en descenso y cayeron nuevamente en 2016, pasando de 1 de cada 1.846 correos electrónicos para 1 de cada 2.596 correos electrónicos.

Tasa General de Phishing

2014	2015	2016
1 de cada 965	1 de cada 840	1 de cada 2596

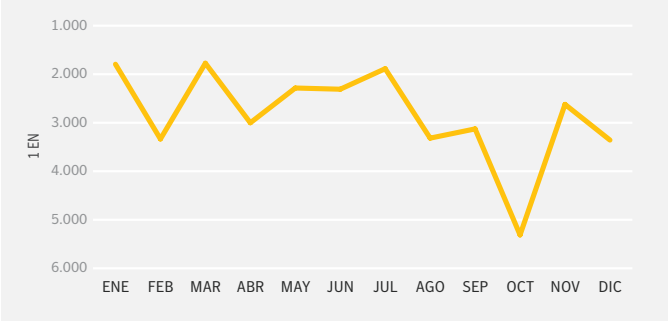
Hubo una notable caída en octubre, cuando la tasa de phishing fue de apenas 1 de cada 5.313 correos electrónicos, antes de que la tasa retornase a una figura más próxima del “promedio” de 1 de cada 2.621 correos electrónicos en noviembre.

En octubre se produjeron muchos hechos en el mundo de la seguridad de la información, incluyendo la botnet Mirai que ganó destaque tras un ataque distribuido de denegación de servicio (DDoS) en el proveedor de DNS Dyn, que afectó a varios

sitios web de gran importancia, incluyendo Spotify, Netflix y PayPal. También se relató un aumento de la actividad en torno de la familia de amenazas Kovter (Trojan.Kotver). Sin embargo, no existe ninguna evidencia para que la tasa de phishing haya caído tan acentuadamente en ese mes.

Tasa mensual de phishing

Las cifras mensuales de la tasa de phishing muestran una caída notable en octubre, pero no hubo ninguna evidencia motivo para una caída tan significativa en ese mes.



Es posible que existan innúmeras razones responsables de la disminución de las actividades de phishing. Cada vez más los consumidores conocen los peligros de hacer clic en enlaces desconocidos o bajar archivos adjuntos sospechosos, lo que demuestra que es posible que las campañas de phishing "estándar", indiscriminadas y de envío masivo de correo electrónico, se vuelvan menos eficaces para los delincuentes.

Tasa de phishing por sector

La agricultura fue el sector más afectado por el phishing en 2016, con 1 de cada 1.815 correos electrónicos clasificados como intentos de phishing.

Sector	Tasa de Phishing (1 de cada)
Agricultura, Forestal y Pesca	1815
Finanzas, Seguros y Mercado Inmobiliario	1918
Minería	2254
Administración Pública	2329
Comercio Minorista	2419
Establecimientos No Clasificables	2498
Servicios	3091
Manufactura	3171
Comercio Mayorista	4742
Construcción	4917
Transporte & Servicios Públicos	6176

Tasa de phishing por tamaño de empresa

La tasa más grande de phishing se produjo en el grupo de empresas de tamaño de 251 a 500 funcionarios, con 1 de cada 2.554 correos electrónicos recibidos clasificados como intentos de phishing.

Tamaño de la Empresa	Tasa de Phishing (1 de cada)
1-250	2897
250-500	2554
501-1000	4023
1001-1500	6640
1501-2500	2610
+2501	3323

Sin embargo, spear phishing continúa creciendo. Algunos casos de gran importancia fueron vistos a lo largo de 2016, como el hackeo de los correos electrónicos del presidente de la campaña de Hillary Clinton, John Podesta, y del exsecretario de Estado norteamericano Colin Powell, donde se utilizaron correos electrónicos de phishing.

Fraudes BEC

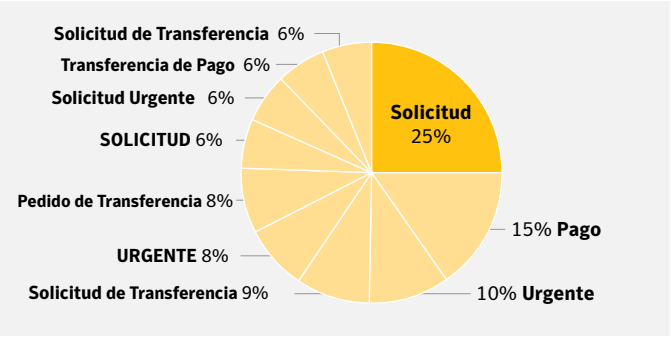
Los fraudes BEC, que emplean correos electrónicos de spear phishing, tuvieron un creciente destaque en 2016. También conocidos como fraude de CEO o "caza a las ballenas", los fraudes BEC son una forma de estafa financiera de baja tecnología donde se envían correos electrónicos falsos hacia el equipo financiero por estafadores fingiendo ser el CEO o Directores. A seguir, los estafadores solicitan una gran transferencia de dinero. Esos fraudes pueden ser perjudiciales, pues exigen poco conocimiento técnico, pero pueden generar grandes recompensas financieras para los delincuentes y pérdidas significativas para las empresas implicadas. Por ejemplo, a inicios de 2016, una compañía aeroespacial austríaca despidió a su CEO después de haber perdido casi US $ 50 millones para los fraudes BEC

La investigación de Symantec en el primer semestre de 2016 descubrió que más de 400 empresas son víctimas de fraudes BEC todos los días, y que las pequeñas y medianas empresas son las más afectadas. Estimativas del FBI indican que en los últimos tres años más de US$ 3.000 millones fueron perdidos para fraudes BEC, con más de 22.000 víctimas en todo el mundo.

La investigación de Symantec descubrió que esos fraudes son una evolución de los famosos fraudes de correos electrónicos nigerianos; casi la mitad de las direcciones de correo electrónico analizados por Symantec tenían direcciones de IP nigerianos. Los correos electrónicos enviados de lunes a viernes, siguiendo una semana normal de trabajo y generalmente contenían líneas de asunto inofensivas, con palabras como "Solicitud", "Pago", "Urgente", etc.

Fraudes BEC: Líneas frecuentes de asunto

"Solicitud" fue la palabra clave más popular usada en las líneas de asunto para los correos electrónicos de fraudes BEC. Este es seguido de "Pago" (15%) y "Urgente" (10%).



Las técnicas de los fraudes BEC continúan evolucionando para asegurar el éxito de las estafas. La investigación de Symantec en noviembre reveló que, en lugar de pedir una transferencia directa de dinero, los estafadores usaban un lenguaje informal para verificar si una víctima estaba en su mesa o para encontrar más información antes de solicitar el dinero.

Recientemente una nueva técnica observada por nuestros investigadores es el "secuestro" de facturas legítimas enviadas por las empresas, para que el número de la cuenta sea alterado para el del estafador. Algunos casos ya vistos involucraban el ataque de los estafadores al servidor de correo electrónico para alterar los detalles de la factura. Otros eran apenas correos electrónicos falsos de factura enviados sin la necesidad de hackear el servidor de correo electrónico, pero que eran eficaces desde que fuesen enviados antes de las facturas legítimas.

Con la confirmación de la gran lucratividad de fraudes BEC, es posible que continúen siendo una fuerte tendencia en 2017.

Spam permanece estable

Las tasas de spam permanecieron constantes en un 53% en 2016, tras una disminución en los últimos años.

Sin embargo, este número aún demuestra que la mayoría de los correos electrónicos corporativos enviados en 2016 eran spam. Generalmente el spam es considerado como cualquier correo electrónico no solicitado que es enviado en masa y, en algunos casos, puede no contener amenazas maliciosas. Los correos electrónicos de spam pueden ser irritantes e indeseados, o pueden llevar a sitios web que realizan fraudes de clics.

Tasa general de spam

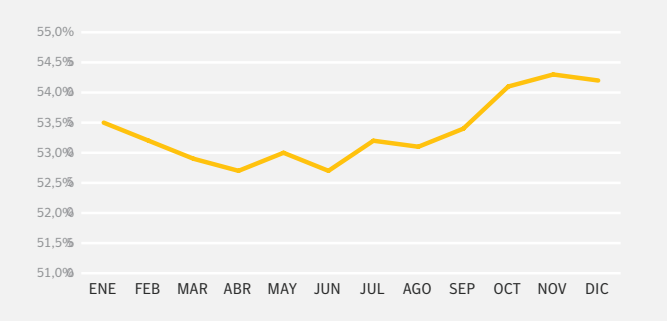
La tasa de spam entre 2015 y 2016 permaneció relativamente estable.

2014	2015	2016
60%	53%	53%

En 2015, el nivel de spam fue el más bajo visto desde 2003, y mantuvo este porcentaje en 2016. Es posible que esto se deba al crecimiento anteriormente mencionado en ransomware y campañas más específicas de spear phishing, tales como fraudes BEC. La lucratividad de esas campañas puede estar distanciando a los grupos de ataque de las antiguas campañas antispam hacia esos nuevos métodos.

Tasa mensual de spam

La tasa de spam aumentó ligeramente en el fin de 2016. En noviembre, la tasa de spam alcanzó el 54,3%, la tasa más alta vista desde marzo de 2015.



Si bien la tasa general de spam permaneció inmovilizada durante el año, hubo un aumento en el spam enviado en el último trimestre de 2016. En noviembre, la tasa de spam alcanzó el 54,3%, la tasa más alta vista desde marzo de 2015.

Algunos factores influyeron en ese gran aumento. La elección presidencial de EE.UU., que se llevó a cabo a inicios de noviembre, causó un aumento en el spam relacionado a las elecciones. Symantec bloqueó casi 8 millones de correos electrónicos relacionados a la elección presidencial en el período de la segunda quincena de septiembre a la primera quincena de octubre.

También en octubre, dos campañas significativas impactaron a los clientes de Symantec. Un ataque de spam con temas para adultos que comenzó en España impactó a los usuarios en Europa, Medio Oriente y África, una vez que se propagó rápidamente hacia varios diferentes idiomas europeos. La segunda campaña, un ataque de snowshoe significativo (vea Panel Ice-cold) envió correos electrónicos relacionados a productos y servicios de spam. Los grupos de ataque enviaban un bajo volumen de correo electrónico para sondear detecciones y abortaban la ejecución de spam en pocos minutos si los mensajes fuesen bloqueados.

El spam relacionado a Black Friday y a Cyber Monday también fue responsable de los elevados volúmenes de spam en noviembre, con una campaña usada para distribuir ransomware Locky. En diciembre, se reportó que la técnica de spam hailstorm estaba siendo usada para distribuir Dridex y Locky, pero la tasa de spam se mantuvo estable.

Los spammers parecen no discriminar cuando se trata del tamaño de las empresas que ponen como blanco de ataque. La diferencia entre las pequeñas empresas, que son los blancos más grandes, y las grandes empresas, fue de poco más del 1%.

Tasa de spam por tamaño de empresa

Se identificó una pequeña diferencia en relación al tamaño de las empresas que fueron víctimas de spam, con la tasa variando entre el 52,6% y 54,2%.

Tamaño de la Empresa	Tasa de Spam (%)
1-250	54,2
250-500	53,1
501-1000	53,4
1001-1500	53,2
1501-2500	52,6
+2501	52,8

Tasa de spam por sector

Algunos sectores reciben más spam que otros, pero el intervalo es de apenas el 8 %.

Sector	Tasa de Spam (%)
Construcción	59.5
Minería	57,1
Comercio Minorista	54,9
Manufactura	54,4
Agricultura, Forestal y Pesca	54,0
Establecimientos No Clasificables	53,0
Servicios	53,0
Finanzas, Seguros y Mercado Inmobiliario	52,9
Transporte & Servicios Públicos	52,9
Comercio Mayorista	52,6
Administración Pública	51,6

Investigaciones/Estudios de casos

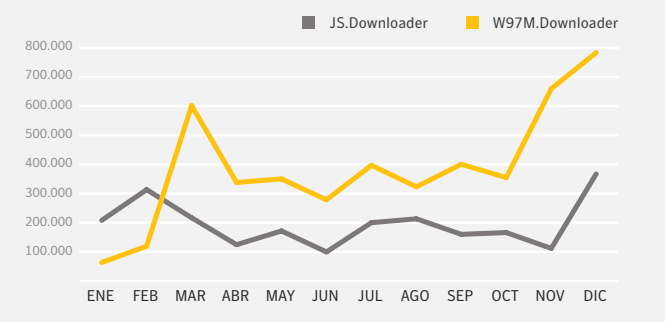
Los grupos involucrados en campañas de envío masivo de correo electrónico continuamente perfeccionan sus tácticas, en un intento de situarse un paso adelante de los sistemas de seguridad de correo electrónico.

Cambio de táctica

Una tendencia relevante en 2016 fue un cambio en el tipo de archivo ejecutable usado para entregar algunas de las amenazas más prolíficas. En el inicio del año, los documentos del Office con macros maliciosos (W97M.Downloader y variantes) eran la forma más popular de archivos ejecutables y eran usados en campañas que distribuían amenazas como Dridex (W32.Cridex). En marzo de 2016, ocurrió un cambio y el uso de archivos JavaScript (JS.Downloader y variantes) aumentó significativamente.

Detecciones de archivos ejecutables por mes

Los arhivos ejecutables de macros del Office (W97M.Downloader y variantes) y downloaders JavaScript (JS.Downloader y variantes) son los archivos usados con más frecuencia para distribuir malware vía correo electrónico. La actividad de downloaders JavaScript aumentó en 2016, mientras que los macros del Office resurgieron en diciembre de 2016.



Symantec cree que las operaciones de spam con el uso de downloaders JavaScript y macros del Office son operadas por diferentes grupos de cibercriminales. Los grupos de malware pueden contratar uno (o los dos) canales para entregar sus amenazas. Si este es el caso, hubo una tendencia de caída de los grupos de malware que favorecen las operaciones de spam con downloaders JavaScript en el final de 2016.

Si bien la propagación de archivos ejecutables de macros del Office ha sido menor a lo largo del año, Symantec no cree que ese vector desaparecerá. En realidad, podemos ver que las detecciones de W97M.Downloader aumentaron en diciembre, a pesar de que JS.Downloader continúe dominando. Esa variación podría atribuirse a la campaña de hailstorm mencionada anteriormente (vea el panel abajo) que estaba siendo usada para distribuir Locky y Dridex, que pueden ser transmitidos a través de macros maliciosos en documentos del Word.

Ice-cold: Técnicas snowshoe y hailstorm

Snowshoe spamming distribuye una amplia carga de spam a través de un conjunto de direcciones IP, para aumentar las oportunidades de éxito. Los spammers que usan la técnica snowshoe anticipan que algunos correos electrónicos serán bloqueados por filtros de spam. Sin embargo, esta técnica de envío de correos electrónicos a partir de un gran número de direcciones IP aumenta las chances de evitar filtros de spam y llegar a la bandeja de entrada de un usuario. Los spammers snowshoe envían una pequeña cantidad de spam de cada dirección IP para que permanezcan desapercibidos.

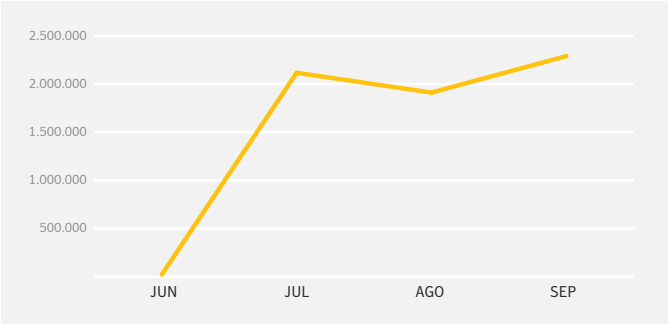
La técnica de spam hailstorm es una evolución de la técnica de spam snowshoe, y ambas existen desde hace muchos años. El spam Hailstorm también se envía usando un gran número de direccioness IP de transmisión, pero las campañas hailstorm se envían en un volumen muy alto en un corto período de tiempo. Los spammers Hailstorm pueden enviar miles de correos electrónicos muy rápidamente y, a seguir, parar inmediatamente. Algunos ataques de spam hailstorm se producen en un período tan corto de tiempo que muchas veces terminan antes de que las defensas antispam más rápidas tradicionalmente consigan actualizar su respuesta a los mismos.

Con la migración para los downloaders de JavaScript, desde julio Symantec vio un aumento significativo en el uso de adjuntos maliciosos de Windows Script File (WSF) (detectados como JS.Downloader). Los archivos WSF se proyectan para permitir una mezcla de lenguajes de script dentro de un único archivo. Son abiertos y ejecutados por Windows Script Host (WSH). Su uso como adjuntos malintencionados puede ser debido al hecho de que los archivos con la extensión .wsf no son bloqueados automáticamente por algunos clientes de correo electrónico y pueden lanzarse como un archivo ejecutable.

En especial, Ransomware fue distribuido empleando esta nueva táctica. En el segundo semestre de 2016, Symantec bloqueó una serie de grandes campañas de distribución ds Locky (Ransom.Locky), que involucraba archivos WSF maliciosos.

Correos electrónicos bloqueados con adjuntos WSF

La cifra de correos electrónicos bloqueados que contenían adjuntos WSF maliciosos aumentó considerablemente entre junio y septiembre de 2016.



Ingeniería social experimentada y comprobada

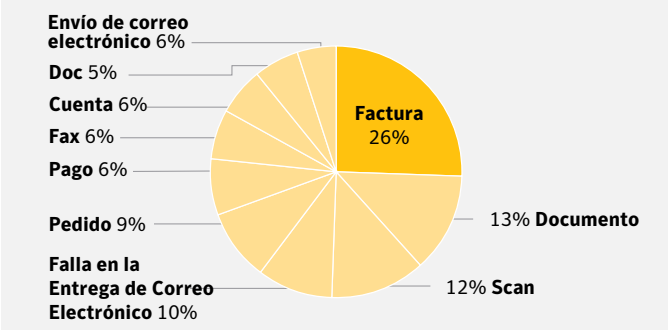
Si bien las campañas de spam que distribuyen malware dependen de una variedad de tácticas, las principales operaciones de spam de malware normalmente dependen de trucos de ingeniería social. Las amenazas como ransomware Locky o el troyano financiero Dridex pueden transmitirse por correos electrónicos camuflados como confirmaciones de transacciones financieras.

El análisis de 623 grandes campañas de spam de malware registradas por Symantec en 2016 descubrió que "factura" era la palabra clave usada con más frecuencia en las líneas de asunto. Otros términos financieros, tales como "Pedido", "Pago", y "Cuenta" también aparecen en el top 10.

El uso de palabras clave financieras ha sido una característica constante de las campañas de spam de malware a lo largo del año, indicando que los grupos de ataque poseen un alto grado de éxito con esa táctica. Como la mayoría de las empresas recibe diariamente un gran volumen de correos electrónicos legítimos de clientes y proveedores, los correos electrónicos maliciosos pueden ser inadvertidamente abiertos si no se bloquean por un software de seguridad de correo electrónico. A su vez, los consumidores pueden también ser engañados al abrir estos correos electrónicos, por desconfianza de haber sido cobrados por bienes que no solicitaron.

Palabras clave usadas en campañas de spam de malware

Las 10 principales palabras clave observadas en líneas de asunto en las principales campañas de spam de malware en 2016.

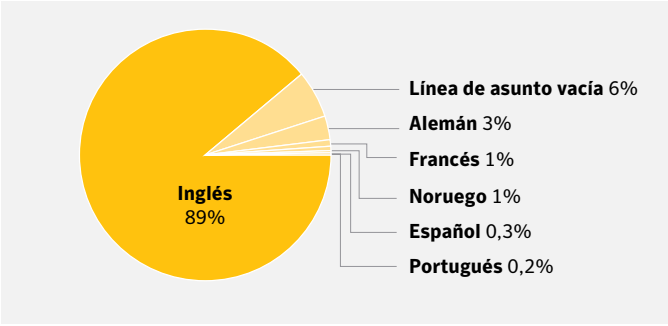


Otra táctica frecuente es disfrazar los correos electrónicos como provenientes de un escáner, impresora o dispositivo multifuncional (MFD). Los correos electrónicos que contenían las palabras clave "Scan", "Documento" y "Fax" generalmente estaban disfrazados como enviados desde estos dispositivos.

Una tercera táctica observada en 2016 fue disfrazar campañas maliciosas de spam como algún tipo de mensaje de falla de entrega de correo electrónico. El 10% de las principales campañas de spam analizadas tenían alguna forma de mensaje de falla de entrega en la línea de asunto.

Idiomas preferidos usados en campañas de spam

El idioma usado en las líneas de asunto en las principales campañas de spam de malware, 2016.



La gran mayoría (89%) de las principales campañas analizadas de spam de malware tenía líneas de asunto en inglés. El alemán fue de lejos el segundo lugar, con un 3%, y pequeños porcentajes de correos electrónicos en francés, noruego, portugués y español. Curiosamente, los grupos de ataque adoptaron tácticas similares, más allá del idioma, con muchas campañas en idiomas diferentes del inglés que también emplearon un tema financiero. Por ejemplo, la palabra clave más utilizada en las campañas alemanas fue "Rechnung", la palabra alemana para Factura.

Ingeniería social y nuevas plataformas de mensajería

A medida que las empresas y los consumidores migran hacia nuevas plataformas de mensajería además del correo electrónico, los invasores probablemente intentarán aprovechar esas plataformas para fines maliciosos.

Cada vez más las empresas usan herramientas colaborativas, tales como Slack, tanto para la comunicación interna como para la interacción con su cliente. En China, WeChat ha dominado el mercado de mensajería, donde ofrece recursos extensivos, incluso un sistema de pago. Donde las transacciones financieras van, los cibercriminales van atrás. WeChat probablemente servirá como un modelo para otras aplicaciones de mensajería. Facebook Messenger ya aumentó su atención en el uso de bots automatizados para permitir que las marcas consigan interactuar en las conversaciones de usuarios.

A pesar de que algunas de las técnicas usadas en correos electrónicos maliciosos típicos no sean transferibles hacia otras plataformas de mensajerías, el fundamento de las campañas de correo electrónico es el uso de la ingeniería social. Las lecciones aprendidas con el éxito de fraudes y las campañas de correo electrónico posiblemente se aplicarán a las plataformas de mensajería, a medida que se adopten de forma más amplia por las empresas y los consumidores.

Lectura adicional

- Dridex: Troyano financiero distribuido de forma agresiva a diario en millones de correos electrónicos de spam
- Ransomware Locky en la caza agresiva por víctimas
- Locky, Dridex y Angler entre los grupos de cibercrimen que enfrentan reducción en sus actividades
- Gran aumento de ataques de correo electrónico usando adjuntos WSF maliciosos
- Necurs: La botnet de envío de correo electrónico masivo retorna con nueva ola de campañas de spam

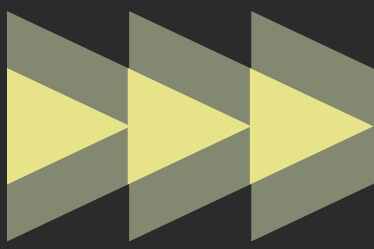
Mejores prácticas

- Una completa solución de protección ayuda a defenderse contra las amenazas enviadas por correo electrónico. La solución Symantec Email Security.cloud puede bloquear las amenazas generadas por correo electrónico y Symantec Endpoint Protection puede bloquear el malware en los endpoints.
- Excluya cualquier correo electrónico de apariencia sospechosa que reciba, especialmente si incluyen enlaces o adjuntos.
- Desconfíe de cualquier adjunto de correo electrónico del Microsoft Office que aconseje a habilitar macros para exhibir su contenido. A menos de que esté absolutamente seguro de que este es un correo electrónico genuino de una fuente confiable, no active macros y, en vez de eso, excluya inmediatamente el correo electrónico.
- Mantenga siempre actualizado su software de seguridad a fin de protegerse contra cualquier nueva variante de malware.
- Mantenga su sistema operativo y otros softwares actualizados. Las actualizaciones de software incluirán frecuentemente parches para vulnerabilidades de seguridad recientemente descubiertas que podrían ser explotadas por grupos de ataque.
- Desconfíe de los correos electrónicos que exigen alguna acción diferente de los procedimientos comunes.
- Elabore su respuesta con el correo electrónico del supuesto remitente obtenido directamente de la lista corporativa de contactos, en lugar de simplemente hacer clic en el botón Responder, para garantizar que se eliminen los estafadores de las respuestas.
- No responda los correos electrónicos sospechosos y no suministre información confidencial.
- Reporte los correos electrónicos sospechosos u obviamente falsos a las autoridades competentes.
- Imponga una política eficaz de contraseñas a todos sus funcionarios para garantizar que las contraseñas sean fuertes y alteradas regularmente.
- Nunca use enlaces en un correo electrónico para conectarse a un sitio web, a menos de que esté seguro de su genuidad. Digite direcciones URL directamente en la barra de direcciones para garantizar que se conecte a un sitio web legítimo y no a uno con una dirección que simplemente parezca similar.

Ataques web, toolkits y explotación de vulnerabilidades online

Sección

05



Symantec

Introducción

En 2016 se produjo un cambio marcante en el panorama de ciberseguridad, debido a que hubo una reducción de casi un 33% en los ataques web en relación al año pasado. El cambio involucró la transición del uso de kits de exploits como vector primario de invasiones para correos electrónicos, que ahora es el método más usado por los delincuentes para entregar amenazas. Esto es un gran contraste en relación a 2015, cuando el número de ataques web duplicó en relación al año anterior.

Sin embargio, esa migración de kits de exploits al correo electrónico puede que no sea permanente. Los delincuentes alternan regularmente entre el correo electrónico y los kits de exploits y es posible que continúen haciéndolo.

Principales conclusiones

- Los ataques Web cayeron un tercio (32%) en relación al año pasado. Sin embargo, los ataques web todavía son un gran problema, con un promedio de más de 229.000 ataques detectados todos los días en 2016. Más de tres cuartos (76%) de los sitios web verificados en 2016 contenían vulnerabilidades, de las cuales un 9% fueron consideradas críticas.
- La actividad maliciosa de los kits de exploits cayó un 60% en 2016, con nuestra investigación indicando que los delincuentes ahora favorecen el correo electrónico como un vector primario para invasiones. La reducción en los kits de exploits es significativa, pero no representa necesariamente que la amenaza de los delincuentes está disminuyendo, apenas que están empleando métodos diferentes para distribuir las amenazas.
- El kit de exploit RIG fue el más activo a fines de 2016. Fue responsable del 35% de todos los ataques web en diciembre, distribuyendo principalmente Ransom.Cerber.
- En promedio, 2,4 vulnerabilidades en navegadores se descubrieron a cada día en 2016, una ligera caída en comparación con 2015, cuando aproximadamente tres vulnerabilidades en navegadores eran descubiertas todos los días.

Tendencias y análisis

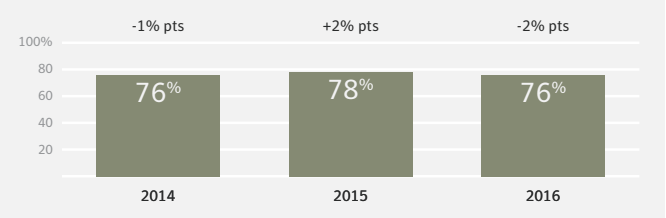
A pesar de que ha caído el número de ataques web y kits de exploits, el porcentaje de sitios verificados que contenían vulnerabilidades permaneció en el mismo nivel alto de los últimos años.

Evaluación de vulnerabilidades

Nuestros datos revelaron que el 76% de los sitios verificados contenían vulnerabilidades - el mismo porcentaje de 2014 y apenas un 2% menos que en 2015.

Sitios web escaneados con vulnerabilidades

El 76% de los sitios verificados fueron encontrados con vulnerabilidades en 2016, una caída de un 2% en relación a 2015.

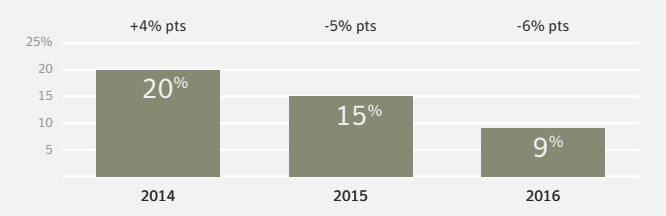


Las vulnerabilidades críticas cayeron un 6% en relación al año pasado. Las vulnerabilidades críticas fueron encontradas en un 9% de los sitios verificados. Eso comparado al 20% en 2014 y al 15% en 2015, mostrando una tendencia de constante descenso en el número de sitios con vulnerabilidades críticas.

Una vulnerabilidad crítica es aquella que, si es explotada por los delincuentes, puede permitir que el código malicioso sea ejecutado sin la interacción del usuario, potencialmente resultando en una violación de datos y mayor riesgo de los visitantes a los sitios afectados.

Porcentaje de vulnerabilidades que eran críticas

El porcentaje de vulnerabilidades encontradas y consideradas críticas cayó constantemente en los últimos tres años y está ahora en un 9%.



Kits de Exploit

Sin lugar a dudas, el mayor destaque para las amenazas web en 2016 fue la caída fenomenal en la actividad de kits de exploits. La detección de kits de exploits cayó un 60%, con algunas de las familias de kits de exploits más importantes desapareciendo durante el año.

Existen algunas razones que justifican esa caída en la cifra de detección de kits de exploits. Como fue mencionado anteriormente y discutido en profundidad en el capítulo Correo Electrónico: malware, spam & phishing, nuestros datos indican que a lo largo de 2016 el correo electrónico se tornó el vector de invasión favorito para los atacantes. La tasa de malware de correo electrónico aumentó en 2016, de 1 de cada 220 correos electrónicos para 1 de cada 131 correos electrónicos.

El desaparecimiento de muchas familias de kits de exploits a lo largo del año también puede observarse, como muestra el análisis de nuestros datos mensuales.

El mayor porcentaje detectado de kits de exploits en 2016, como en 2015, no posee clasificación. Esta categoría está compuesta por muchos kits de exploits diferentes, pequeños y no relacionados, que no se encuadran en la definición de una familia de kit de exploit conocida.

El kit de exploit Angler continuó siendo la familia de kit de exploit más detectada en 2016, dominando la primera mitad del año y respondiendo por más del 50% de toda la actividad de kits de exploits en mayo. Sin embargo, la actividad de Angler cayó alrededor del 30% en junio y siguió cayendo hacia niveles casi inexistentes hasta el fin del año.

Esa caída acentuada en la actividad de Angler coincidió con el arresto de 50 personas en Rusia, acusadas de participación con el grupo de fraude bancario Lurk, y se especula que esa prisión fue la razón para el desaparecimiento de este kit de exploit anteriormente dominante. Para más información, vea el estudio de caso más adelante en este capítulo.

El desaparecimiento de Angler llevó a un pico de actividad del kit de exploit Neutrino en los meses siguientes, con el aumento del 10% en sus actividades en junio, inmediatamente tras la caída en la actividad de Angler. Sin embargo, a fin de año, los niveles de actividad de Neutrino fueron en gran parte idénticos a los registados en el inicio del año.

Nuclear y Spartan son otros dos toolkits que básicamente desaparecieron en 2016. Se estima que una revelación sobre el kit de exploit Nuclear que explicó mucho acerca de su funcionamiento, es el factor responsable de su desaparecimiento. No obstante, el desaparecimiento de Spartan parece ser simplemente un caso de un ciberdelincuente o delincuentes responsables del mismo, decidiendo "jubilar" el kit de exploit. La telemetría de Symantec muestra que Spartan estuvo extremadamente activo hasta el fin de marzo de 2016, razón por la cual aparece en el top 10 del año, pero después desaparece.

El desaparecimiento de tantos kits de exploits de destaque puede demostrar que no son más vistos como una opción confiable. Los cibercriminales pueden no querer comprar un "kit de exploit como servicio" por miedo de que el kit de exploit podría simplemente desaparecer de circulación al cabo de un mes.

Hubo un aumento en la actividad del kit de exploit RIG en el último trimestre del año, lo que posiblemente está relacionado con el desaparecimiento de tantas otras familias de kits de exploits de destaque. El kit de exploit RIG fue el más activo en el final de 2016, y responsable de 35% de todos los ataques en diciembre. Estos ataques distribuyeron principalmente el ransomware Ransom.Cerber.

Los 10 principales kits de exploit

El kit de exploit Angler fue el más usado en 2016, y respondió por el 22% de todos los ataques web con uso de kits de exploits. No obstante, la actividad del Angler cayó alrededor de un 30% en junio y continuó cayendo a niveles casi inexistentes en el final del año. El kit de exploit RIG fue el más activo en el final de 2016, y responsable del 35% de todos los ataques en diciembre.

Clasif.	Kit de Exploit	2015 (%)	2016 (%)	Diferencia de Porcentaje
1	Sin clasificación	38,9	37,9	-1,0
2	Angler	13,3	22,2	8,9
3	Spartan	7,3	11,9	4,6
4	RIG	2,0	7,9	5,9
5	Magnitude	1,1	5,8	4,7
6	Neutrino	1,3	5,8	4,5
7	VIP	24,8	3,2	-21,6
8	Nuclear	4,0	1,6	-2,4
9	Fiesta	2,5	1,0	-1,5
10	G01 Pack	2,2	0,8	-1,4

Ataques web

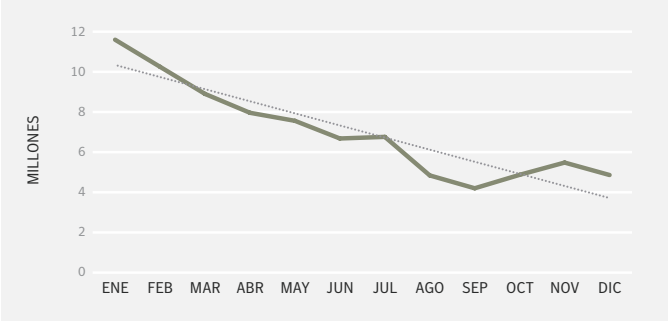
En general, los ataques Web cayeron más del 30% entre 2015 y 2016. Esta caída puede explicarse por los atacantes que usaron el correo electrónico como vector primario de invasión. Como fue mencionado anteriormente, el correo electrónico ofrece una forma más fácil para que los atacantes distribuyan malware y, actualmente, también es más confiable. Los kits de exploit exigen mantener una infraestructura de back-end y son simplemente más trabajosos para los grupos de ataque que enviar un correo electrónico.

No obstante, vale la pena recordar que las amenazas no han disminuido, sino que los grupos de ataque simplemente usan tácticas diferentes para distribuir las amenazas.

La telemetría de Symantec muestra que la caída en las amenazas web fue casi continua en los 12 meses de 2016. Alcanzaron su nivel más bajo en septiembre, aumentando ligeramente en octubre y noviembre, antes de caer nuevamente en diciembre.

Ataques web bloqueados por mes

El número de ataques web por sistema único cayó de forma constante durante 2016.



A pesar de esta caída general en la actividad de amenazas web, todavía representan una gran amenaza, con Symantec bloqueando un promedio de más de 229.000 ataques web en computadoras en los endpoints todos los días en 2016. Los datos de los productos de gateway de Blue Coat que operan en el nivel de red muestran que, en el final de 2016, la cifra de amenazas web bloqueadas en el gateway creció un 24% en relación al mismo período de 2015. Sin embargo, la tasa de aumento es baja, cuando se compara a un crecimiento de 124% de 2014 a 2015.

Los sitios web relacionados a tecnología y negocios fueron las categorías más explotadas en 2016. Los sitios de tecnología fueron explotados casi el doble que los sitios de negocios. Consulta, que fue la tercera categoría más explotada en 2015, cayó del top 10 en 2016.

Clasificación de los sitios web explotados con más frecuencia

En 2016, los sitios relacionados con negocios y tecnología fueron los más populares para el alojamiento de contenido malicioso y malvertising.

Clasif.	Categorías de Dominio	2015 (%)	2016 (%)	Diferencia de Porcentaje
1	Tecnología	23,2	20,7	-2,5
2	Negocios	8,1	11,3	3,2
3	Blogs	7,0	8,6	1,6
4	Alojamiento	0,6	7,2	6,6
5	Salud	1,9	5,7	3,8
6	Compras	2,4	4,2	1,8
7	Educativo	4,0	4,1	< 0,1
8	Entretenimiento	2,6	4,0	1,4
9	Viajes	1,5	3,6	2,1
10	Apuestas	0,6	2,8	2,2

Vulnerabilidades del navegador

En 2016, en promedio, se descubrieron por día 2,4 vulnerabilidades en navegadores. El número de vulnerabilidades en navegadores públicamente anunciadas cayó durante el año, con Microsoft Internet Explorer/Edge enfrentando la mayor caída en el volumen de vulnerabilidades. Eso puede ser explicado por el hecho de que no hubo ninguna nueva versión de Explorer lanzada en 2016, con Microsoft básicamente encerrando su desarrollo. El uso del navegador Explorer también decayó durante el año. El nuevo navegador de Microsoft, Edge, está disponible apenas para las personas que usan Windows 10, y su nueva arquitectura de seguridad dificulta explotaciones de éxito.

La cifra de vulnerabilidades en Firefox y Safari también cayó, mientras Symantec midió un ligero aumento en la cifra de vulnerabilidades de Google Chrome. Sin embargo, una cifra extrañamente alta de vulnerabilidades en navegadores fue descubierta en 2015, parcialmente debido al gran número de vulnerabilidades de día cero descubiertas en el mismo año. En 2016, la cifra de vulnerabilidades en navegadores simplemente retornaron a niveles más “normales”, sin embargo aún están bastante elevadas.

Estudio de caso

Angler: La ascensión y caída de un kit de exploit

El kit de exploit Angler apareció por primera vez en el panorama de amenazas en el final de 2013, tras el desaparecimiento del kit de exploit Blackhole en octubre de ese año. Inmediatamente se volvió bastante popular, pero realmente se destacó en 2015, cuando dominó el panorama de kits de exploits.

Angler era un kit de exploit sofisticado, pionero en muchos avances técnicos que otros kits de exploits siguieron, como el uso de medidas contra soluciones de ciberseguridad. Angler era capaz de bajar y ejecutar malware a partir de la memoria, sin la necesidad de grabar ningún archivo en el disco, en un intento de evadir la detección por tecnologías tradicionales de seguridad. También fue muy rápido en la integración de nuevos exploits de día cero en su arsenal, lo que explicaría su crecimiento en popularidad en 2015. En 2015 se descubrieron varias vulnerabilidades de día cero, incluso algunas en el Adobe Flash Player, que fue un blanco común de Angler.

Una de las grandes ventajas de Angler en relación a otros kits de exploits era la posibilidad de evitar varias medidas tradicionales de seguridad. Usaba una serie de técnicas para evadir la detección, incluyendo el cambio de nombres de host y números de IP rápidamente, y también usaba la técnica de domain shadowing, registrando nombres de dominio que parecían pertenecer a sitios legítimos, para camuflarse en dominios legítimos.

Angler fue uno de los kits de exploits más activos en 2015. El sistema de protección contra invasiones de Symantec bloqueó cientos de miles de ataques realizados por Angler diariamente. El número total de bloqueos de ataques basados en Angler totalizó más de 19,5 millones apenas en 2015. El mecanismo primario de entrega usado por Angler eran malvertisements, y explotaba principalmente vulnerabilidades del Adobe Flash. Las computadoras que ejecutaban Windows, particularmente Windows 7, eran sus blancos de ataque favoritos.

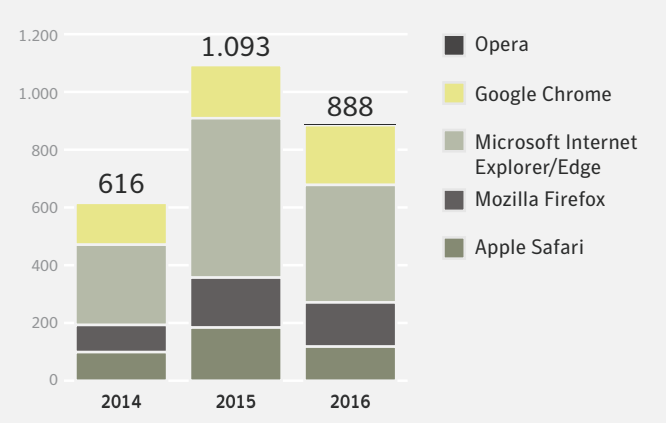
Angler fue usado primeramente para propagar ransomware. Su desaparecimiento en junio de 2016 coincidió con un declinio en las detecciones de ransomware CryptXXX (Ransom.CryptXXX), que fue distribuido principalmente a través de Angler.

Angler sufrió un descenso en su actividad a inicios de 2016, pero aumentó nuevamente de forma rápida, antes de desaparecer completamente en junio. Su desaparecimiento se produjo tras el arresto de 50 personas por autoridades en Rusia, supuestamente asociadas al grupo de fraude bancario Lurk. Se estima que esas detencionesson la razón por tras del desaparecimiento de Angler.

El desaparecimiento de un kit de exploit tan dominante anteriormente dejó una especie de laguna en el mercado, que fue temporalmente ocupado por un aumento en la actividad del kit de exploit Neutrino. Seguramente, los cibercriminales encontrarán una forma de llenar ese espacio en poco tiempo.

Vulnerabilidades del navegador

La cifra de vulnerabilidades descubiertas en navegadores cayó de 1.093 en 2015 para 888 en 2016.



Otra posible razón responsable de la caída en las vulnerabilidades en navegadores es que debido al aumento del número de programas de recompensas de bugs y a la creciente participación de investigadores de seguridad en los mismos, muchas vulnerabilidades en navegadores fueron descubiertas y corregidas en años anteriores y los bugs más accesibles que podrían haber sido explotados por grupos maliciosos no están más disponibles.

Lectura adicional

- Locky, Dridex y Angler entre los grupos de cibercrimen que enfrentan reducción en sus actividades.

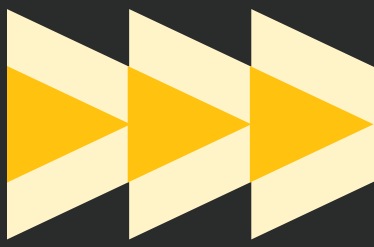
Mejores prácticas

- Examine regularmente su sitio web por vulnerabilidades y malware.
- Escanee su sitio web diariamente por malware.
- Defina la opción de seguridad para todos los cookies de sesión.
- Proteja sus sitios web contra ataques man-in-the-middle (MITM) e infección de malware.
- Escoja Certificados SSL con Extended Validation que muestre la barra de direcciones verde del navegador para los usuarios del sitio.
- Muestre marcas de confianza conocidas en locales altamente visibles en su sitio web.
- Sea exigente con sus plugins. El software que usted usa para administrar su sitio viene también con vulnerabilidades. Cuanto mayor es el número de software de terceros que usted usa, más grande es la superficie de ataque, entonces solamente implemente lo que sea absolutamente necesario.

Cibercrimen y la economía clandestina

Sección

06



Symantec

Introducción

En 2016, surgieron dos lados diferentes del cibercrimen. Los tradicionales grupos de ciberdelito para mercados de masa realizaron campañas de correo electrónico en gran escala con el objetivo de distribuir malware como "commodity", por ejemplo, ransomware y las amenazas enfocadas en la banca online. Si bien sus motivaciones y cargas útiles permanecieron básicamente las mismas, sus métodos de distribución cambiaron de kits de exploits basados en la web para métodos más tradicionales, especialmente el uso de archivos adjuntos de correo electrónico.

El otro lado del cibercrimen está constituido por grupos de delincuentes organizados, responsables de una serie de sofisticados asaltos financieros. Sin embargo, no fueron apenas los delincuentes profesionales que dirigieron esas campañas - también hubo evidencias de participación de naciones.

Tanto los grupos de cibercrimen para mercados de masa como los con blancos dirigidos, han adoptado técnicas con uso de "herramientas del día a día". Esa tendencia, conforme es discutido en el capítulo de Ataques dirigidos, muestra que los atacantes aprovechan el sistema operativo y los recursos de aplicaciones, junto con las herramientas públicamente disponibles, en lugar de explotar vulnerabilidades y desarrollar herramientas personalizadas.

Principales conclusiones

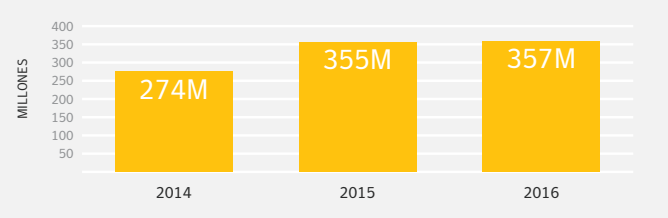
- En 2016, los cibercriminales aumentaron su popularidad, con víctimas de destaque y recompensas financieras nunca vistas antes. Los ataques Banswift (Trojan.Banswift) fueron también la primera vez en la que se encontraron fuertes indicios de la participación de naciones en ciberdelitos financieros.
- El cibercrimen para los mercados de masa continúa con fuerza, a pesar de los esfuerzos para interrumpir las actividades de estos grupos. Los atacantes adaptaron sus métodos para la distribución tradicional de malware en ciberdelitos. En particular, el uso de downloaders JavaScript y archivos ejecutables de macro maliciosos en archivos del Office fue difundido y responsable por poco más de 7 millones de intentos de invasiones en 2016.
- Si bien en 2016 la cifra de violaciones de datos se mantuvo estable en comparación a 2015, la cifra de identidades robadas aumentó significativamente. Casi 1.100 millones de identidades fueron robadas en 2016, un gran aumento si comparamos esa cifra con las 563,8 millones de identidades robadas en 2015.
- Se observaron casi 100 millones de bots en 2016, un aumento de un 7% en relación a 2015.

Malware

El malware continúa siendo una plaga sobre el panorama de amenazas, con más de 357 millones de nuevas variantes observadas en 2016. Sin embargo, por primera vez, la tasa de nuevas instancias de malware vistas en endpoints se mantuvo prácticamente estancada en 2016 - un aumento de un 0,5%.

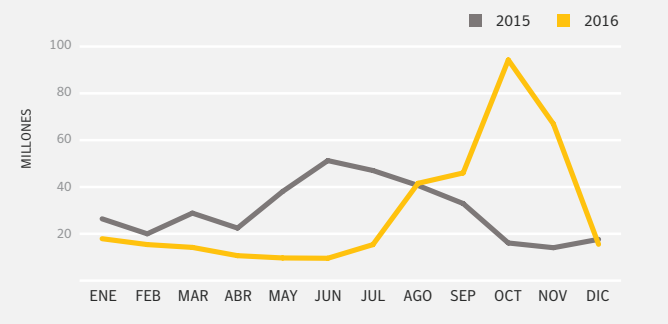
Variantes únicas de malware detectadas por primera vez

Hubo un ligero (0,5%) aumento entre 2015 y 2016 en la cifra de variantes de malware únicas detectadas por primera vez.



Cálculo mensual de variantes únicas de malware vistas por primera vez en 2016

En este cálculo mensual de variantes de malware únicas vistas por primera vez en 2016, pudo observarse en octubre un claro aumento.

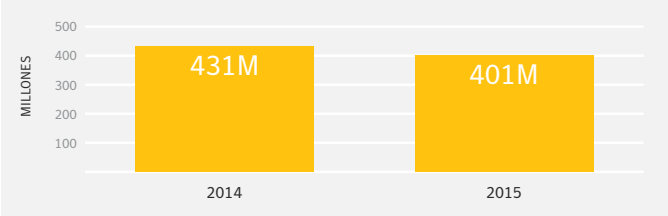


A pesar de que la tasa de nuevas variantes de malware quedó estable en el inicio de 2016, el segundo semestre vio una explosión de nuevas variantes. Principalmente hubo influencia del elevado volumen de downloaders de ransomware distribuidos por correo electrónico por botnet Necurs (Backdoor.Necurs), que será discutido con más detalles en este capítulo.

En informes anteriores, Symantec siguió un abordaje un poco diferente para contar las variantes de malware, enfocando en variantes exclusivas en aquel año, en lugar de malware visto por primera vez en el mismo período de tiempo. Usando esta metodología en 2016 que considera el legado, los datos reflejan un volumen ligeramente mayor de variantes, pero una caída de 7% de nuevas variantes en el año.

Variantes únicas de malware detectadas

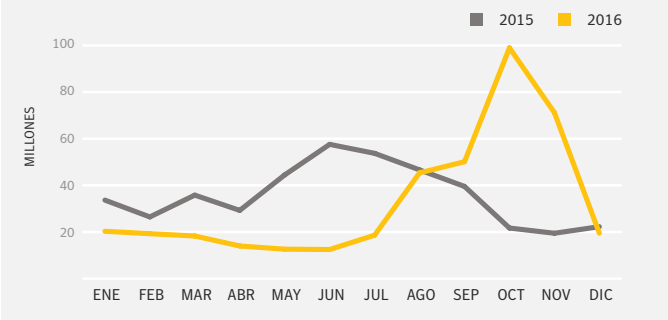
Hubo una ligera caída entre 2015 y 2016 en la cifra de variantes únicas de malware detectadas.



El análisis de los datos a cada mes muestra una tendencia casi idéntica con un aumento considerable en variantes en el fin del año.

Cálculo mensual de variantes únicas de malware en 2016

El cálculo de variantes únicas de malware también muestra un aumento en octubre.



Al analizar esos datos aisladamente, puede parecer que el problema de malware se está estabilizando o incluso mejorando; sin embargo, en un análisis más amplio, queda claro que este no es el caso. Muchos ataques son bloqueados en el inicio de la cadena de ataque y no se representan en la cifra de volumen de malware, que enfoca principalmente en las cargas útiles finales o cerca del final. Como fue discutido en el capítulo que trataba de correos electrónicos, el correo electrónico fue responsable de un gran volumen de malware distribuido en 2016. Symantec también continuó bloqueando un gran número de ataques web. Esto lleva a menos cargas útiles finales entregadas y, por lo tanto, a un número total más bajo de variantes vistas.

Otras explicaciones incluyen una menor incidencia de amenazas polimórficas y una menor dependencia de los grupos de ataque de malware para distribuir sus obras. Ese es un fenómeno que llamamos de "uso de herramientas del día a día".

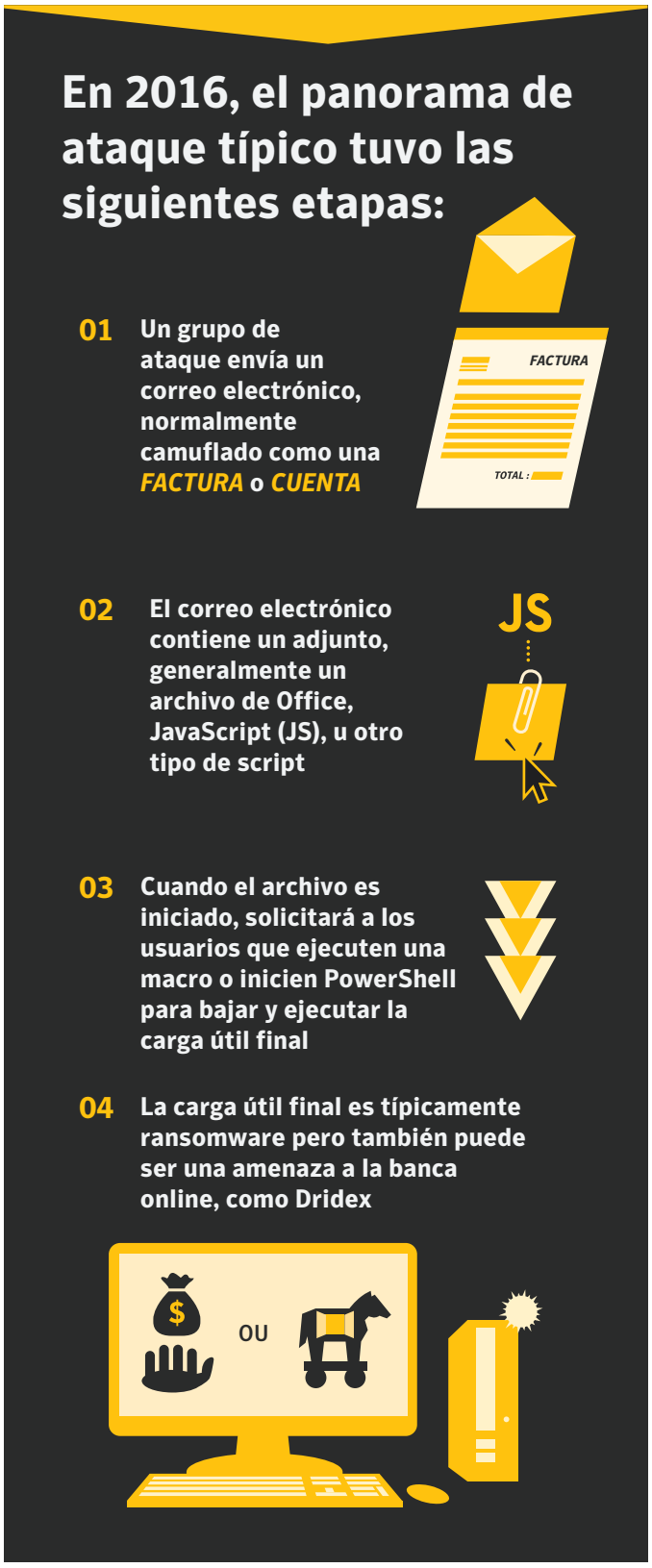
Uso de herramientas del día a día: PowerShell, macros e ingeniería social

Una tendencia surgió en 2016 donde los atacantes emplean programas legítimos del Windows para descargar y ejecutar cargas útiles. Esta táctica del "uso de herramientas del día a día" es discutida con más detalles en el capítulo sobre Ataques dirigidos; sin embargo, las técnicas usadas por los grupos de ataques avanzados también son vistas en el mundo de la cibercrimen.

PowerShell, un poderoso lenguaje de script y shell de línea de comando, se tornó un pilar de la cadena de invasiones y agrada a los grupos de ataques por varios motivos. Se instala de forma estándar en la mayoría de las computadoras Windows, y la mayoría de las organizaciones no tienen el registro extendido activado para el mismo, haciendo que las actividades maliciosas de PowerShell permanezcan invisibles en gran parte. Scripts también pueden ser fácilmente ofuscados, lo que esconde sus intenciones maliciosas. Esto permite que las cargas se ejecuten directamente de la memoria, lo que significa que los grupos de ataque dejan menos rastros.

Un análisis de Symantec en el fin de 2016 mostró que el 95,4% de los scripts de PowerShell inspeccionados eran maliciosos. Scripts maliciosos de PowerShell son utilizados principalmente como archivos ejecutables durante la fase inicial de invasion, pero también pueden usarse para el desplazamiento lateral a través de una red. Este desplazamiento lateral es normalmente visto en ataques dirigidos para permitir que una amenaza ejecute código en una computadora remota al propagarse dentro de la red. En el caso de ataques de cibercriminales, PowerShell es usado para facilitar la descarga y ejecución de la carga útil final.

El uso del PowerShell aumentó bruscamente en 2016. Sandbox de análisis de malware de Blue Coat recibió 22 veces más muestras usando PowerShell en el tercer trimestre de 2016 en comparación con el segundo trimestre. Esto se produjo probablemente debido al aumento de la actividad asociada con downloaders JavaScript y Trojan.Kotver durante este período. En general, el análisis identificó que PowerShell fue usado más frecuentemente con W97M.Downloader (9,4% de muestras), seguido por Kovter (Trojan.Kotver) con 4,5%, y JS.Downloader (4%). Kovter es conocido por su uso de PowerShell por crear una infección sin el uso de archivos, contenido totalmente en el registro.



Los cibercriminales más avanzados, con ataques dirigidos, también aprovecharon PowerShell en 2016. El grupo Odinaff usó scripts maliciosos de PowerShell para atacar a las organizaciones financieras. Estos ataques son discutidos más adelante en este capítulo.

Los macros maliciosos del Office siguen populares entre los grupos de ataques, conforme evidenciado por la prevalencia de detecciones (discutido abajo). Los macros del Office no funcionan por estándar, entonces estos ataques dependen de ingeniería social para convencer a los usuarios a iniciar el macro al abrir un archivo adjunto del Office. Al usar recursos como PowerShell y macros, los grupos de ataque no necesitan depender de exploits de software o herramientas personalizadas que son más propensas a levantar sospechas, además de exigir más tiempo y habilidad para su uso.

También existen ataques que no dependen de cualquier código malicioso o recursos de sistemas. Los ataques BEC (Business Email Compromise), discutidos en detalle en el capítulo sobre correo electrónico, dependen exclusivamente de ingeniería social para engañar a las víctimas a entregar grandes sumas de dinero.

Si bien esta tendencia muestra un movimiento diferente del uso de exploits y herramientas personalizadas, es importante notar que existe un componente de malwares en casi todos los ataques. Esto representa que el malware continuará a persistir como un problema. Asimismo, este cambio no significa que los atacantes están tornándose menos sofisticados. En realidad, demuestra un aumento de la eficiencia y la capacidad de esconderse en áreas visibles.

Incidencia y tendencias de malware

Detecções genéricas dominaram a lista de malware mais prevalente detectado em endpoints em 2016.

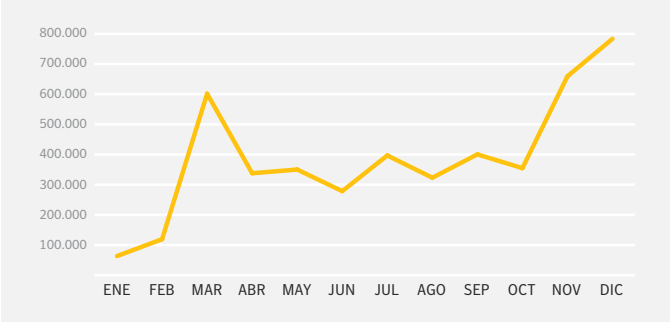
Clasif.	Detección	Número de infecciones
1	Heur.AdvML.B	5.648.434
2	JS.Downloader	3.487.119
3	Packed.Dromedan!Ink	2.615.857
4	W97M.Downloader	2.199.083
5	Heur.AdvML.C	2.039.212
6	SMG.Heur!cg1	1.291.550
7	W32.SillyFDC	1.019.644
8	Trojan.Startpage	908.429
9	W32.Downadup.B	814.687
10	Infostealer	753.783

Al analizar los destaques de malware más frecuentes, es notable el impacto de las detecciones de malware genérico o heurístico. Son responsables de 9 de cada 10 principales tipos de malware detectados en endpoints en 2016. Sin embargo, es importante notar la relevancia del JS.Downloader y W97M. Downloader, que son nuevas entradas en la lista de destaques de 2016.

En 2016, Symantec observó un gran número de campañas de correo electrónico que distribuían ransomware y amenazas para banca online vía macro malicioso del Office (W97M. Downloader y variantes) y archivos de downloader JavaScript (JS.Downloader y variantes). En 2016, fueron responsables de 7 millones de detecciones y han dominado el panorama de amenazas de cibercrimen, especialmente en el segundo semestre del año.

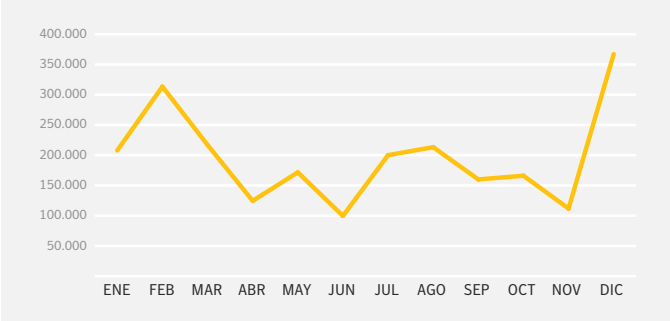
Detecciones de archivos ejecutables de JavaScript por mes

En el segundo semestre de 2016 aumentaron las detecciones de archivos ejecutables de JavaScript (JS.Downloader y variantes).



Detecciones de archivos ejecutables de macros de Office por mes

En diciembre de 2016 hubo un aumento en las detecciones de macro del Office (W97M.Downlader y variantes).



Los grupos de ataques prefieren estos archivos ejecutables por una serie de motivos. Las empresas normalmente no bloquean todos los archivos del Office en el gateway de correo electrónico, ya que podría afectar a los correos electrónicos, lo que explica la popularidad de los archivos ejecutables de macros del Office. Mientras tanto, la facilidad de ofuscar un intento de evitar la detección ha contribuido para el aumento de archivos de JavaScript. Como discutido anteriormente, JS.Downloader típicamente utilizará PowerShell o un Visual Basic Script (VBS) para ejecutar la carga útil final en un intento de pasar desapercibido.

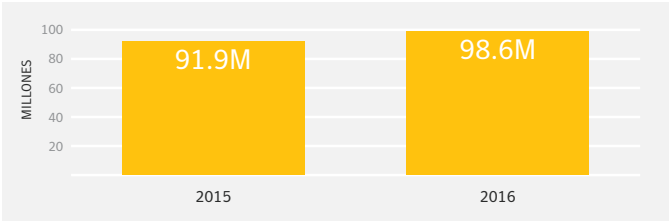
Investigaciones de Symantec indican que algunos grupos favorecen W97M. Downloader, mientras otros prefieren JS.Downloader. Las actividades relacionadas al W97M. Downloader cayeron en el segundo semestre de 2016, pero Symantec estima que los grupos que lo usan pueden aumentar nuevamente la actividad. En realidad, en el último mes de 2016 se observó un aumento en las detecciones de W97M. Downloader.

Muchas de esas amenazas se están propagando principalmente por botnets de spam.

Symantec observó en 2016 un aumento en el número de bots. La cifra saltó de 91,9 millones para 98,6 millones de bots, incluyendo varios botnets.

Cifra de actividad de Bots

A Symantec observou 6,7 milhões a mais de bots em 2016 em relação a 2015.



Algunas instancias de malware tomaron más precauciones, para ser aun más furtivas. El 20% del malware ahora es capaz de detectar e identificar de forma rutinaria la presencia de un entorno de máquina virtual, un aumento del 16% comparado a 2015.

Sandbox de análisis de malware de Blue Coat rastreó un aumento de la utilización del protocolo SSL para la comunicación con servidores de comando y control (C&C), tornando más difícil la inspección del tráfico de red. Tal comportamiento aumentó el 79%, llegando a 3,1% al fin de 2016. Esto posiblemente sucedió debido a la mayor disponibilidad de certificados SSL en 2016, y los grupos de ataque percibieron que tenían una posibilidad mayor de pasar a través del gateway sin ser detectados si usasen el cifrado SSL. Asimismo, la comunicación para servicios en la nube duplicó para más de 4% en 2016.

Un 1% de todas las amenazas usó la red Tor. En esos casos, fue usado principalmente por ransomware para entregar las instrucciones de pago.

Estudio de caso de Botnet: Necurs

La botnet Necurs fue una de los principales distribuidores de malware en 2016 y fue responsable de campañas de correo electrónico masivo para distribución de JavaScript, VBS y archivos ejecutables de macros del Office. La carga útil principal de Necurs en 2016 fue Ransom.Locky. Otras grandes botnets observadas por Symantec se utilizaron para propagar amenazas como Dridex (W32.Cridex), Cerber (Ransom.Cerber), y Kotver (Trojan.Kotver), así como Locky.

Necurs fue una de las botnets más activas en la distribución de malware en 2016. Los operadores responsables de Necurs usaron el período normal de trabajo. Las amenazas se distribuían de lunes a viernes y había poca actividad los fines de semana.

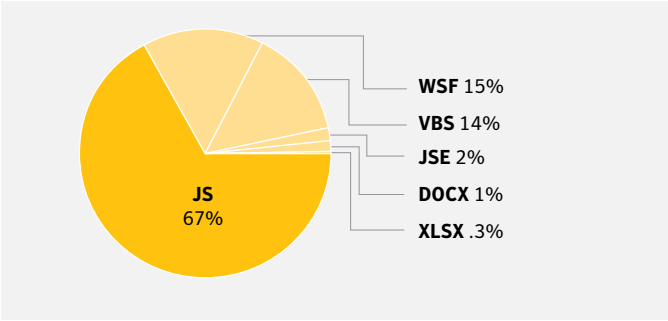
Al analizar apenas un día de actividad de Necurs, queda evidente su capacidad de escala. El 24 de noviembre de 2016, Necurs envió cinco campañas de spam, siendo que dos entregaron archivos JavaScript, dos entregaron adjuntos .wsf, y hubo una entrega de un adjunto VBS. Estas cinco campañas de spam enviaron más de 2,3 millones de correos electrónicos de spam, más de 1,8 millones usaron downloaders JS, mientras que un poco menos de 465.000 usaron VBS.

Una investigación de Symantec sobre las 146 campañas de correo electrónico realizadas por Necurs en el último trimestre del año descubrió que fue responsable del envío de aproximadamente 525 muestras únicas de malware en cada campaña de correo electrónico.

Al analizar las campañas de spam, involucrando principalmente downloaders JS, VBS y WSF, nuestro estudio constató que los archivos JavaScript fueron de lejos el tipo más popular de archivo ejecutable distribuido por Necurs.

Archivos ejecutables entregados por la botnet de spam Necurs

En el período observado por Symantec, Necurs envió predominantemente campañas de spam que contenía JS.Downloader.



Cuando empezó este estudio de Necurs a fines de octubre, las amenazas eran distribuidas principalmente con el uso de VBS, pero en noviembre y diciembre los archivos JavaScript dominaron.

Este uso de diferentes archivos ejecutables indica que Necurs era una "botnet de alquiler", que estaba siendo utilizado por diferentes grupos de ataque.

Curiosamente, Symantec observó la detención de la actividad de Necurs por casi tres meses a partir del final de diciembre. Su última campaña de spam comenzó el 22 de diciembre y terminó el 24 de diciembre. Si bien la primera deducción es que esto se produjo pues el grupo responsable de Necurs hizo una pausa para las vacaciones, la botnet permaneció quieta hasta el 20 marzo de 2017.

El desaparecimiento de Necurs produjo una gran reducción del volumen de correos electrónicos maliciosos enviados en el fin de 2016 e inicio de 2017. El motivo por detrás de su desaparecimiento permanece un misterio. El 20 de marzo, el día de su retorno, Symantec bloqueó casi dos millones de correos electrónicos maliciosos. El hecho de que Necurs logró retomar campañas de spam en masa en su retorno indica que, no importa cual sea el motivo de su ausencia, parece no haber perdido sus capacidades.

Todo está relacionado al dinero: malware financiero

El malware financiero, específicamente las amenazas dirigidas a la banca online, ha sido históricamente un gran conductor del cibercrimen. Sin embargo, una cantidad de detenciones e interrupciones, juntamente con el éxito continuo de ransomware, demuestra que se ha tornado menos dominante.

Los datos de invasiones muestran que esta área está dominada por cinco familias, y la actividad fuera de este top cinco es insignificante.

Los 10 principales troyanos financieros

La lista de los 10 principales troyanos financieros demuestra que un pequeño grupo de troyanos financieros dominaron el panorama en 2016.

Clasif.	Amenazas financeiras	Máquinas afectadas
1	Ramnit	460.673
2	Bebloh	310.086
3	Zbot	292.160
4	Snifula	121.624
5	Cridex	23.127
6	Dyre	4.657
7	Shylock	4.512
8	Pandemiya	3.330
9	Shifu	2.177
10	Spyeye	1.480

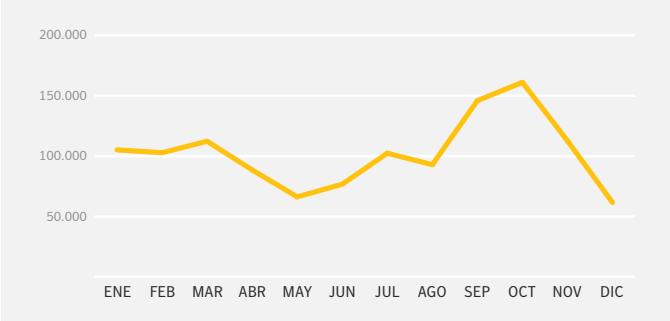
Ramnit (W32.Ramnit) tuvo una vuelta triunfal al mundo del fraude financiero en 2016. Ramnit está en operación desde 2010, pero con la prisión del grupo de cibercriminales responsable de la botnet, en febrero de 2015, asistida por Symantec, se pensaba que las operaciones de la botnet habían concluido. Se estima que la botnet fue compuesta por 350.000 computadoras en el momento de la interrupción de sus actividades. Ramnit desapareció por un tiempo, pero fue observada una nueva variante en diciembre de 2015.

Ramnit pasó a dominar el panorama de los troyanos financieros en 2016 y se detectó en cifras elevadas de forma consistente durante todo el año. Curiosamente, como Ramnit era frecuentemente distribuido a través del kit de exploit Angler en el pasado, no presentó ninguna caída en la actividad tras el desaparecimiento de Angler a mediados del año. Eso indica que sus responsables pueden haber adaptado sus técnicas de infección, y hubo relatos de Ramnit distribuido a través de correo electrónico en el Reino Unido. El hecho de que algunas variantes del Ramnit autorreplican, contribuyó para su predominancia.

En 2016 hubo relatos sobre Bebloh (Trojan.Bebloh), que ocupa el segundo lugar en la lista de los troyanos financieros, iniciando campañas agresivas en Japón, teniendo como victimas a pequeños bancos y cooperativas de crédito. Bebloh también causó un gran pico en la actividad de troyanos financieros en septiembre y octubre. Bebloh formaba parte de la red Avalanche de alojamiento de malware, que fue derribada en 2016, y sintió una caída acentuada en las actividades en noviembre y diciembre.

Actividades de troyanos financieros por mes

La caída en las actividades después de octubre de 2016 refleja el impacto de una serie de interrupciones de servicio de destaque.



El posible hacker responsable del malware bancario Neverquest, que Symantec detecta como Trojan.Snifula, también fue arrestado en enero de 2017. Todos esos factores pueden contribuir con que la lista de los 5 principales troyanos financieros sea muy diferente a fines de 2017.

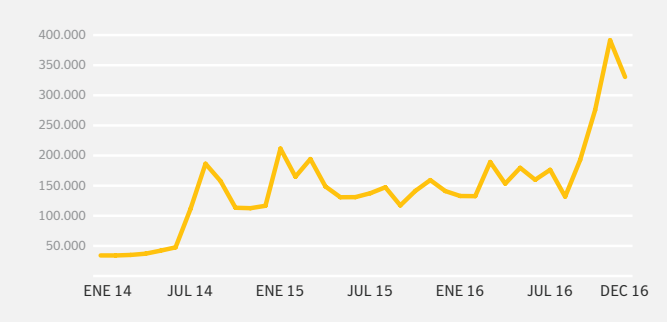
El impacto de las interrupciones, con muchos más detalles más adelante en este capítulo, se refleja en la disminución en el número de infecciones después de octubre de 2016. Caídas significativas en la actividad de Dridex (que dominó el panorama de amenazas en 2015), Dyre y Shylock (Trojan.Shylock) pueden atribuirse a interrupciones.

Incluso Mac

El sistema operativo de Apple, que ya fue visto como casi impenetrable, sintió una cantidad creciente de malware detectado a lo largo de 2016. Un aumento constante en malware detectado en Macs comenzó en septiembre y continuó por el último trimestre del año; una cifra casi tres veces mayor de detecciones de malware se produjo en noviembre de 2016 en comparación con el inicio del año.

Distribución de malware para Mac por mes, 2014-2016

En el segundo semestre de 2016, puede verse claramente el crecimiento en el malware para Mac.



No obstante, esta cifra no refleja necesariamente que los grupos de ataque están centrados cada vez más en el ecosistema Mac.

Un análisis más detallado del malware bloqueado en endpoints OS X, downloaders JavaScript (JS.Downloader) y archivos ejecutables de macro del Office (W97M.Downloader) son dos de los principales vectores de infección, siendo responsable por tres de los cinco primeros. JS.Nemucod, que entrega ransomware Locky, también está en el top 10.

Posiblemente los usuarios de Mac están sufriendo con campañas de correo electrónico para la distribución de las amenazas usando JS.Downloader, W97M.Downloader y JS.Nemucod, en lugar de la posibilidad que los responsables de las amenazas están cada vez más dirigiendo sus ataques a los usuarios de Mac.

Eso también es evidente en un aumento en el malware detectado en Mac en noviembre y diciembre, época en la cual también se produjo un aumento en los incidentes de JS.Downloader y W97M.Downloader.

Las otras detecciones que componen la lista de los cinco primeros, OSX.Malcol y OSX.Malcol.2, son detecciones genéricas que protegen contra troyanos individuales y variados de OS X.

Las 10 principales instancias de malware bloqueadas en los endpoints del OS X en porcentaje de las infecciones totales

JS.Downloader y W97M.Downloader está en la lista de las 5 principales instancias de malware bloqueadas en endpoints OS X en 2016.

Clasif.	Detección	Total de Infecciones (%)
1	OSX.Malcol	6,88
2	JS.Downloader	5,76
3	OSX.Malcol.2	5,73
4	W97M.Downloader	5,11
5	JS.Downloader.D	1,87
6	JS.Nemucod	1,09
7	VBS.Downloader.B	1,04
8	VBS.Downloader.Trojan	0,83
9	Trojan.Malscript	0,59
10	SMG.Heur!cg1	0,57

Odinaff and Banswift: El año del asalto financiero dirigido

Si bien el panorama de amenazas de cibercrimen normalmente es dominado por ataques masivos indiscriminados, 2016 vio el surgimiento o resurgimiento de grupos de cibercrimen más sofisticados y de elite. Mientras que el cibercrimen tradicional tiene un abordaje más "generalista", los delincuentes de elite usan técnicas normalmente vistas en ataques dirigidos avanzados. Los recursos, paciencia y absoluto coraje necesarios para ejecutar esos ataques, demuestran como el cibercrimen está potencialmente entrando en una nueva era.

El surgimiento de dos grupos que tenían como objetivo el funcionamiento interno del sistema financiero internacional, al tiempo que disminuyeron las amenazas tradicionales a la banca online, refleja como las instituciones financieras están enfrentando un tipo bastante diferente de amenaza en 2017.

Banswift

Uno de los asaltos más osados a bancos ya vistos fue el ciberasalto al Banco Central de Bangladesh a inicio de 2016. Los criminales huyeron sin problemas con US$ 81 millones y si no fuese por un error de digitación y la sospecha de astutos funcionarios del banco, el grupo podría haber robado US$ 1 billón.

Los criminales explotaron debilidades en la seguridad del Banco de Bangladesh para infiltrarse en su sistema y robar sus credenciales SWIFT, permitiéndoles realizar transacciones fraudulentas.

A seguir, los criminales usaron malware para cubrir sus pistas. El malware alteró los mensajes de confirmación de transacciones impresas del Banco de Bangladesh para retrasar el descubrimiento del fraude. Los responsables del ataque llevaron a cabo la acción en el inicio de un fin de semana prolongado en Bangladesh, para reducir aún más la posibilidad de descubrir el robo.

Usando las credenciales SWIFT robadas del Banco de Bangladesh, los criminales efectuaron varias solicitudes de transferencia al Federal Reserve Bank of New York y desde allí el dinero del Banco de Bangladesh fue transferido inicialmente hacia localidades en las Filipinas y Sri Lanka. Cuatro solicitudes de transferencia en el total de US$ 81 millones para entidades en las Filipinas fueron efectuadas con éxito, pero una solicitud para transferir US$ 20 millones hacia una "fundación" sin fines de lucro en Sri Lanka despertó sospechas puesto que el nombre de la fundación estaba escrito de forma incorrecta. Esto llevó a la suspensión de las transferencias y a buscar aclaraciones por el banco en Bangladesh, que descubrió el fraude. Sin embargo, en aquel momento los US$ 81 millones ya habían desaparecido, principalmente en cuentas relacionadas con casinos en las Filipinas.

La mayor parte de los US$ 81 millones aún no ha sido recuperada, sin embargo, US$ 15 millones fueron devueltos por un casino en las Filipinas al Banco Central de Bangladesh en noviembre.

Los métodos empleados en este ataque, especialmente el profundo conocimiento de los sistemas SWIFT y las medidas tomadas para cubrir evidencias, indican que son actores altamente competentes. Este fue un fraude increíblemente osado, y también la primera vez que observamos fuertes indicios de participación de naciones en ciberdelitos financieros. El ataque se atribuyó a responsables en Corea del Norte.

El análisis llevado a cabo por Symantec del malware (Trojan.Banswift) usado en el ataque al banco de Bangladesh encontró evidencias de uso compartido de código entre este malware y las herramientas usadas por el grupo Lazarus - que el FBI afirma tener relación con el gobierno norcoreano. El grupo Lazarus fue asociado con el famoso hack de Sony en 2014, y ha sido asociado a una serie de ataques contra EE.UU. y Corea del Sur desde 2009.

Ese mismo grupo también fue vinculado a otros dos asaltos que tenían como objetivo bancos que hacen transferencias usando la red SWIFT, si bien la red SWIFT no haya sido afectada en ninguno de esos ataques.

El banco vietnamita Tien Phong Bank reveló que había interceptado una transferencia fraudulenta de más de US$ 1 millón en el cuarto trimestre de 2015. Investigación realizada por Symantec también descubrió evidencias de que otro banco fue víctima del mismo grupo en octubre de 2015.

Un tercer banco, el Banco del Austro en Ecuador, también reportó haber perdido US$ 12 millones en ataques usando transacciones fraudulentas SWIFT, a pesar de que ninguna relación definitiva puede realizarse entre aquel fraude y los ataques en Asia.

Symantec estima que el grupo Lazarus puede haber reaparecido en 2017, con nuevos ataques contra instituciones financieras.

Odinaff

Una campaña que contenía Trojan.Odinaff fue descubierta teniendo como objetivo organizaciones financieras globales en 2016. Los ataques que usaron Odinaff eran sofisticados y ejecutados claramente por un grupo profesional de cibercrimen. A pesar de que también tenga como blanco a usuarios del sistema SWIFT, no existen pruebas que vinculen estos ataques con los ataques Banswift.

La investigación de Symantec indica que las campañas que utilizan Odinaff comenzaron en enero de 2016 y fueron enfocadas en organizaciones de los sectores bancario, títulos, trading y nómina de pago. El troyano Odinaff fue típicamente implantado en la primera etapa de un ataque para establecer su posición en la red.

Los ataques que contenían Odinaff fueron altamente sofisticados, exigiendo una gran cantidad de participación directa, con la implantación metódica de una serie de backdoors ligeros y herramientas con objetivos explícitos en computadoras de interés específico.

La implantación más frecuente del troyano fue en documentos que contenían macros maliciosos, siendo que los botnets también fueron usados para implantarlo. Los ataques fueron cuidadosamente administrados, con los responsables de las amenazas manteniendo un perfil discreto en la red de la organización de la víctima, apenas descargando e instalando nuevas herramientas cuando era necesario.

Las herramientas utilizadas en los ataques Odinaff recuerdan el abominable grupo Carbanak, que ha dirigido sus ataques al sector financiero desde 2013.

Las actividades de Carbanak fueron descubiertas a fines de 2014 y se estima que el grupo tiene como blanco de ataque cientos de bancos en varios países. Algunos miembros de la comunidad de ciberseguridad estiman que el grupo puede haber robado hasta US$ 1 billón. Symantec descubrió varios vínculos entre Carbanak y los responsables de los ataques Odinaff, sin embargo, la convergencia de infraestructura es atípica, es decir, Odinaff puede cooperar de una forma libre con Carbanak, o incluso formar parte de una organización más amplia liderada por Carbanak.

Los ataques Odinaff y Banswift demostraron que a pesar de que en 2016 muchos grupos de ataque volvieron al uso de herramientas y técnicas existentes, todavía existen grupos de cibercriminales extremadamente sofisticados que centran su atención en la implantación de campañas avanzadas para obtener grandes recompensas financieras.

Violaciones de datos y la economía clandestina

Violaciones de datos

En los últimos ocho años, más de 7.000 millones de identidades online fueron robadas en violaciones de datos, que es casi lo equivalente al número de personas en el planeta.

En 2016, más de 1.100 millones de identidades fueron robadas en violaciones de datos, casi el doble del número robado en 2015, cuando poco más de 563 millones de identidades fueron robadas. Este aumento se produjo a pesar de una reducción en la cifra de violaciones de datos entre 2015 y 2016, pasando de 1.211 para 1.209.

La cifra promedio de identidades robadas por violación en 2016 saltó para casi 1 millón, el mayor promedio de los últimos tres años.

En 2016, se produjeron 15 megaviolaciones, en las que más de 10 millones de identidades fueron robadas, un aumento comparado a las 11 megaviolaciones en 2014 y 13 en 2015.

Violaciones de datos, 2014-2016

Si bien en 2016 la cifra de violaciones de datos se mantuvo estable, el número de identidades robadas aumentó significativamente.

Año	Violaciones	Identidades robadas	Promedio por violación	Mega-violaciones
2014	1523	1.226.138.929	805.081	11
2015	1211	563.807.647	465.572	13
2016	1209	1.120.172.821	926.528	15

As violações de dados também foram destaque em 2016, principalmente devido a Yahoo. Em setembro, a empresa revelou que uma violação em 2014 comprometeu 500 milhões de suas contas de usuários. Então, em dezembro, a empresa revelou que, em agosto de 2013, mais de 1 bilhão de contas de usuários foram comprometidas, tornando-se a maior violação de dados já reportada.

A companhia disse que acredita que as duas violações estão conectadas e que os ataques são patrocinados por nações. As revelações tiveram sérias implicações para a empresa, que está no meio do processo de venda para a Verizon, e viu o seu valor despencar como resultado destas revelações.

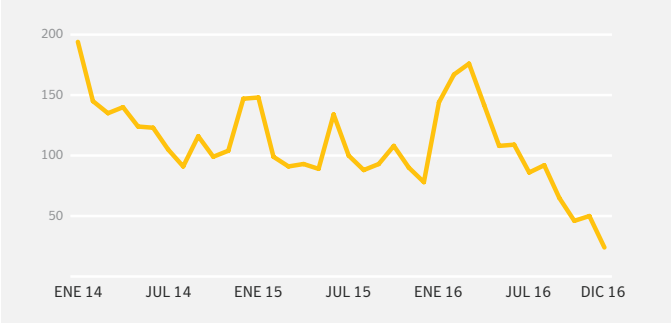
Retrospectiva del año

A pesar de que las noticias de las violaciones de datos en Yahoo fueron reveladas en 2016, no se incluyen en la telemetría de Symantec para el año, pues Symantec registra una violación de datos cuando se produce, en vez de cuando es relatada.

La cifra mensual de violaciones en 2016, fue más elevada en el inicio del año y, a seguir, disminuyó hasta el fin del año. Esta situación es bastante frecuente para violaciones de datos, pues muchas veces existe una laguna entre la ocurrencia de una violación de datos y cuando es reportada, como puede verse claramente en el caso de las violaciones de Yahoo, entonces las violaciones de datos producidas a fines de 2016 pueden aún no haber sido relatadas.

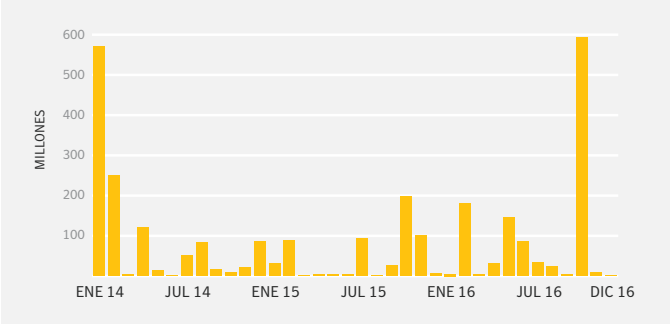
Violaciones de datos por mes, 2014-2016

La cifra mensual de violaciones de datos disminuyó a fines de 2016. Es posible que las violaciones de datos ocurridas en noviembre y diciembre aún no hayan sido relatadas.



Identidades robadas por mes, 2014-2016

Hubo un aumento de identidades robadas en octubre de 2016, que fue en gran parte causado por una violación en Friend Finder Networks.



Si bien la cifra de violaciones de datos se redujo en el fin del año, el número de identidades robadas alcanzó su pico en octubre, subiendo para casi 600 millones. Este aumento puede atribuirse principalmente a una violación de datos de Friend Finder Networks, que expuso la información privada de 412 millones de cuentas de usuarios.

Friend Finder Networks es una compañía de sitios web de pornografía y de cupido para adultos que opera sitios como Adult Friend Finder y Cams.com, así como algunos otros sitios menores. También era responsable del sitio web Penthouse.com, vendido en febrero de 2016. A pesar de la venta, Adult Friend Finder, todavía poseía información almacenada de usuarios del sitio Penthouse.com y, como resultado, también fue expuesta en la violación.

La violacion reveló direcciones de correo electrónico, contraseñas (almacenadas em un simple formato visible o SHA-1 hash), fechas de las últimos visitas, informaciones del navegador, direcciones IP y status de los miembros del sitio. Fue la segunda invasión de la organización en poco más de un año.

Tipos de datos perdidos en violaciones en 2016

Información personalmente identificable aún fue la forma más frecuente del robo de datos en 2016, sin embargo la Información Financiera Personal no quedó muy atrás.

Tipo	2015 (%)	2016 (%)	Diferencia de Porcentaje
Información Personalmente Identificable (PII)	54,5	42,9	-11,6
Información Financiera Personal (PFI)	32,9	39,2	6,3
Otras informaciones	1,6	11,1	9,5
Información Personal de Salud (PHI)	11,0	6,8	-4,2

Casi el 40% de la información perdida en violaciones de datos en 2016 era Información Financiera Personal, que puede incluir detalles de tarjetas de crédito o débito o registros financieros bancarios. Este número aumentó más del 6% al compararlo con 2015.

La exposición de datos financieros en violaciones de datos es grave, ya que los afectados corren un riesgo directo de pérdida financiera si estos datos son explotados.

Causas de violaciones de datos

Robo de datos fue la causa responsable del porcentaje más elevado (36%) de violaciones de datos en 2016, así como lo fue en 2015. Fue seguido por el uso impropio de datos, sin clasificación u otra causa (donde la causa no puede ser determinada) y phishing, spoofing o ingeniería social.

Las 10 principales causas de violaciones de datos en 2016

El robo de datos lideró la lista en 2016 como la principal causa de violaciones de datos, representando más de un tercio de las violaciones.

Clasif.	Causa	2015 (%)	2016 (%)	Diferencia de Porcentaje
1	Robo de Datos	42,4	36,2	-6,2
2	Uso Impropio de Datos	20,4	19,3	-1,1
3	Sin Clasificación u Otra Causa	11,9	19,2	7,3
4	Phishing, Spoofing o Ingeniería Social	21,8	15,8	-6,0
5	Pérdida Accidental de Datos	1,7	3,2	1,5
6	Pérdida o Robo de Dispositivo	0,6	3,1	2,5
7	Errores de TI que Llevan a la Pérdida de Datos	0,5	1,6	1,1
8	Interrupción de red o DDoS	0,3	1,6	1,3
9	Extorsión, Chantaje o Interrupción	0,1	0,2	0,1
10	Robo de Identidad o Fraude	0,1	0	-0,1

Mientras que el Robo de Datos es la causa de poco más de un tercio de las violaciones de datos al analizar la cifra de violaciones, cuando la medición es realizada por la cifra de identidades robadas, más del 91% de las violaciones se encuadran en esta categoría.

Las 10 principales causas de violaciones de datos por identidades robadas en 2016

El robo de Datos fue responsable de la gran mayoría de las identidades robadas en 2016.

Clasif.	Causa	2015 (%)	2016 (%)	Diferencia de Porcentaje
1	Robo de Datos	85,3	91,6	6,3
2	Phishing, Spoofing o Ingeniería Social	9,8	6,4	-3,4
3	Pérdida Accidental de Datos	1,1	1,0	- 0,1
4	Errores de TI que Llevan a la Pérdida de Datos	< 0,1	0,9	0,9
5	Interrupción de red o DDoS	< 0,1	< 0,1	< 0,1
6	Uso Impropio de Datos	3,3	< 0,1	- 3,3
7	Pérdida o Robo de Dispositivo	< 0,1	< 0,1	< -0,1
8	Sin Clasificación u Otra Causa	0,4	< 0,1	- 0,4
9	Extorsión, Chantaje o Interrupción	< 0,1	< 0,1	< 0,1
10	Robo de Identidad o Fraude	< 0,1	0	< -0,1

Sectores expuestos

El sector de Servicios fue el más afectado por la violación de datos en 2016, siendo que casi el 45% de las violaciones ocurrieron en ese sector, seguido por Finanzas, Seguros y el Sector Inmobiliario con 22%. Los dos primeros de la lista son los mismos que en 2015. Al analizar una subdivisión más detallada en subsectores, el sector de servicios empresariales presentó el mayor porcentaje de violaciones de datos (24%), seguido de servicios de salud (11%).

Debido a la confidencialidad de la información que podría ser revelada, existen rigurosas reglas relacionadas al relato de violaciones de datos en el sector de servicios de salud, lo que es responsable por su posición tan alta en la lista.

Los 10 principales sectores que sufrieron violaciones por cifra de incidentes

El sector de Servicios fue el más afectado por la violación de datos en 2016.

Clasif.	Sector	Violaciones	Porcentaje
1	Servicios	452	44,2
2	Finanzas, Seguros y Mercado Inmobiliario	226	22,1
3	Manufactura	116	11,3
4	Comercio Minorista	84	8,2
5	Transporte & Servicios Públicos	75	7,3
6	Comercio Mayorista	32	3,1
7	Construcción	20	2,0
8	Minería	8	0,8
9	Administración Pública	6	0,6
10	Estabelecimentos Não Classificáveis	3	0,3

Los 10 principales subsectores que sufrieron violaciones por cifra de incidentes

Los Servicios Empresariales fue el subsector más afectado, seguido por los Servicios de Salud.

Clasif.	Sector	Violaciones	Porcentaje
1	Servicios Empresariais	248	24,2
2	Servicios de Saúde	115	11,2
3	Instituciones Depositarias	71	6,9
4	Instituciones No Depositarias	62	6,1
5	Comunicaciones	42	4,1
6	Aseguradoras	41	4,0
7	Servicios de Gestión & Ingeniería	38	3,7
8	Ventas al por Menor - Diversos	34	3,3
9	Ventas al por Mayor - Bienes Duraderos	25	2,4
10	Holding & Otras Agencias de Inversión	23	2,2

Los 10 principales sectores y subsectores analizados por número de identidades robadas reflejan, en gran parte, los números arriba, con el sector de Servicios (90%) en la cumbre de la lista de sectores y Servicios Empresariales (78%) en la cumbre de los subsectores.

Tras analizar las violaciones de datos por número de identidades robadas, los Servicios de Salud representan un porcentaje bastante menor - es el 9º en la lista de subsectores, representando menos del 1% de las identidades robadas.

Los 10 principales sectores que sufrieron violaciones por cifra de identidades robadas

El sector de Servicios fue responsable por más del 90% de las identidades robadas en 2016.

Clasif.	Sector	Identidades	Porcentaje
1	Servicios	914.382.512	90,1
2	Manufactura	56.782.089	5,6
3	Comercio Minorista	13.173.167	1,3
4	Minería	9.758.832	1,0
5	Construcción	7.963.470	0,8
6	Transporte & Servicios Públicos	6.243.712	0,6
7	Finanzas, Seguros y Mercado Inmobiliario	3.554.225	0,4
8	Comercio Mayorista	2.051.635	0,2
9	Administración Pública	1.198.971	0,1
10	Establecimientos No Clasificables	685	< 0,1

Los 10 principales subsectores que sufrieron violaciones por cifra de identidades robadas

Los Servicios Empresariales fue el subsector más afectado en lo que se refiere a identidades robadas, respondiendo por casi el 78% del total.

Clasif.	Sector	Identidades	Porcentaje
1	Servicios Empresariais	786.918.569	77,5
2	Películas	85.200.000	8,4
3	Gráficas y Editoras	49.299.205	4,9
4	Servicios Personales	27.001.398	2,7
5	Ventas al por Menor - Diversos	10.694.512	1,1
6	Minería de Carbón	9.746.241	1,0
7	Servicios de Gestión & Ingeniería	8.216.181	0,8
8	Prestadores de Servicios Especiales	7.932.817	0,8
9	Servicios de Salud	6.868.017	0,7
10	Comunicaciones	5.304.054	0,5

Una característica interesante en la lista de subsectores es la presencia de Películas en el segundo lugar con 85,2 millones de identidades robadas (8%). Esta cifra puede atribuirse a una única violación de datos, la invasión del sitio francés de uso compartido de vídeos online Dailymotion, que se encuadra en la categoría Películas.

La violación de datos de Dailymotion ocurrió en octubre, sin embargo no fue revelada hasta diciembre. La violación resultó en la exposición de 85,2 millones de direcciones de correo electrónico y nombres de usuarios únicos que estaban en los sistemas de la empresa. Sin embargo, aproximadamente cerca del 20% de las cuentas expuestas tenían contraseñas asociadas que fueron cifradas con el método fuerte bcrypt hashing, tornándolas difíciles de descifrarlas.

Datos por país

Estados Unidos fue el primero de la lista, tanto en número de violaciones por país como en el número de identidades robadas por país. Este descubimiento no sorprende por varios motivos. EE.UU. posee una gran población, alta adopción de tecnología, y un gran número de compañías con sede en el país. Existen también rigurosas exigencias legales en EE.UU. sobre los reportes de violaciones de datos. Las violaciones de datos frecuentemente no se relatan en su totalidad, en territorios donde no existen exigencias legales.

Los 10 principales países por cifra de violaciones de datos

Estados Unidos fue el país más afectado por las violaciones de datos en 2016.

Clasif.	País	Identidades
1	Estados Unidos	1023
2	Reino Unido	38
3	Canadá	19
4	Australia	15
5	India	8
6	Irlanda	8
7	Japón	7
8	Israel	6
9	Alemania	5
10	Tailandia	5

Los 10 principales países por cifra de identidades robadas

Una vez más, Estados Unidos lidera la lista de identidades robadas en 2016.

Clasif.	País	Identidades
1	Estados Unidos	791.820.040
2	Francia	85.312.000
3	Rusia	83.500.000
4	Canadá	72.016.746
5	Taiwán	30.000.051
6	China	11.344.346
7	Corea del Sur	10.349.341
8	Japón	8.301.658
9	Holanda	6.595.756
10	Suecia	6.084.276

Al analizar las identidades robadas en EE.UU. un descubrimiento interesante es que las identidades fueron expuestas principalmente en megaviolaciones. El 90% de las identidades robadas en EE.UU. fueron expuestas en apenas ocho megaviolaciones.

En 2016, hubo apenas cuatro violaciones de datos en Francia, pero el país se encuentra en el segundo lugar en la lista de identidades robadas debido a la violación de Dailymotion discutida anteriormente, en la que más de 85 millones de identidades fueron robadas.

De la misma forma, en Rusia, dos violaciones de datos fueron responsables de la mayor parte de las identidades expuestas. Ambas violaciones se produjeron en Mail.Ru. Una violación reveló 57 millones de direcciones de correo electronico, mientras que la segunda vio 25 millones de cuentas de usuario afectadas en un foro online.

Economía Clandestina

Mientras que la economía clandestina está típicamente asociada al robo de información personal y detalles de tarjetas de crédito, los investigadores de Symantec observaron el creciente interés de los cibercriminales en la venta de cuentas de medios de comunicación, como Netflix y Spotify, con precios que varían desde 10 centavos a US$ 10 por cuenta. Si bien los valores que pueden cobrarse por estas cuentas son bajos, si un grupo de ataque tiene un dispositivo infectado es posible que tendrá esas informaciones de cuenta de cualquier modo, entonces intenta venderlas en un esfuerzo para maximizar sus lucros.

La economía clandestina en 2016 tiene algo para todos: desde cuentas para aplicaciones de transporte como Uber por US$ 1 hasta servicios DDoS (denegación de servicio distribuido) que pueden costar hasta US$ 1.000.

Las tarjetas de regalo de restaurantes, reservas de hoteles y millas de fidelidad de compañías aéreas también estaban entre los servicios a la venta. Las cuentas bancarias online también estaban a la venta, junto con cuentas PayPal y cuentas de compras de ventas al detalle como Amazon y Walmart.

En relación al malware, toolkits de ransomware pueden comandar hasta US$ 1.800, y fueron muchas veces vendido como "Crimeware-as-a-Service" (CaaS), con troyanos de Android banking vendidos por US$ 200.

Symantec observó un aumento en la oferta de servicios de transferencia de dinero, que se estaban vendiendo por aproximadamente 10% de su valor, por ejemplo, pagar US$ 100 en bitcoins para una transferencia de dinero de US$ 1.000. Eso indica que el proceso de sacar dinero robado todavía es el paso más difícil en la cadena para los cibercriminales.

Los valores observados, en foros clandestinos públicamente accesibles y sitios Tor en la web oscura, se mantuvieron estables desde 2015. Las tarjetas de crédito aún son el bien digital más vendido en foros clandestinos.

Los valores para las tarjetas de crédito variaron mucho, dependiendo del país de origen (tarjetas de crédito de la UE son más caras que las tarjetas de EE.UU.), bandera, nivel (Gold, Platinum, etc), y la información adicional proporcionada. Las tarjetas de crédito con información completa tuvieron un valor más elevado que aquellas sin estos detalles, y si un número de identificación personal (PIN) estuviese incluido, el precio podría ser 10 veces mayor.

Lista de precios de mercados clandestinos

Tarjetas de pago	Precio (USD)
Tarjeta de crédito única	$0.5 - $30
Tarjeta de crédito única con detalles completos (Fullz)	$20 - $60
Datos de la banda magnética 1&2 & PIN	$60 - $100
Malware	
Kit básico de troyano bancario con soporte	$100
Troyano de robo de contraseña	$25 - $100
Troyano para Android banking	$200
Generador de downloader de macro del Office	$5
Servicio de cifrado de Malware (dificultar la detección)	$20 - $40
Kit de ransomware	$10 - $1800
Servicios	
Servicios de streaming de audio	$0.10 - $10
Cuentas de programa de recompensa de hoteles (100K puntos)	$10 - $20
Cuenta de millas de fidelidad de compañía aérea (10K millas)	$5 - $35
Cuentas de aplicaciones de táxi con créditos	$0.5 - $10
Tarjetas de regalo de vendedores online	20% - 65% del valor de la tarjeta
Tarjeta de regalo de restaurantes	20% - 40% del valor de la tarjeta
Reservas de hotel y pasajes aéreos	$10 del valor de la reserva
Servicio DDoS, < 1h de duración, blanco de ataque medio	$5 - $20
Servicio DDoS, > 24h de duración, blanco de ataque mediano y fuerte	$10 - $1000
Alojamiento blindado dedicado (por mes)	$100 - $200
Servicios de Transferencia de dinero	
Servicio de cash-out	10% - 20%
Cuentas	
Cuentas bancarias online	0.5% - 10% do saldo de la cuenta
Cuentas de vendedores	$20 - $50
Cuentas de prestadores de servicios en la nube	$6 - $10
Identidades	
Identidad (Nombre, DNI y fecha de nacimiento)	$0.1 - $1.5
Pasaportes y otros documentos digitalizados (ej.: cuenta de luz)	$1 - $3

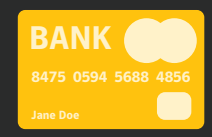
El mercado clandestino

Toolkit de Ransomware
$10 - $1.800 (USD)

DDoS corta duración
(< 1 hr)
$5 - $20 (USD)

Documentos
(Pasaportes, cuentas de servicios públicos)
$1 - $3 (USD)

Trojan bancario para Android
$200 (USD)



Tarjetas de crédito
$0,5 - $30 (USD)

Cuenta de servicios de nube
$6 - $10 (USD)

Tarjeta de regalo
20% - 40% del valor de la tarjeta

Servicio de cash-out
10% - 20% del valor de la tarjeta

Donde *todo* tiene un precio

Interferencias y interrupciones

Mientras el cibercrimen continúa siendo un negocio rentable, hubo una serie de interferencias legales significativas, incluyendo varias interrupciones de destaque, que ayudaron a atrapalhar las actividades y enviar una señal de alerta.

Avalanche

La operación para derribar Avalanche fue un duro golpe para la comunidad de cibercriminales, tras la interferencia en la infraestructura usada por al menos 17 familias de malware. La operación fue un esfuerzo conjunto de varias agencias de autoridades legales internacionales, promotores públicos y organizaciones de seguridad y de TI, incluyendo a Symantec. Eso resultó en la aprensión de 39 servidores y cientos de miles de dominios que estaban siendo usados por la organización criminal responsable por la red Avalanche.

El trabajo de Symantec relacionado a la red Avalanche tuvo inicio en 2012 cuando publicó una investigación sobre ransomware que tenía como blanco predominante las personas que usaban el idioma alemán en Alemania, Austria y regiones de Suiza. Al mismo tiempo, la policia alemana estaba ejecutando una investigación sobre el malware Bebloh (Trojan. Bebloh), que estaba en la investigación de Symantec. Los investigadores de Symantec brindaron asistencia técnica para la investigación policial y esos esfuerzos combinados eventualmente lllevaron al descubrimiento de la botnet Avalanche. Avalanche era una inmensa operación responsable de controlar un gran número de computadoras afectadas en todo el mundo.

La investigación culminó en la operación llevada a cabo el 30 de noviembre de 2016 y resultó en el derribo de la infraestructura de apoyo para al menos 17 familias diferentes de malware, así como la detención de varios individuos sospechosos de participar en la operación.

Bayrob

La operación para derribar Bayrob culminó una investigación de 8 años del FBI con soporte de Symantec, que acompañó la prisión y extradición hacia EE.UU de tres rumanos que pueden haber robado hasta US$ 35 millones de víctimas durante varios años.

Los cibercriminales de carrera responsables del Bayrob (Trojan. Bayrob) iniciaron con la creación de falsas subastas online de vehículos para engañar a las víctimas y extorsionar decenas de miles de dólares, antes de diversificar en otras operaciones fraudulentas y de malware, incluyendo robo de tarjeta de crédito y minería de criptomonedas.

Durante su investigación, Symantec descubrió varias versiones del malware Bayrob, recopiló datos de inteligencia y observó como Bayrob se transformó de una operación de fraude online para una botnet de más de 300.000 computadoras usadas para la minería de criptomonedas. Symantec consiguió exponer las operaciones del grupo de delincuentes, ganando insights sobre sus principales responsables, tácticas, malware, además del impacto potencial y las actividades criminales realizadas.

Symantec escribió por primera vez sobre el grupo Bayrob en 2007, cuando expuso su fraude altamente sofisticado de ventas falsas de coches en eBay. Sin embargo, esta atención pública no intimidó a los criminales y los delincuentes prosiguieron sus actividades criminales, ejecutando más fraudes en subastas online, así como diversificaron sus actividades con fraudes de tarjetas de crédito. También reclutaron una red de mulas de dinero en EE.UU. y en Europa, para transportar los rendimientos de sus estafas hacia Rumania.

En los últimos años, el grupo había centrado su atención en la construcción de una botnet para minería de criptomonedas, y en 2016 su botnet había crecido para más de 300.000 computadoras.

En el transcurso de los años, Symantec monitoreó continuamente las actividades del grupo, permitiendo que pudiésemos continuar mejorando la protección hacia nuestros clientes, así como auxiliar la investigación del FBI. Esta cooperación, eventualmente, llevó a las detenciones a fines de 2016.

Lurk/Angler

Fuerzas de seguridad rusas realizaron una operación para reprimir el grupo de malware bancario Lurk en junio de 2016, arrestando a 50 personas en Moscú.

El troyano bancario Lurk tuvo como blanco instituciones financieras rusas y se estima que el grupo responsable del mismo pudo haber robado más de US$ 25 millones de las cuentas de varias instituciones financieras rusas.

Estas detenciones coincidieron con la caída en las actividades de una serie de grupos de amenazas, incluyendo Locky, Dridex, y el kit de exploit Angler. Sin embargo, mientras Locky y Dridex experimentaron un aumento en sus actividades nuevamente en el segundo semestre de 2016, Angler no tuvo el mismo comportamiento. Eso llevó a la especulación de que las mismas personas eran responsables tanto por el troyano bancario Lurk como por el kit de exploit Angler.

Desde las capturas vinculadas a Lurk, Angler desapareció del panorama de amenazas, un hecho que fue relatado en detalles en el capítulo de Ataques Web.

Dyre

Una de las historias más grandes a ser publicadas en el inicio de 2016 fue relacionada al troyano de fraude financiero Dyre.

En febrero surgieron relatos que una operación de autoridades legales rusas en noviembre de 2015 coincidió con la interrupción casi total de las actividades que usaban este troyano financiero. La telemetría de Symantec confirmó esta caída en las actividades. Dyre (Infostealer.Dyre) era distribuido a través de campañas de correo eelctrónico de spam, y ninguna campaña de spam relacionada a Dyre se ha observado por Symantec desde el 18 de noviembre de 2015.

La operación para derribar Dyre fue significativa porque el troyano se había vuelto una de las herramientas de fraude financiero más activas en operación. Dyre tenía como objetivo las computadoras con Windows para robar datos bancarios y otras credenciales, y también podría ser usado para infectar a las víctimas con otros tipos de malware y añadirlos a las botnets de spam.

Las campañas de spam de Dyre contenían un adjunto malicioso que, al abrirlo, instalaría el downloader Upatre (Downloader.Upatre) en la computadora de la víctima. Las detecciones de Upatre afectaron un pico de más de 250.000 en julio de 2015. Las detecciones de Upatre y Dyre cayeron drásticamente después de noviembre de 2015.

Las circunstancias que rodean el derribo de Dyre no son claras, sin evidencias definitivas relacionadas a quienes o cuantas personas fueron arrestadas. Relatos a fines de 2016 afirmaron que el nuevo troyano bancario Trickbot (Trojan.Trickybot) era una relectura de Dyre. Investigadores de Fidelis creen "con moderada confianza" que uno o más de los creadores originales de Dyre estaban involucrados con Trickbot.

Lectura adicional

- Malware de grupos de ataques SWIFT vinculado a más ataques financieros
- Odinaff: Nuevo troyano usado en ataques financieros de destaque
- Red de malware Avalanche es afectada por operación de autoridades legales
- Bayrob: Tres sospechosos extraditados para enfrentar acusaciones en EE.UU.
- Aumento de amenazas PowerShell: el 95,4% de los scripts analizados eran maliciosos
- Necurs: La botnet de envío de correo electrónico masivo retorna con nueva ola de campañas de spam

Mejores prácticas

- Efectúe el backup periódico de cualquier archivo almacenado en su computadora y otros dispositivos.
- Mantenga siempre actualizado su software de seguridad en todos sus dispositivos, incluso los dispositivos móviles, a fin de protegerse contra cualquier nueva variante de malware.
- Mantenga su sistema operativo y otros softwares actualizados. Las actualizaciones de software incluirán frecuentemente parches para vulnerabilidades de seguridad recientemente descubiertas que podrían ser explotadas por grupos de ataque.
- Excluya cualquier correo electrónico de apariencia sospechosa que reciba, especialmente si incluyen enlaces o adjuntos.
- Desconfíe de cualquier adjunto de correo electrónico del Microsoft Office que aconseje a habilitar macros para exhibir su contenido. A menos de que esté absolutamente seguro de que este es un correo electrónico genuino de una fuente confiable, no active macros y, en vez de eso, excluya inmediatamente el correo electrónico.
- Absténgase de realizar la descarga de aplicaciones de sitios desconocidos y solamente instale aplicaciones de fuentes seguras. Además, preste mucha atención a las autorizaciones solicitadas por apps.
- Asegúrese de que las contraseñas que usa para sus cuentas online sean exclusivas y fuertes. No reutilice contraseñas para varias cuentas, y si está disponible, habilite la autenticación de dos factores.
- Regístrese para recibir alertas de su banco para avisarlo si se efectúa alguna transacción sospechosa en su cuenta.

Ransomware: Extorsionando a consumidores y empresas

Sección

07

Symantec

Introducción

En 2016, ransomware fue una de las amenazas más significativas enfrentadas por individuos y organizaciones. Los grupos de ataque mejoraron y perfeccionaron el modelo de negocio de ransomware, con el uso de cifrado fuerte, pagos anónimos en Bitcoin, y grandes campañas de spam para crear malware peligroso y amplio. El número creciente de nuevas familias de ransomware indica que cada vez más los grupos de ataque están usando esta estrategia. Si bien especialmente los consumidores (69% de todas las infecciones) corren riesgos de ataques de ransomware, este año vieron evidencias que los grupos de ataques de ransomware están creando nuevas ramificaciones y desarrollando ataques aún más sofisticados, tales como ataques de ransomware dirigidos a las empresas que involucraron una infección inicial y movimiento por la red, llevando al cifrado de varias máquinas. Ransomware parece destinado a seguir siendo una gran fuente de preocupación mundial en 2017.

Principales conclusiones

- Debido a su prevalencia y poder de destrucción, ransomware continuó siendo la amenaza de cibercrimen más peligrosa para los consumidores y las empresas en 2016.
- El valor promedio de rescate aumentó considerablemente, 266%, de US$ 294 en 2015 para US$ 1.077. Es evidente que los grupos de ataque consideran que pueden exigir más de las víctimas.
- Las detecciones de ransomware aumentaron un 36% en 2016.

Tendencias y análisis

El número de detecciones de ransomware aumentó un 36% en 2016, de 340.000 en 2015 para 463.000 en 2016. La tasa diario de detecciones de antivirus para ransomware también aumentó en 2016, con un promedio de aproximadamente 846 por día en el inicio del año y aumentó para más de 1539 por día en el fin del año.

Es importante percibir que estos números de detección representan una pequeña fracción de la cantidad total de ransomware bloqueado por Symantec, con la mayoría de los ataques bloqueados en el inicio del proceso de infección.

Ransomware es distribuido de diferentes formas y, de un modo general, el proceso de infección involucra diferentes etapas en las que el ataque puede ser bloqueado. Por ejemplo, en el caso de ransomware distribuido vía correo electrónico, la mayoría de los ataques (cientos de miles al día) son bloqueados por defensas antispam. La mayoría de los correos electrónicos de ransomware vienen con un archivo ejecutable escondido en un adjunto malicioso. El archivo ejecutable es usado para bajar e instalar el ransomware en la computadora de la víctima y un volumen significativo de ataques es bloqueado en esta fase, antes de que el ransomware se descargue en la computadora de la víctima.

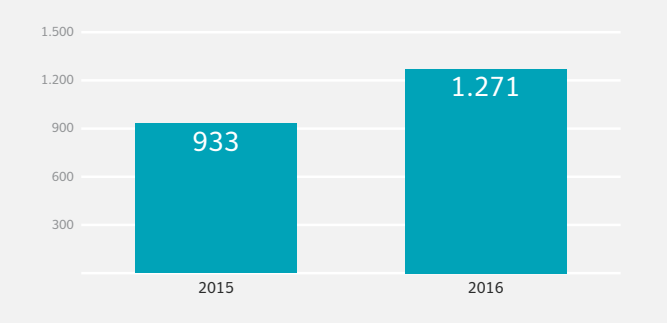
En el caso de ataques web, un volumen significativo de ataques ransomware es realizado con el uso de kits de exploits, páginas web maliciosas proyectadas para explotar vulnerabilidades en la computadora de la víctima para instalar malware. Un gran volumen de ataques de ransomware es bloqueado en la fase del kit de exploit, antes de que el ransomware logre instalarse en la computadora de la víctima.

Además de los ataques que se bloquean en el inicio del proceso de infección, ransomware es frecuentemente detectado y bloqueado por tecnologías de detección genérica, que identifican comportamientos maliciosos comunes en malware.

Si bien las detecciones de ransomware realizadas por antivirus representan un pequeño porcentaje del número total de ataques, un aumento considerable en las detecciones durante el año sugiere que la actividad de ransomware aumentó en 2016.

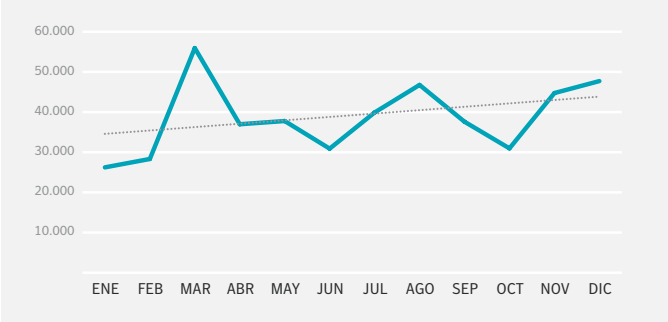
Promedio de detecciones globales de ransomware por día

Las detecciones de ransomware por antivirus aumentaron un 36% en comparación con 2015, aumentando de un promedio de 933 por día en 2015 para 1.270 por día en 2016.



Detecciones globales de ransomware por mes

Las detecciones mensuales de ransomware por antivirus aumentaron en el transcurso de 2016, con un promedio de aproximadamente 35.000 por mes en el inicio del año y subiendo para más de 40.000 por mes en el fin del año.

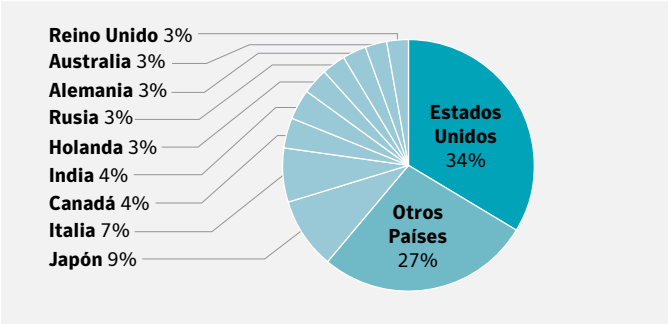


Con más de un tercio de todas las infecciones registradas en 2016, EE.UU. sigue siendo la región más afectada por ransomware. Japón (9%), Italia (7%), Canadá (4%) e India (4%) también son fuertemente afectados. Los países europeos como Holanda (3%), Rusia (3%), Alemania (3%), y Reino Unido (3%) también presentan posiciones de destaque en las estadísticas de infección. Otro país a figurar en el top 10 es Australia (3%).

Las estadísticas indican que los grupos de ataque están en gran parte, concentrando sus esfuerzos en economías desarrolladas y estables.

Detecciones de ransomware por país

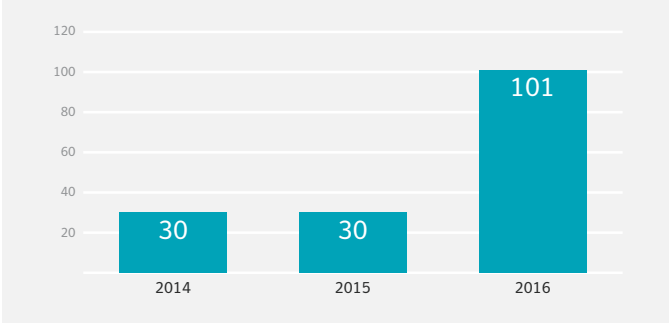
Las detecciones de ransomware por antivirus por país en 2016. EE.UU. sigue siendo la región donde ransomware es más predominante.



La cifra de nuevas familias de ransomware aumentó drásticamente en 2016. Con 30 nuevas familias a cada año en 2014 y 2015, la cifra más que triplicó para 101 en 2016. La tendencia sugiere que cada vez más los grupos de ataque están usando la estrategia de ransomware y creando nuevas familias de ransomware, en lugar de modificar las ya existentes.

Nuevas familias de ransomware

Nuevas familias de ransomware descubiertas por año. La cifra más que triplicó para 101 en 2016, lo que sugiere que cada vez más los grupos de ataque están usando la estrategia de ransomware.

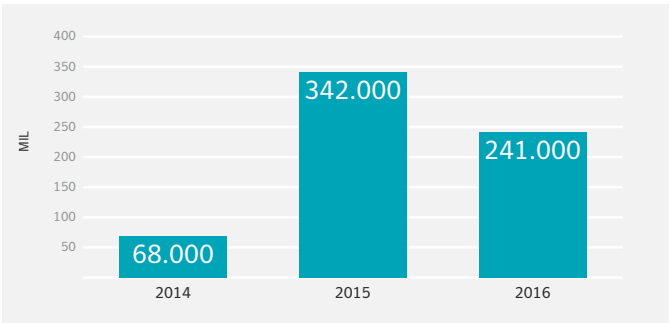


La cifra de variantes de ransomware (es decir, variantes distintas de familias de ransomware) disminuyó en comparación con el último año, una caída de 29% de 342.000 en 2015 para 241.000 en 2016. Esa tendencia de caída se reflejó en las cifras mensuales de nuevas variantes de ransomware, donde el promedio cayó de más de 20.000 en enero para menos de 20.000 en el fin del año.

La cifra de nuevas variantes es otra tasa de la actividad general de ransomware, donde los grupos de ataque crean nuevas variantes de sus amenazas, en la esperanza de escapar de la detección. La caída en la cifra de variantes puede ser explicada cuando es analizada junto al gran aumento de nuevas familias de ransomware en 2016. Los números sugieren que más grupos de ataque optan por comenzar desde cero con la creación de una nueva familia de ransomware en vez de ajustar las familias existentes, creando nuevas variantes.

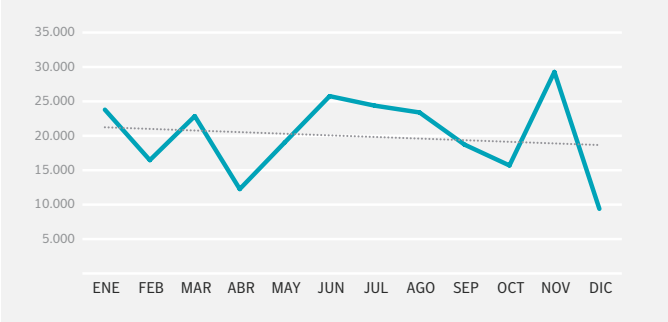
Nuevas variantes de ransomware

Nuevas variantes de ransomware (número de ejemplos únicos, individuales) por año. La cifra de nuevas variantes cayó un 29% de 342.000 en 2015 para 241.000 en 2016.



Variantes de ransomware por mes

Nuevas variantes de ransomware por mes. La cifra promedio cayó de más de 20.000 en enero para menos de 20.000 en el fin del año.

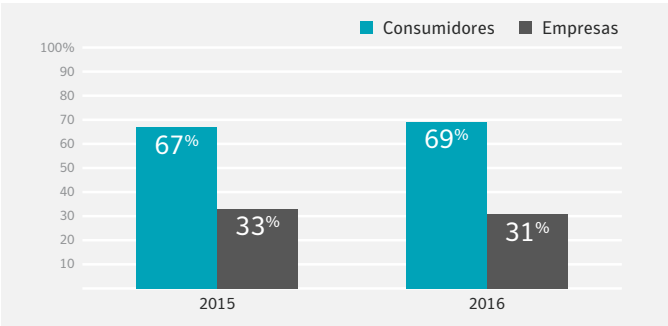


La mayor parte de las infecciones de ransomware en 2016 se produjo en las computadoras de consumidores (69%). Esta cifra subió ligeramente en relación a 2015, cuando la proporción de infecciones de ransomware que se produjeron en las computadoras de consumidores fue del 67%.

El porcentaje de infecciones de consumidores versus infecciones en empresas y otras organizaciones permaneció relativamente estable durante gran parte de 2016, con infecciones de consumidores representando entre el 59% y el 79%a cada mes. La única excepción fue diciembre de 2016, cuando hubo casi una paridad, con la proporción de infecciones de consumidores cayendo para el 51%.

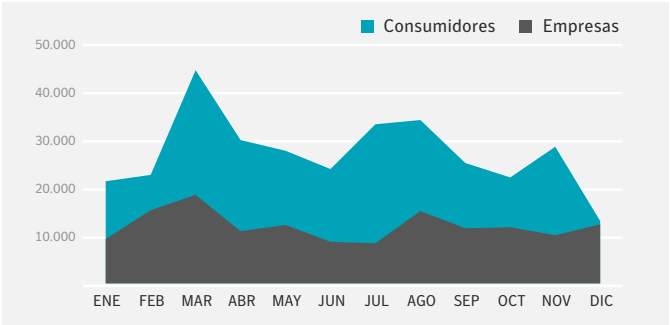
Infecciones de consumidores x corporativas

Infecciones de ransomware en consumidores x empresas. La mayor parte de las infecciones de ransomware en 2016 se produjo en las computadoras de los consumidores. El porcentaje de infecciones de consumidores (69%) subió apenas ligeramente en relación a 2015, cuando llegó al 67%.



Infecciones de consumidores x corporativas por mes

El porcentaje de infecciones de consumidores versus las infecciones en empresas y otras organizaciones permaneció relativamente estable durante gran parte de 2016.



Investigaciones/Estudios de casos

Cómo ransomware puede afectar a los consumidores

Actualmente existen cientos de diferentes familias de ransomware, distribuidas a través de una variedad de métodos, pero las amenazas de ransomware más activas que se observaron en 2016 fueron generalmente distribuidas por correo electrónico. En muchos casos, la víctima recibe un correo electrónico de spam proyectado para parecer una factura o recibo de una empresa. El correo electrónico está escrito de tal forma para atraer al destinatario a abrir un adjunto malicioso, por ejemplo, “Siguen los detalles de su reciente compra, más información vea el recibo adjunto.”

Abrir el adjunto puede iniciar el proceso de infección. Eso puede ejecutar un pequeño pedazo de malware, conocido como downloader o archivo ejecutable, que bajará el ransomware y lo instalará en la computadora de la víctima. Una vez instalado, el ransomware comenzará entonces el cifrado de varios archivos predefinidos en la computadora (o archivos en determinados directorios o archivos con determinadas extensiones o ambos). La mayor parte de las familias de ransomware más recientes emplean un cifrado fuerte, es decir, la víctima no tiene ninguna chance de abrir los archivos cifrados sin una chave de cifrado.

Muchas veces la víctima no tendrá conocimiento del problema hasta que se exhiba un mensaje en su pantalla. El mensaje generalmente explicará lo que sucedió con los archivos de la víctima y como puede pagarse el rescate, que muchas veces es hecho mediante sitios web en la red anónima Tor.

Cómo ransomware puede afectar a las empresas

La mayor parte de las amenazas de ransomware son de uso indiscriminado y la experiencia de infección es semejante para las empresas y los consumidores. Sin embargo, un pequeño número de grupos comenzó a dirigir sus ataques específicamente en empresas, con ataques de ransomware proyectados para infectar a varias computadoras en una única red y cifrar datos valiosos.

En el caso de SamSam (Ransom.SamSam) el punto inicial de ataque del grupo de ataque fue un servidor web volcado al público. Explotaron una vulnerabilidad no corregida para afectar el servidor e invadir la red de la víctima. A partir de este momento, el grupo de ataque usó herramientas polivalentes como Microsoft Sysinternals para desplazarse en la red de la víctima. Esto les permitio mapear cada computadora con acceso a la red de la organización e identificar los activos más valiosos.

A seguir, el grupo de ataque utilizó un script batch llamado f.bat para implantar SamSam y una clave de cifrado pública en cada computadora. El script también excluyó los archivos de copia de sombra de las computadoras, lo que impidió que cualquier archivo fuese restaurado a partir de ellos tras la infección. Después, distribuyeron una herramienta llamada sqlsrvtmg1.exe. Este archivo ejecutable buscó cualquier proceso de backup en ejecución y lo interrumpió. También se excluyó cualquier archivo de backup relacionado que fuese encontrado.

La última etapa fue la distribución de otro script batch llamado reg.bat. Este inició el proceso de cifrado en cada computadora infectada. SamSam está configurado para cifrar cientos de diferentes tipos de archivo. Una vez que finalizaba el cifrado, el ransomware era excluido, dejando los archivos cifrados y un pedido de rescate en el escritorio del equipo. El pedido instruía a la víctima a acceder a un sitio web y pagar un rescate de 1,5 Bitcoin (US$ 1.587 en el momento en que el documento fue creado) para cada computadora afectada.

Aumentan los pedidos de rescate

El rescate promedio exigido por los grupos de ataque aumentó drásticamente en 2016. Tras un ligero descenso en 2015, el rescate promedio demandado, conforme visto en nuevas familias descubiertas en 2016, subió de US$ 294 para US$ 1.077.

El aumento del rescate promedio demandado fue, en parte, afectado por el mayor rescate visto en 2016, un valor extremadamente alto de US$ 28.730, que fue exigido por el ransomware MIRCOP (Ransom.Mircop). Sin embargo, incluso si excluimos el rescate pago por MIRCOP, el rescate promedio habría más que doblado para US$ 678. Es evidente que los grupos de ataque consideran que puede cobrarse más de las víctimas.

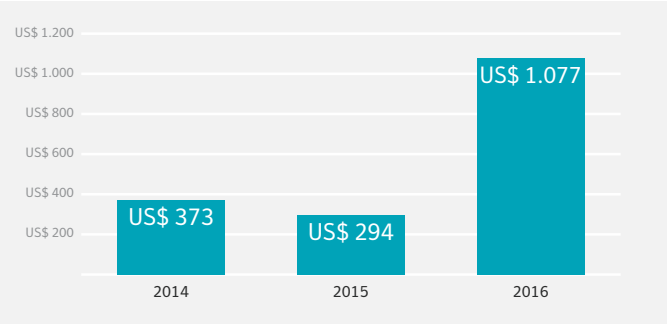
De acuerdo con una investigación realizada por el equipo Norton Cyber Security Insight, el 34% de las víctimas pagará el rescate. En EE.UU. este porcentaje sube para el 64% de las víctimas, lo que proporciona algunos indicios a respecto del motivo por el cual el país es un blanco tan grande de ataque. Disposición para pagar el rescate debe ser uno de los principales motivos para el aumento del valor de los pedidos de rescate.

El pago del rescate también quedó más fácil de administrarse. Para incentivar a las víctimas a pagar, los grupos de ataque muchas veces ya ofrecen soporte sobre cómo pagar la tasa y una mayor disponibilidad de servicios de pago torna incluso más fácil el uso del Bitcoin, especialmente ahora que Bitcoin no es tan obcuro como solía ser.

Sin embargo, pagar el rescate no garantiza la descodificación de los archivos de la víctima. De acuerdo con el equipo Norton Cyber Security Insight, apenas el 47% de las víctimas que pagaron el rescate relataron haber recibido sus archivos de vuelta.

Promedio de pedido de rescate

El pedido de rescate promedio visto en nuevas familias descubiertas en 2016 triplicó, de US$ 294 para US$ 1.077.



Los grupos de ataque también se han vuelto más creativos en sus intentos de extraer más de las víctimas, con varias familias de ransomware más recientes presentando pedidos de rescate variables. Por ejemplo, Cerber (Ransom.Cerber) duplica su pedido de rescate de 1 bitcoin (US$ 1.255) para 2,5 bitcoin después de cinco días, si no se paga el rescate .

Existen también algunas evidencias de que los grupos de ataques de ransomware comenzaron a adaptar sus pedidos de rescate en función del tipo y volumen de datos que cifraron. El grupo de ataque responsable del HDDCryptor (Ransom.HDDCryptor) habría exigido US$ 70.000 tras un ataque a la Agencia Municipal de Transportes de San Francisco, lo que ocasionó la interrupción del servicio ferroviario urbano de la ciudad (estos pedidos de rescate "personalizados" no se toman en cuenta en nuestros cálculos para valores promedios de rescate).

Vectores de infección

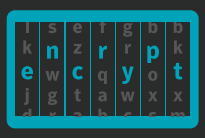
Ransomware es distribuido con el uso de varios vectores de infección. Uno de los vectores más comunes usados es el correo electrónico de spam, con algunas de las amenazas más frecuentes de 2016, tales como Locky (Ransom. Locky), distribuidas de esta forma.

Las campañas de spam en gran escala, algunas compuestas por millones de correos electrónicos, ocurren casi que diariamente y son alimentadas por botnets, redes de computadoras afectadas, que varían de cientos a millones de computadoras. La mayoría de las campañas utilizan trucos de ingeniería social para atraer a los destinatarios a abrir los correos electrónicos y adjuntos, por ejemplo, camuflar el correo electrónico como una factura o una notificación de envío.

Principales amenazas de ransomware

Locky

Cerber



CryptXXX

Rescate Aprox:

Locky	Cerber	CryptXXX
US$ 965	US$ 1.200	US$ 500

Descubierta:

Locky	Cerber	CryptXXX
Febrero 2016	Marzo 2016	Abril 2016

Distribuido por:

Locky

- Campañas de correo electrónico
- Kit de exploit Neutrino
- Kit de exploit Nuclear
- Kit de exploit RIG

- Una de las amenazas de ransomware más distribuidas en 2016
- Distribución a través de campañas de correo electrónico masivo generadas por la botnet Necurs
- Caída significativa en la incidencia del Locky en el inicio de 2017 debido a la reducción en la actividad de Necurs desde el fin de diciembre de 2016

Cerber

- Campañas de correo electrónico
- Kit de exploit RIG
- Kit de exploit Magnitude

- Bastante difundido en el fin de 2016, resultado de extensas campañas de correo electrónico y kit de exploit RIG
- Las campañas de correo electrónico usan principalmente JavaScript y archivos ejecutables de macros del Office, pero también pueden usar adjuntos de un archivo zip

CryptXXX

- Kit de exploit Angler
- Kit de exploit Neutrino

- El desaparecimiento del Angler a inicios de junio de 2016 provocó una disminución de las actividades
- Reapareció en el inicio de 2017 distribuido por el kit de exploit Neutrino
- Variantes más antiguas usaban cifrado débil que podría romperse. Las versiones más recientes emplean cifrado más fuerte, tornando imposible la descodificación

El método de infección más común involucra un adjunto malicioso que contiene un archivo ejecutable, generalmente un archivo JavaScript (JS.Downloader) o archivo ejecutable de Macro del Word (W97M.Downloader), que posteriormente baja e instala el ransomware. En algunos casos, ningún archivo es usado y el adjunto malicioso instala directamente el ransomware. En otros, el correo electrónico de spam contendrá un enlace que dirige hacia un kit de exploit, que instalará el ransomware en la computadora del destinatario. Algunos enlaces no llevan a un kit de exploit, en lugar de ello, llevan directamente a un archivo ejecutable o la carga útil del ransomware.

Kits de exploits son otro vector importante de infeccción y han sido utilizados para distribuir grandes amenazas de ransomware como Cerber (Ransom.Cerber) y CryptXXX (Ransom. CryptXXX). Los grupos de ataques que usan kits de exploits generalmente invaden los servidores web de terceros e ingresan un código malicioso en páginas web alojadas en ellos. Esto les permite dirigir los navegadores hacia los servidores de los kits de exploits.

Además de enlaces distribuidos a través de campañas de spam o publicaciones de medios sociales, los grupos de ataque pueden usar una serie de otros métodos para redirecionar el tráfico de los servidores de kits de exploits, tales como anuncios maliciosos (conocidos como malvertising) o redireccionar el tráfico de los servicios de distribución de tráfico.

Kits de exploit dependen de la explotación de vulnerabilidades. Los usuarios que ejecutan software desactualizado o sin parches de corrección corren más riesgo. Los usuarios con software actualizado solamente serán expuestos en los casos en que una vulnerabilidad de día cero es usada por un kit de exploit. A fines de 2016, Symantec estaba bloqueando en torno de 388.000 ataques por día a partir de kits de exploits.

Si bien las campañas de spam y kits de exploits son los principales vectores de infección, se han usado una serie de otras tácticas también para distribuir ransomware, incluyendo:

- **Infecciones secundarias:** En algunos casos el malware que ya infectó una computadora puede ser usado para bajar más malware, incluyendo ransomware. Un caso fue el ransomware CryptoLocker original, siendo que algunas víctimas quedaban supuestamente infectadas tras la infección original realizada por una de las varias botnets.
- **Ruptura de contraseñas por fuerza bruta:** Algunas familias de ransomware son distribuidas a través de la ruptura de credenciales de ingreso por fuerza bruta de software usado en servidores. Un ejemplo es Bucbi (Ransom. Bucbi), que usa este método para establecerse en servidores Remote Desktop Protocol (RDP).
- **Explotación de vulnerabilidades del servidor:** Varios grupos de ransomware tienen como blanco el software vulnerable que se ejecuta en servidores para tener acceso a la red de una organización. El grupo responsable por el ransomware SamSam (Ransom.SamSam) encuentra y explota vulnerabilidades para propagar su malware a través de una red.
- **Autopropagación:** A pesar de que un pequeño volumen de ransomware para Android demuestra comportamiento similar a un gusano, propagándose hacia todos los contactos vía SMS, 2016 vio el primer ransomware Windows usar autopropagación. ZCryptor (W32.ZCrypt) infecta todas las unidades removibles con una copia de sí mismo antes de comenzar el cifrado, aumentando las chances de propagarse hacia otras computadoras.
- **Tiendas de aplicaciones de terceros:** Algunas instancias de ransomware móvil pueden ser transmitidas vía tiendas de aplicaciones de terceros no seguras. Un ejemplo es Android.Lockdroid.E, que se presenta como un player de vídeo pornográfico en tiendas de aplicaciones de terceros.

Llega el ransomware como servicio

Un factor que puede haber influido el aumento de las actividades de ransomware en 2016 fue la llegada de Ransomware como Servicio (RAAS). Esto involucra la creación de kits de ransomware por los desarrolladores de malware, que pueden usarse para crear y personalizar fácilmente sus nuevas variantes de ransomware. Los desarrolladores generalmente ofrecen los kits para los grupos de ataque, en cambio de un porcentaje de los ingresos.

Un ejemplo de RaaS es Shark (Ransom.SharkRaaS), que surgió en 2016. Shark es distribuido a través de su propio sitio web y permite a los usuarios personalizar el valor del rescate y cuáles serán los archivos cifrados. El pago es automatizado y enviado directamente a los creadores de Shark, que retienen el 20% y envía lo restante para los grupos de ataques.

Nuevas técnicas: ataques dirigidos y "uso de herramientas del día a día"

A pesar de que los ataques de ransomware hasta hoy han sido generalmente indiscriminados, existen evidencias que los grupos de ataques tienen un creciente interés en centrarse en organizaciones con ataques dirigidos. Si bien en un volumen relativamente pequeño en comparación con las amenazas enviadas de forma masiva, estos ataques pueden ser devastadores para las organizaciones afectadas, con potencialmente cientos de computadoras cifradas.

Uno de los ejemplos más peligrosos de esta nueva generación de ataques dirigidos es SamSam (Ransom.SamSam). SamSam tiene como blanco los servidores que ejecutan versiones más antiguas, comunitarias y sin parches de corrección de JBoss Application Server, con los grupos de ataque usando herramientas disponibles de forma gratuita, por ejemplo,

la herramienta de prueba de código abierto JexBoss, para identificar servidores vulnerables.

Luego de ingresar en un servidor, los grupos de ataque pueden robar credenciales y usar una serie de herramientas disponibles públicamente, como servicios de Microsoft Sysinternals, para desplazarse en la red de la víctima. Cuando se identifican las computadoras ideales para infeccionar, los atacantes usan un script batch para implantar SamSam y un cifrado de clave pública en cada computadora. El script también excluye los archivos de copia de sombra de las computadoras, lo que impide que cualquier archivo sea restaurado a partir deles tras la infección. También buscan cualquier proceso de backup en ejecución y los interrumpe, además de excluir cualquier archivo encontrado relacionado a backup.

Las técnicas empleadas en los ataques SamSam son más vistas en campañas de ciberespionaje e indican el nivel de conocimiento disponible para algunos grupos de ransomware. A pesar de que es más difícil que se ejecuten, esos tipos de ataques dirigidos pueden potencialmente infectar miles de computadoras en una organización afectada, causando la interrupción de varios servicios.

Otras plataformas ahora vulnerables

Hasta la actualidad, los grupos de ataques de ransomware se han centrado, en gran parte, en usuarios del Windows, sin embargo, la variedad de plataformas bajo amenazas empezó a crecer. Han surdigo varias amenazas Android, inclusive un cripto-ransomware para Android en Ruso llamado Simplocker (Android.Simplocker) y su variante en inglés llamada (Android.Simplocker.B). Los dispositivos móviles no son los únicos dispositivos Android potencialmente vulnerables a ransomware. Investigaciones de Symantec han descubiero que las smartTVs que ejecutan el Android podrían también ser potencialmente afectadas.

En 2016, una amenaza conocida como KeRanger (OSX.Keranger) se volvió el primer ransomware generalizado que tenía como blanco los usuarios de Mac. KeRanger fue distribuido brevemente en una versión afectada del instalador para el cliente de Transmission BitTorrent.

Además de las amenazas específicamente proyectadas para un sistema operativo, se crean una serie de variantes de ransomware en JavaScript, lo que significa que puede infectar múltiples plataformas, como Ransom.Nemucod y Ransom.Ransom32.

Operaciones de autoridades legales

Hubo una serie de operaciones lideradas por autoridades legales que afectaron algunos de los grupos de ransomware menores en 2016. En agosto, la policía holandesa aprendió la infraestructura de comando y control (C&C) perteneciente al grupo WildFire (Ransom.Zyklon).

En diciembre, Symantec colaboró en una operación de destrucción de la red de alojamiento de malware Avalanche. La operación resultó en la detención de 39 servidores y cientos de miles de dominios que la organización criminal estaba usando para distribuir por lo menos 17 familias de malware, incluso el ransomware Trojan.Ransomlock.P.

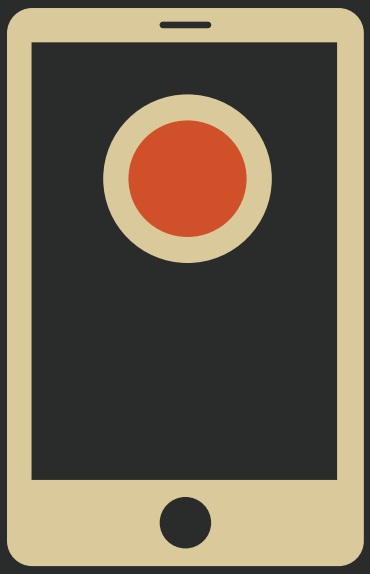
Lectura adicional

- Ransomware y Negocios 2016
- Ransomware Locky en la caza agresiva por víctimas
- KeRanger: Surge el primer ransomware para Mac OS X
- SamSam puede señalizar una nueva tendencia de ransomware dirigido

Mejores prácticas

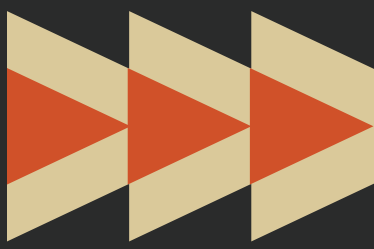
- Nuevas variantes de ransomware aparecen de forma periódica. Mantenga siempre actualizado su software de seguridad para protegerse contra ransomware.
- Mantenga su sistema operativo y otros softwares actualizados. Las actualizaciones de software incluirán frecuentemente parches para vulnerabilidades recientemente descubiertas que podrían ser explotadas por grupos de ataque de ransomware.
- El correo electrónico es uno de los principales métodos de infección. Excluya cualquier correo electrónico de apariencia sospechosa que reciba, especialmente si incluyen enlaces y/o adjuntos.
- Desconfíe de cualquier adjunto de correo electrónico del Microsoft Office que aconseje a habilitar macros para exhibir su contenido. A menos de que esté absolutamente seguro de que este es un correo electrónico genuino de una fuente confiable, no active macros y, en vez de eso, excluya inmediatamente el correo electrónico.
- Realizar backup de datos importantes es la manera más eficaz de combatir la infección por ransomware. Los grupos de ataque tienen poder sobre sus víctimas, al cifrar archivos valiosos y dejándolos inaccesibles. Si la víctima tiene copias de backup, puede restaurar sus archivos así que la infección haya sido eliminada.
- El uso de servicios en la nube puede ayudar a mitigar la infección por ransomware, ya que muchos mantienen versiones anteriores de archivos, permitiendo que usted "revierta" para los archivos no cifrados.

Nuevas fronteras: El Internet de las Cosas, dispositivos móviles y amenazas en la nube



Sección

08



Symantec

A pesar de que los ataques tradicionales contra equipos de escritorio y servidores han dominado en volumen el panorama de amenazas, existen otras plataformas que están siendo activamente atacadas o que están en el punto de mira de los responsables de las amenazas.

El uso generalizado de los dispositivos móviles y la adopción dominante de tecnologías en la nube y del Internet de las Cosas (IoT), abrió nuevas plataformas y usuarios para los grupos de ataque, y en 2016 pueden observarse una serie de amenazas emergentes cada vez más importantes contra esas tres áreas.

El Internet de las Cosas

El rápido aumento en el destaque dado a la seguridad de los dispositivos IoT en 2016 no surgió de la nada. Symantec alertó sobre la "inseguridad del Internet de las Cosas" en el ISTR de 2015. Sin embargo, habria sido difícil predecir el nivel de atención que IoT y su seguridad, o la falta de ella, recibiría en el último trimestre de 2016.

El motivo para tal atención se resume en una palabra: Mirai. La botnet Mirai, que está compuesta por dispositivos IoT, fue usada en varios ataques distribuidos de denegación de servicio (DDoS) hasta el fin de 2016.

Es difícil afirmar definitivamente cuantos dispositivos realmente fueron infectados por Mirai, no obstante muchos de los números mencionados son bastante alarmantes. La investigación de Incapsula descubrió casi 50.000 IPs originales que alojan dispositivos infectados por Mirai y que intentan lanzar ataques en su red. Level 3 dijo haber identificado aproximadamente 493.000 bots de Mirai: 213.000 antes que el código fuente fuese liberado, y 280.000 en los últimos meses de 2016.

Symantec estableció un honeypot de IoT en el fin de 2015 para rastrear intentos de ataque contra dispositivos IoT. Los datos recopilados de este honeypot muestran como los ataques a IoT están obteniendo fuerza y como los dispositivos IoT están atrayendo la atención de los grupos de ataque.

Principales conclusiones

- Los ataques contra el honeypot del Internet de las Cosas de Symantec casi duplicaron de enero a diciembre de 2016. Un promedio de casi 4,6 direcciones IP únicos afectaron el honeypot a cada hora en enero, pero eso aumentó para un promedio de poco más de 8,8 en diciembre. En momentos de pico de actividad, cuando Mirai estaba expandiéndose rápidamente, los ataques al honeypot estaban ocurriendo a cada dos minutos.
- En 2016, los dispositivos IoT fueron responsables por el mayor ataque DDoS ya visto. El ataque a la compañía de alojamiento francesa OVH, que llegó a alcanzar 1 Tbps, fue el mayor ataque DDoS ya registrado. Fue conducido principalmente por la botnet Mirai.
- Las contraseñas estándar todavía son la principal falla de seguridad para los dispositivos IoT. La contraseña "admin" es la más usada por los grupos de ataque.

Tendencias y análisis

¿Qué significa IoT? Muchas personas imaginan termostatos inteligentes y asistentes virtuales que responderán a los comandos de voz, pero IoT está compuesta principalmente por dispositivos frecuentemente usados. Los ruteadores domésticos, DVRs y las cámaras conectadas a Internet - que forman parte de IoT - fueron los dispositivos que más sufrieron como blancos de la botnet Mirai.

Una botnet es un "ejercito zombie" de dispositivos conectados a Internet, infectados con software malicioso y controlados como un grupo sin el conocimiento de sus propietarios. El grupo de ataque puede usar los dispositivos controlados para ejecutar actividades maliciosas, como ataques DDoS o campañas de spam. Los dispositivos IoT son un blanco atractivo para las botnets por tres motivos:

01 La seguridad muchas veces no es una prioridad para el fabricante del dispositivo. Eso lleva a prácticas inadecuadas, como el uso de contraseñas estándar y puertas abiertas, que los usuarios no alteran o no pueden cambiar.

02 Normalmente, no tienen mecanismos internos para recibir actualizaciones automáticas de firmware, posibilitando vulnerabilidades sin corrección.

03 Frecuentemente, son olvidados tras la instalación. Eso significa que sus propietarios no saben cuando los dispositivos están usándose para propósitos malicosos y tienen poco incentivo para aplicar actualizaciones de firmware.

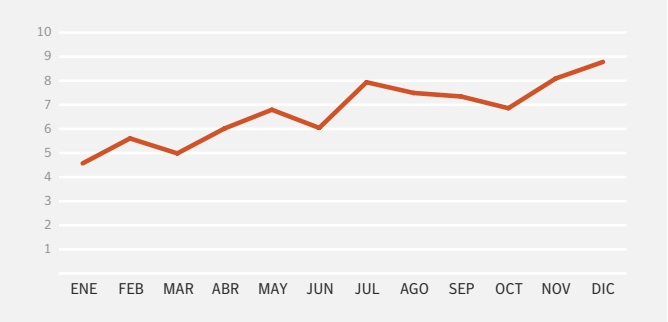
Mientras que el único propósito de Mirai parece ser los ataques DDoS, malware en un ruteador inalámbrico puede llevar que la información personal - incluso nombres de usuarios, contraseñas y datos financieros - sea robada. Los dispositivos IoT infectados también pueden usarse como un punto de partida para atacar otros dispositivos en una red privada. Eso también supone que uno de sus dispositivos puede participar de una botnet global enfocada en interrumpir la operación de sitios o servicios.

Symantec estableció un honeypot de IoT en 2015 para observar los ataques contra dispositivos IoT. El honeypot es camufado como un ruteador abierto y los intentos de conectarse al sistema son registrados para el análisis. Entre enero y diciembre de 2016, el número de direcciones IP únicas dirigidas al honeypot casi duplicó.

En enero, el número promedio de IPs únicos que escaneaban el honeypot a cada hora era casi 4,6. En diciembre, ese número creció para un promedio de poco más de 8,8. La mayoría de los IPs que afectaban el honeypot son otros dispositivos IoT.

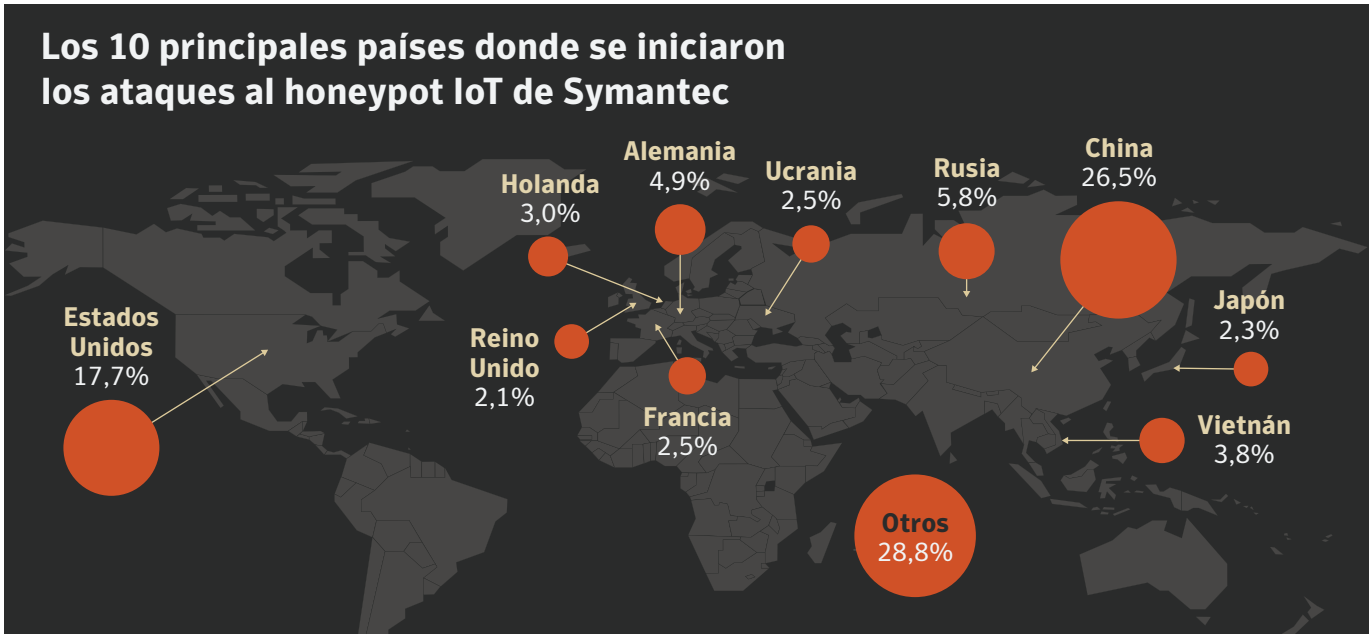
Ataques a cada hora al honeypot de IoT por mes

El aumento en los ataques a cada hora al honeypot de Symantec de enero a diciembre puede ser claramente observado, casi duplicando a lo largo del año.



Si bien ha ocurrido una ligera tendencia de caída de julio a octubre, en noviembre y diciembre los incidentes de ataques aumentaron bruscamente. El código fuente para la botnet Mirai fue divulgado públicamente en el último día de septiembre, lo que probablemente influyó en ese aumento.

El código fuente para Mirai fue revelado en un foro de hackers por un individuo con nombre de usuario Anna-senpai. No es posible decir definitivamente quien está por detrás de Mirai, pero el periodista de seguridad Brian Krebs, una de las primeras víctimas de la botnet, escribió un extenso artículo sobre su investigación con la identidad de Anna-senpai.



Un ataque en gran escala al proveedor de DNS Dyn, ocurrido el 21 de octubre, recibió una amplia atención de la prensa y puso a Mirai en las prinicpales noticias. Eso demostró como era fácil crear una botnet grande y causar daños a los principales sitios. Los autores del ataque Dyn no fueron identificados, pero se estima que eran "script kiddies" (aspirantes a hackers con pocas habilidades), en vez de un grupo de hackeo sofisticado. El ataque Dyn también reveló la existencia de Mirai hacia el mundo en general, y la prensa destacó los llamados "skids", que pidieron tutoriales en foros de hackers para que pudiesen aprender a usar el código fuente de Mirai.

Datos por país

El análisis de los datos de honeypot demostró también que era posible determinar de qué países se iniciaron los ataques al honeypot.

China (26,5%) y EE.UU. (17,7%) dominaron el volumen de ataques, con Rusia (5,8%), Alemania (4,9%) y Vietnán (3,8%) los próximos en la lista de los cinco principales países.

Esas métricas miden los países en los cuales la dirección IP del dispositivo de ataque fue localizado, pero eso no significa necesariamente que los propios grupos de ataque estaban ubicados en esos países.

Contraseñas

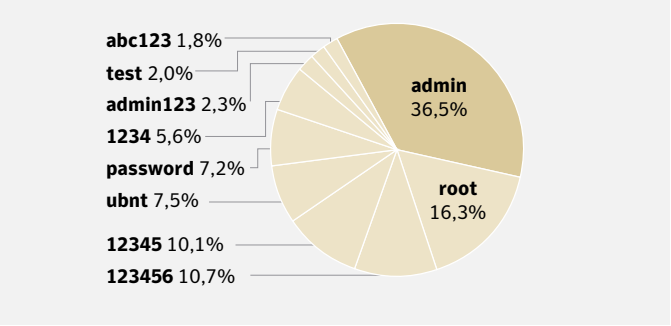
El análisis de las contraseñas usadas por el malware de IoT para intentar ingresar a los dispositivos trajo resultados no sorprendentes, revelando que los nombres de usuarios y contraseñas estándar de los dispositivos de IoT muchas veces no son alterados.

Existen muchas razones para esto. Varios dispositivos de IoT tienen nombres de usuario y contraseñas codificadas que no pueden ser fácilmente alteradas. Muchos usuarios posiblemente no conocen los peligros de las credenciales estándar, por lo tanto, raramente tratan de alterarlas.

La práctica tradicional recomendada determina que los usuarios deben poseer una combinación de nombre de usuario y contraseña exclusiva para todos los dispositivos de IoT, conforme es recomendado para las cuentas online. Sin embargo, a menos que los fabricantes y los proveedores implementen alteraciones que obligan a los usuarios a seleccionar una contraseña exclusiva, las contraseñas probablemente continuarán a ser un punto débil de la seguridad.

Las 10 contraseñas más utilizadas para intentar ingresar en el honeypot IoT de Symantec

Las contraseñas estándar dominaron la lista de las 10 contraseñas más utilizadas para ingresar en el honeypot de Symantec.



"Admin" (37%) y "root" (16%) dominan la lista de contraseñas usadas para intentar ingresar en el honeypot de Symantec, con los sospechosos usuales "123456", "12345", "1234" y "password" también parte de la lista. La contraseña estándar para la marca Ubiquiti de ruteadores, "ubnt", tambiém está en el top 10. Es probable que los ruteadores de Ubiquiti fuesen blancos porque fue revelado en mayo de 2016 que una antigua vulnerabilidad en los ruteadores permitía que los gusanos (worms) dirigiesen los dispositivos incorporados para propagarse por miles de ruteadores de Ubiquiti Networks ejecutando un firmware desactualizado.

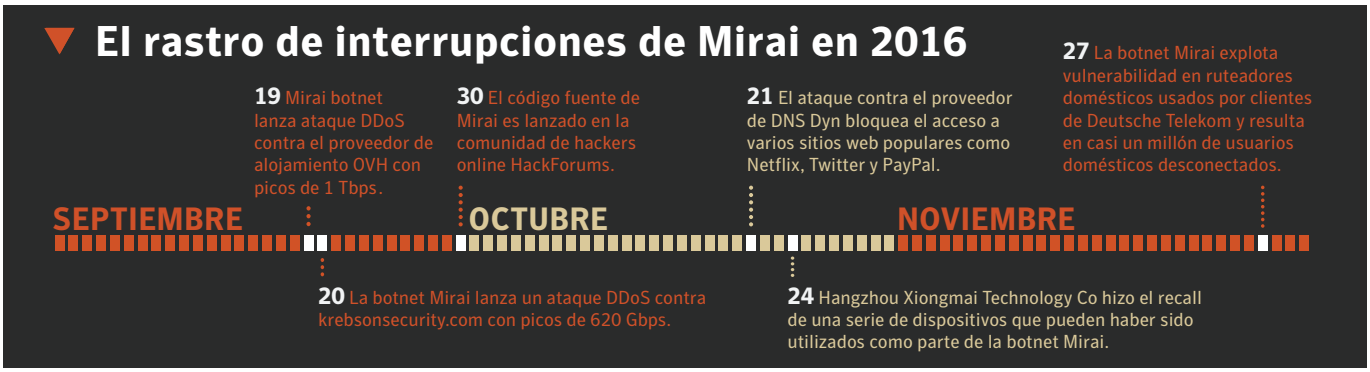
Si bien Ubiquiti, a mediados de 2016, lanzó una actualización de firmware que corrigió esta vulnerabilidad, el gusano aún era capaz de explotar la debilidad en los casos en que la actualización de firmware no había sido descargada.

La botnet Mirai

Mirai primero llamó la atención del público en septiembre, cuando, como mencionado arriba, la botnet fue usada para un enorme ataque DDoS en el sitio web de Brian Krebs. Ese ataque alcanzó el pico de 620 Gbps, tornándose el mayor ataque DDoS ya relatado en aquella época. Sin embargo, algunos días después, surgieron relatos sobre un ataque anterior a la compañía de alojamiento francesa OVH, y fue reportado que alcanzó un pico de 1 Tbps.

No obstante, fue un ataque DDoS en la empresa de DNS Dyn en octubre que puso en primera página a Mirai. El ataque a Dyn interrumpió las actividades de varios de los principales sitios web del mundo, incluso Netflix, Twitter y PayPal.

El ataque mostró lo poderoso que podría ser un ataque DDoS usando dispositivos IoT y levantó preguntas sobre lo que podría representar si los grupos de ataque decidiesen invadir sistemas de control industrial o infraestructura nacional crítica.



Mirai funciona con el escaneo continuo de dispositivos de IoT que son accesibles a través del Internet y protegidos por usuarios y contraseñas estándar de fábrica o codificados. Enseguida, los infecta con malware que los obliga a reportar a un servidor de control central, transformándolos en un bot que puede usarse en ataques de DDoS. Existen también al menos otras 17 familias de malware de IoT que están activamente infectando dispositivos.

Según la estimativa de Gartner, que hasta 2020 habrá más de 20.000 millones de dispositivos de IoT en el mundo, es importante que se resuelvan los problemas de seguridad o las campañas como Mirai puedan verse en una escala aún mayor. Asimismo, el perfil de los dispositivos de IoT posiblemente cambiará. A medida que los coches y los dispositivos médicos conectados se vuelvan más frecuentes, las motivaciones de los grupos de ataque también pueden cambiar.

Los ataques que usan dispositivos IoT también disminuyen las barreras para la entrada de los cibercriminales. Existe mucho menos seguridad a superar para los grupos de ataque cuando intentan asumir el control de un dispositivo de IoT. Al contrario de una computadora o laptop, que normalmente habrán instalados software de seguridad y recibirán actualizaciones automáticas de seguridad, la única protección de un dispositivo de IoT puede ser un nombre de usuario y una contraseña estándar fácilmente adivinados. Actualmente, la débil seguridad en los dispositivos de IoT apenas torna más fácil la vida de los cibercriminales.

Una historia en evolución

El código fuente para Mirai estaba disponible públicamente en el fin de septiembre. Como mencionado, fue publicado en HackForums por un usuario con el nombre Anna-senpai, el 30 de septiembre. Como esperado, la revelación del código fuente resultó en la creación de otras variantes de Mirai.

A fines de noviembre, una variante de Mirai interrumpió el acceso al internet para casi 1 millón de usuarios domésticos en Alemania. Esta variante atacó varios ruteadores donde el puerto TCP 7547 era accesible remotamente en el dispositivo, al tiempo que también explotaba una debilidad en el Protocolo de Administración CPE WAN. También se estima que los ruteadores similares usados por la compañía irlandesa Eir estaban vulnerables al mismo ataque.

Con esta primera variante apareciendo menos de dos meses después que el código fuente fue tornado público, sería razonable suponer que es apenas la punta de lo que podría ser un iceberg muy grande.

Visión futura

El número de dispositivos IoT continuará creciendo y eso puede llevar a un aumento de las solicitudes para la reglamentación del sector de IoT como la única forma de enfrentar el problema de la seguridad. Si la reglamentación se torna una posibilidad, la próxima cuestión es si sería mejor aplicada en el nivel de la industria o del gobierno.

El ataque DDoS contra Dyn, con sede en EE.UU., que fue ejecutado predominantemente con el uso de webcams producidas por la empresa china de electrónicos XiongMai Technologies, enfatiza la dificultad de reglamentar los dispositivos de IoT.

A pesar de que no existe ninguna manera de corregir un problema complejo como este, estándares de seguridad basados en riesgos son parte de la solución. Las naciones individuales deben considerar una reglamentación de seguridad mínima, en particular para usos críticos, a fin de garantizar que la seguridad sea un requisito fundamental en la concepción y fabricación de dispositivos IoT.

Naturalmente, los fabricantes deben asumir el rol principal en la seguridad de los productos que envían al mercado. Deben proporcionar a los consumidores un nivel de transparencia en la seguridad de los dispositivos IoT para que puedan tomar una decisión informada en sus compras. Eso también permite que la seguridad se vuelva un recurso inherente en un dispositivo, lo que permitiría a los fabricantes premium diferenciar sus productos con base en la seguridad.

Independientemente de lo que suceda, es probable que la seguridad del internet de las cosas continuará a ser muy discutida en 2017.

Mejores prácticas

- Examine las capacidades y los recursos de seguridad de un dispositivo de IoT antes de la compra.
- Ejecute una auditoría de los dispositivos de IoT usados en su red.
- Altere las credenciales estándar en dispositivos. Use contraseñas fuertes y únicas para cuentas de dispositivos y redes WiFi. No use contraseñas comunes o fácilmente adivinables como “123456” o “contraseña”.
- Use un método de cifrado fuerte al configurar el acceso a la red Wifi (WPA2).
- Muchos dispositivos vienen con una variedad de servicios habilitados por estándar. Desactive los recursos y servicios que no son necesarios
- Desactive el login Telnet y use SSH siempre que sea posible.
- Modifique las configuraciones estándar de privacidad y seguridad de los dispositivos de IoT de acuerdo con sus necesidades.
- Desactive o proteja el acceso remoto a los dispositivos de IoT cuando no sea necesario.
- Use conexiones cableadas en vez de inalámbricas donde sea posible.
- Regularmente verifique el sitio web del fabricante para actualizaciones de firmware.
- Asegúrese de que una falla de hardware no ocasione un estado inseguro del dispositivo.

Dispositivos Móviles

Symantec continuó observando un aumento en las actividades maliciosas relacionadas a los dispositivos móviles, dirigidas por cibercriminales que usaban métodos comprobados y seguros para obtener dinero de los ataques. Android continúa siendo la plataforma móvil más atacada. Sin embargo, tras un año de crecimento explosivo en 2015, la tasa de crecimiento de los ataques contra Android desaceleró por primera vez en 2016 a medida que los grupos de ataque consolidan sus actividades y utilizan mejores arquitecturas de seguridad.

Principales conclusiones

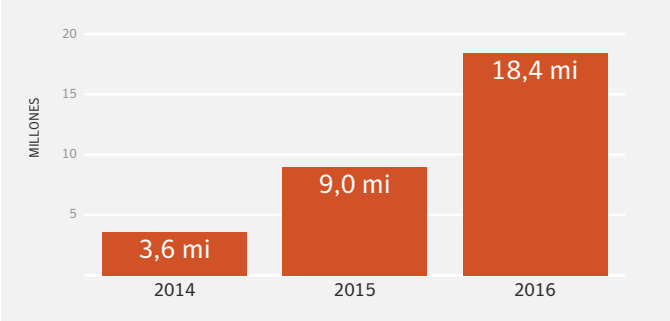
- El sistema operativo Android continúa siendo la atención principal de los responsables por amenazas móviles. Sin embargo, las mejoras de seguridad en la arquitectura del Android han vuelto cada vez más difícil la infección de teléfonos celulares o incluso capitalizar con infecciones exitosas.
- Los ataques al sistema operativo iOS todavía son relativamente raros. Sin embargo, tres vulnerabilidades de día cero en iOS fueron explotadas en ataques dirigidos para infectar celulares con el malware Pegasus en 2016.
- El volumen total de aplicaciones Android maliciosas aumentó significativamente en 2016, con un crecimiento del 105%. Pero, esta tasa de crecimiento desaceleró al compararla con el año anterior, cuando el número de aplicaciones maliciosas aumentó un 152%.
- En 2016, Symantec bloqueó 18,4 millones de infecciones de malware en dispositivos móviles. Los datos de dispositivos móviles protegidos por Symantec muestran que 1 de cada 20 dispositivos sufrió un intento de infección en 2016. Se observaron niveles semejantes en 2015.

Tendencias de malware de dispositivos móviles

El total de detecciones de amenazas en dispositivos móviles, incluso los datos de las tecnologías en la nube de Symantec, duplicó en 2016, resultando en 18,4 millones de detecciones de malware en dispositivos móviles en 2016. Sin embargo, el aumento del 105% en 2016 fue significativamente menor que el aumento del 152% en el año anterior, a pesar del crecimiento en el uso de smartphones. Esto indica que existe una transición en marcha de un período de crecimiento explosivo en el panorama de amenazas móviles, hacia una fase en la que los grupos de ataque están consolidando sus actividades, al mismo tiempo en que se adaptan a las medidas de seguridad implementadas en el Android.

Cifra total de detecciones por año de malware

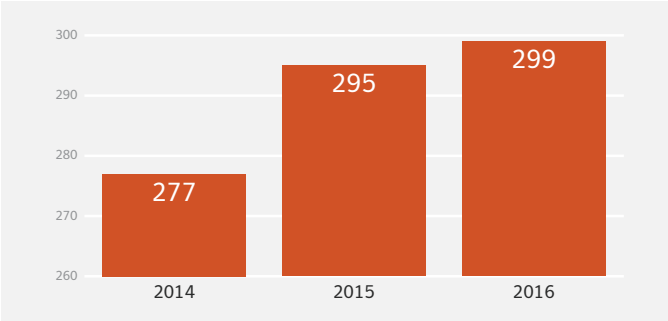
Symantec observó 18,4 millones de detecciones de malware en dispositivos móviles en 2016, un aumento del 105% en comparación con 2015.



Otras evidencias de la consolidación en marcha surgen cuando se analizan las familias de amenazas. Las familias de amenazas son un agrupamiento de amenazas de grupos de ataque, iguales o similares. Symantec registró cuatro nuevas familias de amenazas móviles en 2016, una caída acentuada en relación a 2015, cuando se identificaron 18 nuevas familias. No obstante, se debe notar que las tecnologías de detección más recientes, como heurística, aprendizaje de máquina y detecciones en la nube, detectan las amenazas de forma más genérica, camuflando potencialmente la presencia de nuevas familias. Al analizar más detalladamente las características de las amenazas móviles, pueden observarse conjuntos de 61 nuevas amenazas distintas que surgieron en 2016. Al comparar este número con los 75 grupos identificados en 2015, queda evidente una caída de casi 19%, nuevamente indicando una desaceleración en el crecimiento o innovación en el panorama de amenazas móviles.

Número acumulativo de familias de malware por año

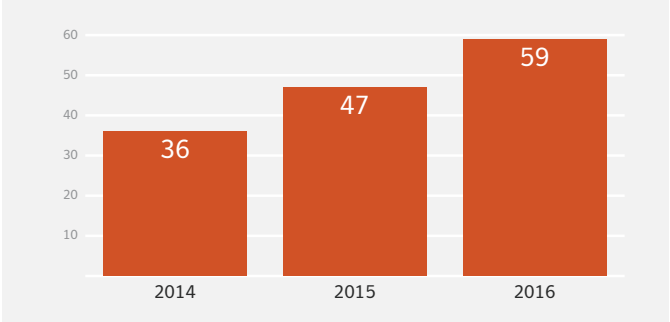
Cuatro nuevas familias de malware móviles fueron registradas por Symantec en 2016, una caída acentuada en relación a 2015, cuando se identificaron 18 nuevas familias.



Al analizar más detalladamente las variantes de amenazas individuales en cada familia, el número de variantes maliciosas de aplicaciones móviles por familia aumentó más del 25% en 2016, un poco menos que el aumento en 2015, cuando el número de variantes móviles maliciosas por familia aumentó un 30%.

Variantes de dispositivos móviles por familia

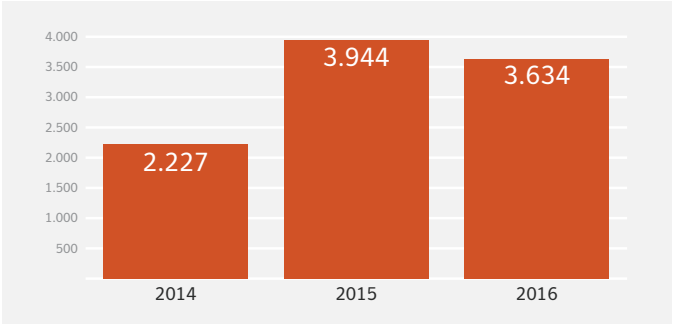
Las variantes móviles por familia aumentaron más del 25% en 2016, un poco menos que el aumento del 30% en 2015.



Al adoptarse una visión más holística, hubo una ligera caída en el número total de variantes maliciosas de aplicaciones móviles detectadas, con una reducción del 8% entre 2015 y 2016. Esta pequeña caída acompañó un enorme aumento en las variantes maliciosas de aplicaciones móviles detectadas entre 2014 y 2015, cuando aumentó más del 75%. Las cifras de este año muestran que la actividad comenzó a estabilizarse.

Variantes de malware para dispositivos móviles por año

La reducción de las variantes móviles detectadas en 2016 indica que la actividad en el área comienza a estabilizarse.



En general, se puede deducir que los grupos de ataque están optando por refinar y modificar las familias y los tipos de malware existentes, en vez de desarrollar nuevos y exclusivos tipos de amenazas.

Motivos y técnicas

El malware móvil continúa teniendo movimiento financiero y usa métodos comprobados y seguros de obtener dinero, como enviar mensajes de texto premium, fraude de clics de anuncios y ransomware.

Al analizar los tipos de malware detectados, las dos principales detecciones - Android.Malapp y Android.MalDownloader - representan más de la mitad del total de las detecciones del año. Estas son detecciones genéricas usadas para detectar una gran variedad de amenazas individuales, pero no clasificadas.

La primera detección que llama la atención en el top 10 es Android.Opfake que está en tercer lugar. Opfake detecta malware que envía mensajes de texto premium, que continúan siendo un gran generador de ingresos para los grupos de ataque de amenazas móviles. Una segunda detección de mensajes de texto premium, Android.Premiumtext, aparece en quinto lugar. El sistema operativo Android añadió avisos cuando se envían los mensajes de texto premium, tornando cada vez más difícil que los responsables por amenazas escondan sus actividades. Algunas de las otras instancias de malware en el top 10 (Android.HiddenAds y Android.Fakeapp) usan métodos de fraude de clics para obtener ingresos y escapar de los avisos.

El malware utilizado para distribuir ransomware y el malware usado en los intentos de robar información bancaria de las víctimas también aparecieron en las 20 principales detecciones en 2016.

Principales amenazas para dispositivos móviles en 2016

Las dos detecciones de malware para dispositivos móviles más frecuentes son nombres genéricos de detección, usados para bloquear una amplia gama de amenazas no clasificadas del Android.

Amenaza Móvil	Porcentaje
Android.Malapp	39,2
Android.MalDownloader	16,1
Android.Opfake	5,2
Android.HiddenAds	4,8
Android.Premiumtext	4,1
Android.Maldropper	2,1
Android.Mobilespy	1,9
Android.Downloader	1,7
Android.Dropper	1,7
Android.Fakeapp	1,7
Android.Smsstealer	1,7
Android.Rootnik	1,6
Android.Lotoor	1,4
Android.SmsBlocker	1,4
Android.MobileSpy	1,3
Android.RegSMS	1,2
Android.FakeInst	1,2
Android.SMSblocker	0,9
Android.HiddenApp	0,8
Android.Lockdroid.E	0,8

Tasas de malware y grayware

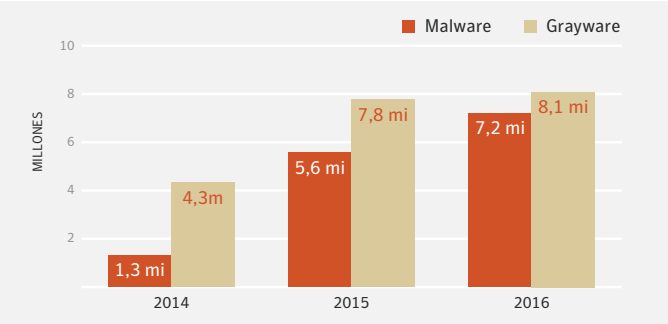
Symantec clasifica de forma proactiva las aplicaciones para dispositivos móviles que contienen grayware o malware.

Grayware está compuesto por programas que no contienen malware y no son directamente maliciosos, pero pueden ser irritantes o perjudiciales para los usuarios. Ejemplos incluyen herramientas de hackeo, accessware, spyware, adware, discadores y programas de bromas.

Hubo picos significativos en aplicaciones de malware y grayware entre 2014 y 2015, pero en 2016 los números de las dos áreas alcanzaron niveles semejantes. Grayware aumentó un poco menos de 4% en 2016, mientras que el malware aumentó aproximadamente un 29%, comparado con un aumento de más del 300% en 2015. Los niveles de grayware y malware identificados en 2016 son bastante parecidos.

Tasas de malware y grayware, 2014-2016

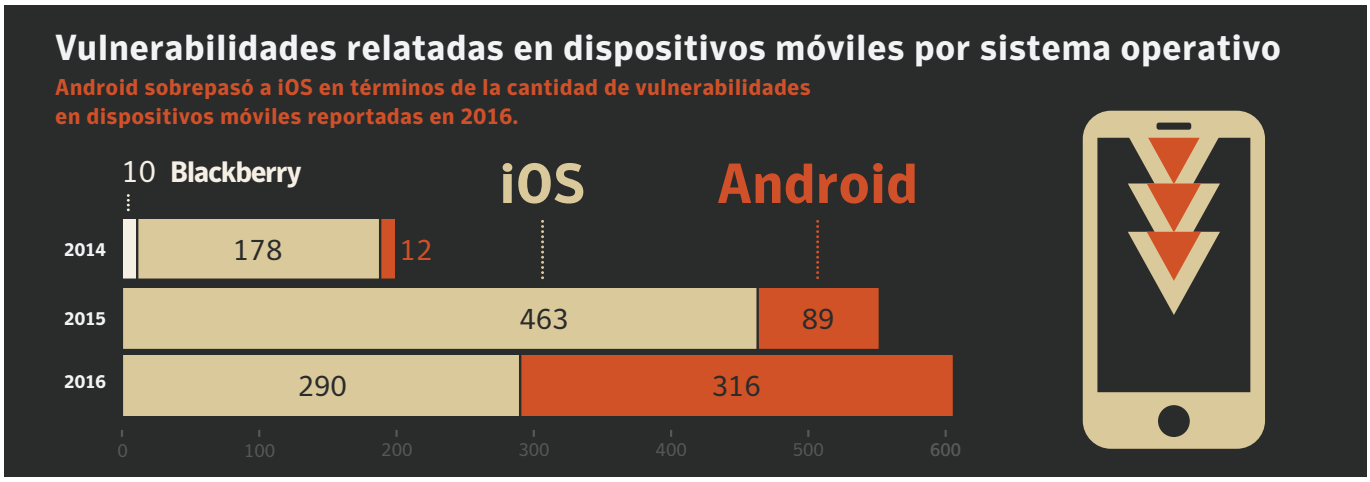
La cifra de aplicaciones de malware y grayware en 2016 alcanzó niveles semejantes en 2016, tras el crecimiento entre 2014 y 2015.



Aumento de empaquetadores en tiempo real

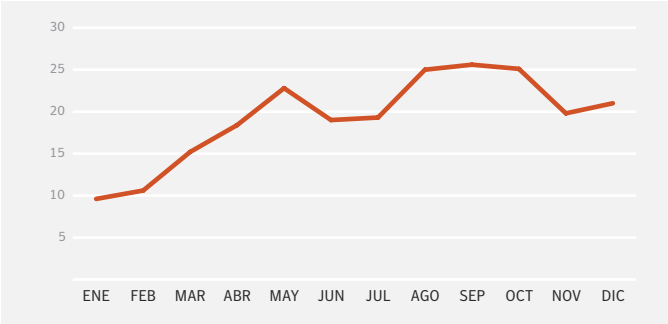
Si bien los grupos de ataque de dispositivos móviles no demuestran innovaciones significativas en los tipos de actividades de amenazas que conducen, están adoptando técnicas que aumentarán las tasas de éxito de infecciones y su longevidad. Los grupos de ataque de dispositivos móviles adoptaron cada vez más el uso de empaquetadores de runtime en un intento de ocultar el malware, una práctica que prácticamente duplicó desde el inicio de 2016 hasta el fin del año.

Los empaquetadores de runtime tornan más difícil la detección de malware y vienen siendo usados por malware tradicional durante varios años. Pueden permitir que una aplicación maliciosa sea recopilada varias veces para que no se detecte como maliciosa, sin embargo en tiempo de ejecución implantará su carga de malware.



Porcentaje de malware para dispositivos móviles en el campo que es empaquetado

Un aumento en el uso de empaquetadores de runtime puede observarse en 2016, con la tasa más que duplicando entre enero y diciembre.



Vulnerabilidades en dispositivos móviles

Un notable cambio en 2016 fue que Android sobrepasó el iOS en términos del número de vulnerabilidades móviles reportadas, un fuerte contraste con los años anteriores, cuando iOS superó Android en esta área. Ese cambio puede ser parcialmente atribuido a mejoras continuas en la seguridad de la arquitectura Android y un interés continuo de los investigadores en las plataformas móviles.

Mejoras en la arquitectura Android

Android ha modificado continuamente su arquitectura para ayudar en mejoras de seguridad. Esto ha impactado a los cibercriminales, dificultándoles la instalación de malware con éxito en los teléfonos. Aun cuando consigan instalar malware en el teléfono de una víctima, varios desarrollos y mejoras en el Android dificultan cada vez más la monetización.

Datos de Symantec muestran que los mensajes de texto premium todavía son una de las formas más eficaces utilizadas por los grupos de ciberataques para obtener dinero con malware en dispositivos móviles. Sin embargo, Android 4.2 (Jelly Bean) incorporó una actualización en 2012 que obstaculizó la operación de troyanos en mensajería de SMS premium, que era utilizada de forma desenfrenada en la época. Con la actualización, el teléfono exhibiría una alerta en caso de que hubiese un intento de enviar un mensaje a un número de teléfono premium, reduciendo considerablemente la eficacia de esos fraudes.

Las restricciones de inicialización automática introducidas en Android 3.1 (Honeycomb) en 2011 también presentaron un reto para los grupos de ataque, pues bloqueaban los recursos de auto-restauración silenciosa, impidiendo que los troyanos iniciasen silenciosamente sin cualquier actividad de front-end. Incluso con la eficacia de estas restricciones, los grupos de ataque también crearon formas de driblar esa restricción.

En otras áreas, las actualizaciones lanzadas pertenecientes a Android 5.0 (Lollipop) y de Android 6.0 (Marshmallow) dificultaron la vida de los grupos de ataque que tratan de implantar malware bancario en dispositivos móviles. El malware bancario en dispositivos móviles funciona a través de overlay de la pantalla, para phishing en la aplicación actualmente en ejecución, pero esas actualizaciones frustraron la capacidad del malware de encontrar la tarea actualmente en ejecución, depreciando a API getRunningTasks(). Desde entonces, los grupos de ataque están determinados a encontrar soluciones alternativas para superar esas medidas adicionales de seguridad.

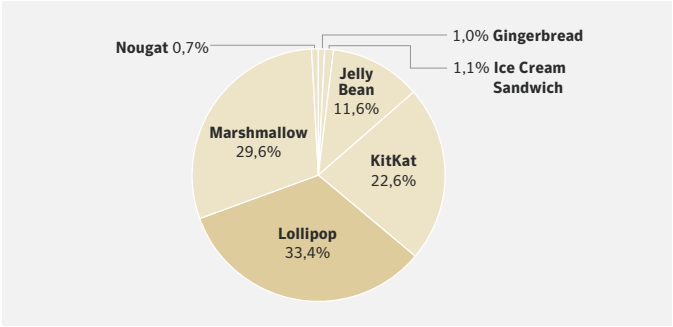
Actualizaciones en Marshmallow también intentaron resolver el problema de ransomware en los dispositivos móviles. Un nuevo modelo de autorizaciones en las actualizaciones dificultó bastante a los responsables del ransomware que tiene como objetivo Marshmallow, lanzar con éxito su malware en un dispositivo, exigiendo que el usuario conceda autorización explícita para que el ransomware bloquee el dispositivo.

Si bien esas actualizaciones y mejoras de seguridad son bienvenidas, las mejoras continuas solamente serán útiles si las personas logran descargar la versión más reciente del Android en sus dispositivos, lo que ni siempre es realidad.

Algunos fabricantes nunca lanzan la versión más reciente del Android para sus smartphones, o existe un gran atraso entre el lanzamiento de la versión más reciente y su disponibilidad para todos. Datos del propio Android muestran que, en el inicio de 2017, la versión más actualizada de su sistema operativo, Nougat, estaba presente en una pequeña parte del mercado, ya que todavía no estaba disponible para la mayoría de los aparatos fuera del ecosistema Google. La próxima versión más actualizada, Marshmallow, tampoco tenía la mayor parte de mercado del sistema operativo, con aproximadamente un 4% por debajo de la versión anterior, Lollipop. La falta de actualizaciones puede crear grandes oportunidades para que los grupos de ciberataques tengan como blanco los sistemas operativos desactualizados en dispositivos móviles.

Participación de mercado de diferentes versiones de Android, enero de 2017

La versión más actualizada del Android, Nougat, tiene apenas un pequeño porcentaje del mercado del sistema operativo.



El predominio de versiones antiguas del sistema operativo demuestra que los grupos de ataque pueden continuar empleando técnicas antiguas, que pueden ser inutilizables en las versiones más actualizadas de SO, para llevar a cabo ataques sin necesidad de innovar.

De alguna manera esto puede explicar la falta de innovación o expansión por parte de los grupos de ataques de dispositivos móviles - tienen un modelo que funciona.

Un sabor amargo para Apple

Aún son relativamente raras las instancias de malware en el iOS. Sin embargo, en agosto de 2016, se descubrió que tres vulnerabilidades de día cero en el iOS, conocidas como Trident, estaban siendo explotadas en ataques dirigidos para inyectar el malware Pegasus en los teléfonos de las víctimas. Pegasus es un spyware que puede acceder a mensajes, llamadas y correo electrónico. También puede recopilar información de aplicaciones como Gmail, Facebook, Skype y WhatsApp.

El ataque funcionaba con el envío de un enlace hacia la víctima por medio de un mensaje de texto. Si la víctima hacía clic en el enlace, a seguir el teléfono estaría desbloqueado y Pegasus podría ingresar e iniciar su trabajo de espionaje.

Las vulnerabilidades que permitieron que ese ataque se produjese incluían una en el WebKit de Safari que le permitía al grupo de ataque invadir el dispositivo si un usuario hacía clic en un enlace, provocaba una fuga de información en kernel y un problema en el cual la corrupción en la memoria de kernel podría desbloquear el dispositivo.

El ataque se descubrió cuando un activista de derechos humanos entregó su teléfono a Citizen Lab, tras recibir un sospechoso mensaje de texto. Las vulnerabilidades parecen haber sido explotadas tan solo en un número limitado de ataques dirigidos.

Pegasus es un spyware desarrollado por el Grupo NSO, una compañía israelense que supuestamente solamente vende su software a gobiernos. Las tres vulnerabilidades fueron corregidas por Apple en el iOS versión 9.3.5.

Este ataque mostró que, aunque son raros los ataques al iOS, el sistema no es infalible.

Mejores prácticas

- Mantenga actualizado su software.
- Absténgase de realizar la descarga de aplicaciones de sitios desconocidos y solamente instale aplicativos de fuentes seguras.
- Preste mucha atención a las autorizaciones solicitadas por apps.
- Instale una aplicación de seguridad móvil adecuada, como Norton, para proteger su dispositivo y los datos.
- Efectúe frecuentes backups de datos importantes.
- Faça backups frequentes de dados importantes.

Nube

Como el uso de la nube por parte de las empresas y los consumidores se ha vuelto la tendencia del momento, ha aumentado naturalmente el interés para los grupos de ataque. Si bien los ataques a la nube aún están en su inicio, 2016 sintió la primera interrupción generalizada de servicios en la nube como resultado de una campaña de denegación de serviço (DoS), y debe servir de aviso sobre cómo los servicios en la nube están sujetos a los ataques maliciosos.

Principales conclusiones

- El uso generalizado de aplicaciones en la nube en las corporaciones, aliado al comportamiento de riesgo de los usuarios que incluso la empresa puede no tener conocimiento, ha ampliado el alcance para los ataques basados en la nube. A fines de 2016, la organización media estaba usando 928 aplicaciones en la nube, un aumento en relación a los 841 en el inicio del año. Sin embargo, la mayoría de los CIOs estima que sus compañías usan apenas aproximadamente 30 o 40 aplicaciones en la nube.
- El análisis de CloudSOC de Symantec descubrió que un 25% de todos los datos relacionados a Shadow IT (datos comerciales almacenados en la nube sin el consentimiento o el conocimiento del departamento de TI de la compañía) son “ampliamente compartidos”, aumentando su riesgo de exposición. 3% de estos datos “ampliamente compartidos” están relacionados a la conformidad de la compañía.
- En 2016, varios ataques y campañas de destaque fueron contra los servicios relacionados a la nube, inclusive los ataques distribuidos de denegación de servicio (DDoS) de Mirai contra el proveedor DNS Dyn y los ataques a las bases de datos Mongo DB alojadas en servicios en la nube.

Tendencias y análisis

Los datos recopilados por CloudSOC de Symantec en los últimos seis meses de 2016 mostraron que está en auge el uso y abuso de aplicaciones y servicios en la nube, así como los datos compartidos y almacenados en los mismos.

El análisis se centró en más de 20.000 aplicaciones en la nube, 176 millones de documentos en la nube y 1.300 millones de correos electrónicos. Se descubrió que la organización media tiene 928 aplicaciones en uso en la nube, un aumento de 87 en relación al número de 841, identificado en el primer semestre de 2016.

Si bien esos números pueden parecer grandes, tenga en mente que una gran variedad de servicios comúnmente usados, como Office 365, Google, Dropbox y Salesforce, son aplicaciones en la nube. De hecho, Office 365, Google y Dropbox fueron consideradas las tres aplicaciones colaborativas más utilizadas y adoptadas con mayor frecuencia en las compañías, tanto en el primero como en el segundo semestre de 2016.

Aplicaciones en la nube más utilizadas en las compañías

La organización común tiene en sus sistemas 928 aplicaciones en uso en la nube, sin embargo la mayoría de los CIOs estima que sus compañías usan apenas aproximadamente 30 o 40 aplicaciones en la nube.

Colaboración	
1S 2016	2S 2016
Office 365	Office 365
Google	Google
Dropbox	Dropbox
Box	Evernote
Evernote	Box
Habilitación de negocios	
1S 2016	2S 2016
Salesforce	GitHub
GitHub	Salesforce
Zendesk	Zendesk
ServiceNow	ServiceNow
Amazon Web Services	Amazon Web Services
Consumidores	
1S 2016	2S 2016
Facebook	Facebook
Twitter	LinkedIn
LinkedIn	YouTube
YouTube	Twitter
Pinterest	Pinterest

una compañía deben usar los servicios en la nube, aumenta el riesgo de uso de las aplicaciones en la nube. Este análisis descubrió que la mayoría de los CIOs estima que sus compañías usan apenas aproximadamente 30 o 40 aplicaciones en la nube, a pesar de la mayoría de las compañías haber adoptado un promedio de 928, una diferencia que supera el 2.000%.

El análisis de CloudSOC de Symantec descubrió que un 25% de todos los datos relacionados a Shadow IT (datos comerciales almacenados en la nube sin la autorización o el conocimiento del departamento de TI de la compañía) son "ampliamente compartidos", es decir, se comparten internamente, externamente y/o con el público.

Incluso más alarmante es que de los 25% de los archivos ampliamente compartidos, un 3% contenían datos relacionados a la conformidad, como Información Personal Identificable (PII), Información de Tarjetas de Pago (PCI) o Información Protegida de Salud (PHI). Si existe una fuga de estos datos confidenciales, puede llevar a significativas multas de conformidad y costos de mitigación para la compañía afectada. Limitar a los funcionarios a usar aplicaciones de uso compartido de archivos seguros y populares, como Office 365 y Box, no puede mitigar completamente los riesgos de esos datos debido al mal uso por parte del empleado o a la invasión deo de la cuenta por hackers. La imposición de prácticas inteligentes de gobernanza de los datos en la nube, como la identificación, categorización y monitoreo del uso de todos los datos de la nube, es esencial para evitar la pérdida de datos.

De forma preocupante, CloudSOC de Symantec descubrió que el 66% de las actividades de riesgo de usuarios en la nube indicaba intentos de exfiltrar datos. Los intentos de exfiltrar los datos se indican por el uso compartido frecuente de cuentas, descargas frecuentes o excesivas y previsualización frecuente de documentos. La previsualización de documentos es un indicio de actividades de exfiltración, pues puede permitir que los grupos de ataque capturen datos. El Análisis Comportamental del Usuario (UBA) es crítico para identificar a los usuarios de riesgo, además de identificar y prevenir exploits, como exfiltración de datos, destrucción de datos e invasión de cuentas.

Negocios de riesgo

El aumento del uso de servicios en la nube por las compañías y sus funcionarios indica que la gobernanza de datos de las empresas está perjudicada y susceptible a fragilidades existentes fuera de la compañía.

Eso puede ser muy serio. El análisis de Symantec descubrió que el 76% de los sitios web contienen vulnerabilidades, de las cuales un 9% son críticas. Esta estadística es explotada con más detalles en el capítulo sobre Ataques Web.

El ataque Dyn, abordado en la sección de IoT en este capítulo, es un ejemplo de un grupo de ataque que tiene como blanco una compañía específica, pero que afectó a los servicios proporcionados por varias empresas, inclusive Amazon Web Services, SoundCloud, Spotify y GitHub. Eso enfatizó los riesgos que corren las empresas al usar los servicios en la nube.

El peligro del ransomware

Una serie de ataques de ransomware contra los servicios basados en la nube demostró la vulnerabilidad de los datos basados en la nube a los ataques de cibercriminales. Un reciente caso de destaque fue cuando decenas de miles de bases de datos de código abierto MongoDB fueron secuestradas y mantenidas como rehenes hasta el pago de rescate. El incidente se produjo luego que las bases de datos MongoDB más antiguas quedaron abiertas, pues los usuarios usaron una configuración estándar.

A pesar de que no hubo ninguna vulnerabilidad en la propia seguridad de MongoDB, y la empresa haya alertado a los usuarios acerca de ese problema, innúmeras implementaciones antiguas que no habían aplicado las mejores prácticas de seguridad permanecieron online, con más de 27.000 bases de datos supuestamente siendo secuestrados. Estos ataques enfatizaron la necesidad de los usuarios a permanecer atentos y asegurarse que cualquier software de código abierto que utilicen sea seguro.

Otro caso, a inicios de 2016, una organización en California ejecutó toda su operación a través de una empresa de soluciones administradas en la nube. Luego de que uno de sus funcionarios abriese un correo electrónico de spam, se descubrió que ninguna persona en la compañía podría acceder a los más de 4.000 archivos almacenados en la nube.

La compañía había sido víctima de ransomware, específicamente TeslaCrypt (Ransom.TeslaCrypt). Afortunadamente, el proveedor de los servicios de la nube mantuvo copias periódicas de seguridad, pero tardó una semana para restaurar los archivos de la empresa. Este es apenas un ejemplo del nivel de interrupción que el ransomware puede causar a las compañías.

IoT y nube: potenciales aliados en el cibercrimen

La prisa de llevar todos y cualquier dispositivo hacia una plataforma online muchas veces deja la seguridad en segundo plano. Eso fue evidente en el caso de CloudPets, animales de peluche conectados a internet. Los CloudPets fabricados por Spiral Toys son mascotas de peluche que permiten que los niños y sus padres puedan intercambiar mensajes grabados a través de Internet. Sin embargo, el investigador Troy Hunt descubrió que la compañía almacenaba datos de clientes en una base de datos MongoDB desprotegida y que era fácil de ser identificada online. Eso expuso más de 800.000 credenciales de clientes, incluso correos electrónicos, contraseñas y más de 2 millones de mensajes grabados. Hunt dijo que, a pesar de que las credenciales fuesen protegidas usando la función de hashing seguro bcrypt, un gran número de contraseñas eran demasiado débiles para que fuese posible descodificarlas.

Este caso ilustra como la combinación de IoT y nube puede poner en riesgo los datos de los clientes. Muchos dispositivos IoT recopilan datos personales y dependen de los servicios en la nube para almacenar esos datos en bases de datos online. Si esas bases de datos no poseen la protección adecuada, entonces la privacidad y la seguridad de los clientes están siendo puestas en riesgo.

Uso de herramientas del día a día

El aumento del uso de servicios en la nube también ayuda a facilitar una tendencia discutida en este informe de grupos de ataque que optan por el "uso de herramientas del día a día", en vez de desarrollar su propia infraestructura de ataque.

Dos de los casos de mayor destaque en 2016, el hackeo de la cuenta de Gmail de John Podesta, jefe de campaña de Hillary Clinton, y el hackeo de la Agencia Mundial Antidoping (WADA) - fueron facilitadas mediante el uso de servicios en la nube. Los grupos de ataque emplearon ingeniería social para adquirir la contraseña de Gmail de John Podesta. Asimismo, los grupos de ataque supuestamente usaron servicios en la nube para exfiltrar los datos robados en lugar de construir una infraestructura personalizada para esa finalidad. Ambos casos de gran destaque son abordados en detalles en el capítulo Ataques Dirigidos.

La nube es atractiva para los grupos de ataque pues, dependiendo de como es usada y configurada, permite que pasen por la seguridad local. Los datos almacenados en la nube pueden ser más fácilmente accesibles a los grupos de ataque que los datos almacenados en los servidores locales. Tener como blanco los servicios en la nube también posibilta que los grupos de ataque causen la máxima interrupción con relativamente poco esfuerzo - como fue visto con el ataque DDoS en el DNS Dyn.

A medida que el uso de los servicios en la nube se vuelve cada vez más común, hace sentido que los ataques a esos servicios también se tornen más frecuentes en el futuro.

Lectura adicional

2S 2016 Informe Shadow Data: Empresas más colaborativas, más seguras y más en la nube que antes

Mejores prácticas

- Excluya cualquier correo electrónico de apariencia sospechosa que reciba, especialmente si incluyen enlaces o archivos adjuntos.
- Desconfíe de cualquier archivo adjunto de correo electrónico del Microsoft Office que aconseje a habilitar macros para exhibir su contenido. A menos de que esté absolutamente seguro de que este es un correo electrónico genuino de una fuente segura, no active macros y, en vez de eso, excluya inmediatamente el correo electrónico.
- Cuidado con las actualizaciones o parches emitidos para cualquier software de código abierto que utiliza. Las actualizaciones de software incluirán frecuentemente parches para vulnerabilidades de seguridad recientemente descubiertas que podrían ser explotadas por grupos de ataque.
- Asegúrese que el servicio que utiliza en la nube efectúe regularmente backup de sus archivos, para garantizar que pueda sustituirlos si se torna una víctima de ransomware.
- Implemente prácticas inteligentes de gobernanza de datos en su compañía para que pueda saber qué datos de negocios están siendo almacenados en los servicios en la nube.

Créditos

Equipo

Kavitha Chandrasekar
Gillian Cleary
Orla Cox
Hon Lau
Benjamin Nahorney
Brigid O Gorman
Dick O'Brien
Scott Wallace
Paul Wood
Candid Wueest

Colaboradores

Shaun Aimoto
Tareq AlKhatib
Peter Coogan
Mayee Corpin
Jon DiMaggio
Stephen Doherty
Tommy Dong
James Duff
Brian Fletcher
Kevin Gossett
Sara Groves
Kevin Haley
Dermot Harnett
Martin Johnson
Sean Kiernan
Bhavani Satish Konijeti
Gary Krall
Richard Krivo
Yogesh Kulkarni
Matt Nagel
Gavin O'Gorman
John-Paul Power
Nirmal Ramadass
Rajesh Sethumadhavan
Ankit Singh
Tor Skaar
Dennis Tan
Suyog Upadhye
Parveen Vashishtha
William Wright
Tony Zhu

Acerca de Symantec

Symantec Corporation (NASDAQ: SYMC) es líder mundial en soluciones de ciberseguridad y ayuda a las compañías, gobiernos e individuos a proteger sus datos más importantes en cualquier lugar. Compañías en todo el mundo buscan a Symantec para soluciones estratégicas e integradas para defenderse contra ataques sofisticados en endpoints, en la nube e infraestructura.

Del mismo modo, una comunidad global de más de 50 millones de personas y familias dependen de la suite de productos Norton de Symantec para protección en casa y en todos sus dispositivos. Symantec opera una de las redes civiles de ciberinteligencia más grande del mundo, lo que le permite ver y proteger contra las amenazas más avanzadas.

Más información

Site Global da Symantec: http://www.symantec.com

ISTR e Symantec Intelligence Resources: https://www.symantec.com/security-center/threat-report

Symantec Security Center: https://www.symantec.com/security-center

Norton Security Center: https://us.norton.com/security-center

Symantec

Sede Mundial de Symantec
350 Ellis Street
Mountain View, CA 94043
USA

+1 650 527–8000
+1 800 721–3934

Symantec.com

Copyright © 2017 Symantec Corporation.

Todos los derechos reservados. Symantec, el logo de Symantec y el logo de Checkmark son marcas registradas o marcas comerciales registradas de Symantec Corporation o de sus subsidiarias en EE.UU. e outros países. Otros nombres pueden ser marcas registradas de sus respectivos propietarios.

Para escritorios regionales y números de contacto específico, por favor acceda a nuestra página web. Para obtener más información sobre los productos en los Estados Unidos, llame al número de teléfono gratuito (800) 745 6054.

04/17