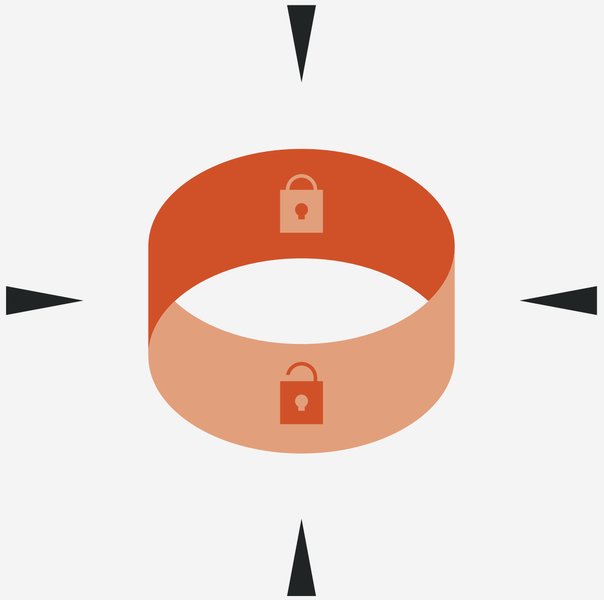
TARGETED RANSOMWARE:

An ISTR Special Report

Authors: Dick O'Brien, Jon DiMaggio, and Hoang Giang Nguyen

Contents



INTRODUCTION

Ransomware continues to be one of the most dangerous cyber crime threats facing any organization. While ransomware remains highly prevalent, the nature of the threat has changed markedly over the past two years and enterprises are increasingly being targeted by ransomware groups.

During 2018, while the overall number of ransomware infections was down 20 percent, attacks against organizations were up by 12 percent. Enterprises last year accounted for 81 percent of all ransomware infections.

However, within that statistic there is another, more worrying trend. Over the past year the number of targeted ransomware attacks has multiplied as new players move into this sector. Although targeted ransomware attacks account for a small percentage of overall ransomware attacks, they present a far greater risk. A successful targeted ransomware attack could cripple an ill-prepared organization.

In some cases, hundreds of computers have been encrypted, backups have been destroyed, and business-critical data has been put beyond reach. Such attacks can effectively shut down the affected organization, leading to loss of business, reputational damage, and multimillion-dollar clean-up bills.

For several years, targeted ransomware was spoken about as a largely theoretical threat. There was only one established targeted ransomware gang (SamSam) operating. However, during 2018 SamSam was joined by another highly active targeted operation (Ryuk), while 2019 has seen the arrival of several new groups who have been linked to a series of highly disruptive attacks in the U.S. and Europe.

Current trends indicate that targeted ransomware is attracting a high degree of interest among cyber criminals, with new groups appearing at an accelerating pace, motivated no doubt by the success of some recent attacks.

Organizations need to make themselves aware of the threat posed by targeted ransomware attacks and ensure that they have robust defenses in place to deter attackers.

Targeted Ransomware
THE GROWING MENACE

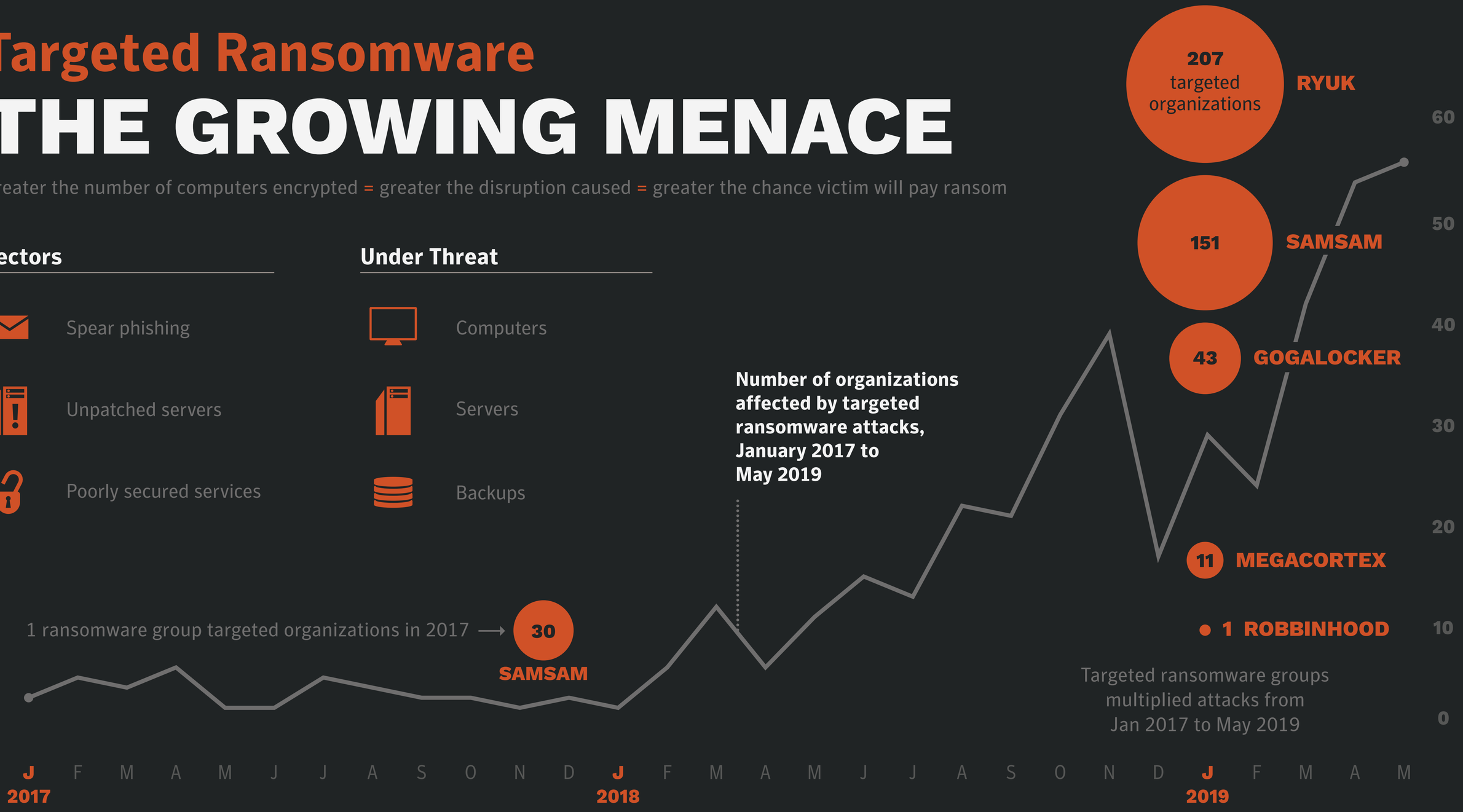
Greater the number of computers encrypted = greater the disruption caused = greater the chance victim will pay ransom

Vectors

- Spear phishing
- Unpatched servers
- Poorly secured services

Under Threat

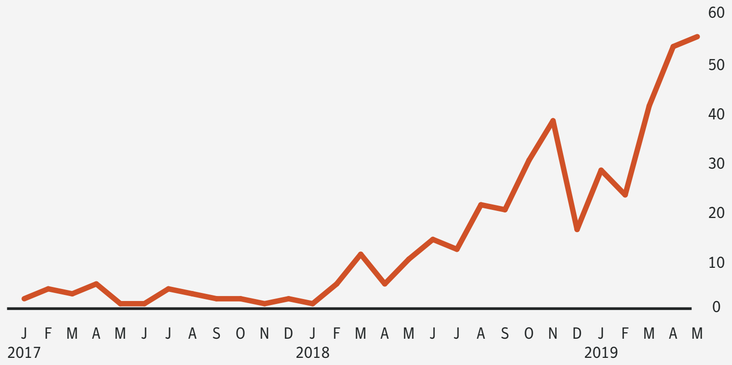
- Computers
- Servers
- Backups



Targeted ransomware trends

The number of organizations affected by targeted ransomware attacks has grown sharply over the past two and a half years. As recently as January 2017, Symantec observed as little as two organizations a month being attacked. However, recent months have seen that figure grow to above 50 organizations a month.

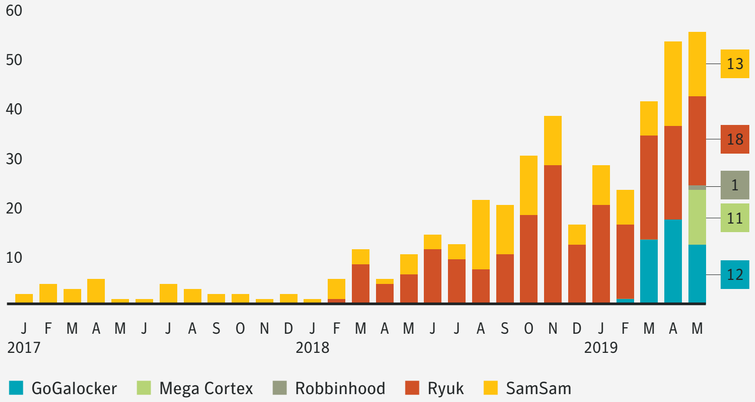
Figure 1. Number of organizations affected by targeted ransomware attacks, January 2017 to May 2019



The true number of targeted ransomware attacks may be higher. Our statistics are based on telemetry for five ransomware families reported to have been used in targeted attacks: SamSam (Ransom.SamSam), Ryuk (Ransom.Hermes), GoGalocker, aka LockerGoga (Ransom.GoGalocker), MegaCortex (Ransom.MegaCortex), and RobbinHood (Ransom.Robbinhood).

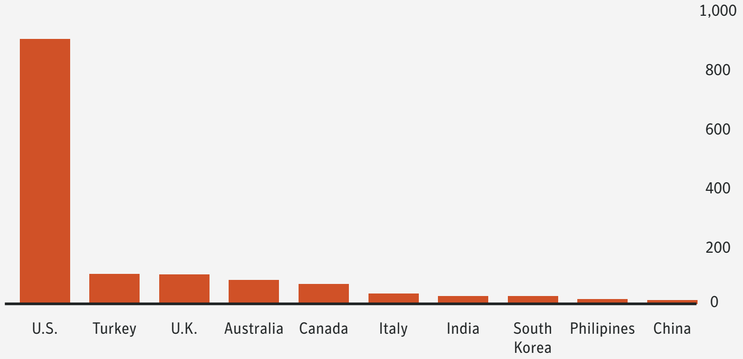
There are a number of other ransomware families, most notably Crysis, aka Dharma, (Ransom.Crysis) and GandCrab (Ransom.GandCrab), which have been used in targeted attacks, but have also been spread using traditional infection vectors such as spam campaigns. The overall number of organizations affected by Crysis and GandCrab dwarfs those affected by the other five families, but there is no way of establishing how many were infected by targeted attacks and how many were infected through other means.

Figure 2. Number of organizations affected by targeted ransomware attacks, by family, January 2017 to May 2019



When the statistics are broken down by ransomware family, it becomes evident that until early 2018, SamSam was the only ransomware family being used exclusively in targeted attacks. Ryuk arrived in early 2018 and, in almost every month since its appearance, has been more active than SamSam. GoGalocker, MegaCortex, and RobbinHood are all relatively recent arrivals and, having mounted a number of highly disruptive attacks, are already making an impact on the overall statistics.

Figure 3. Number of organizations affected by targeted ransomware attacks by country, January 2017 to May 2019



In terms of regional breakdown, the U.S. is by far the worst affected by targeted ransomware attacks, with almost 900 U.S. organizations hit between January 2017 and May 2019. A significant factor behind this trend is the fact that the long-running SamSam group heavily focused on the U.S. Turkey is a distant second, with just over 100 organizations affected, followed by a number of Anglophone countries: the U.K., Australia, and Canada.

Targeted ransomware families

The number of ransomware families being used in targeted attacks has multiplied in recent months. There are now at least five distinct families being used in an exclusively targeted fashion: SamSam, Ryuk, GoGalocker, MegaCortex, and RobbinHood.

Two further families, Crysis and GandCrab, have also reportedly been used in targeted attacks but have also been deployed in indiscriminate campaigns involving distribution through spam emails or exploit kits.

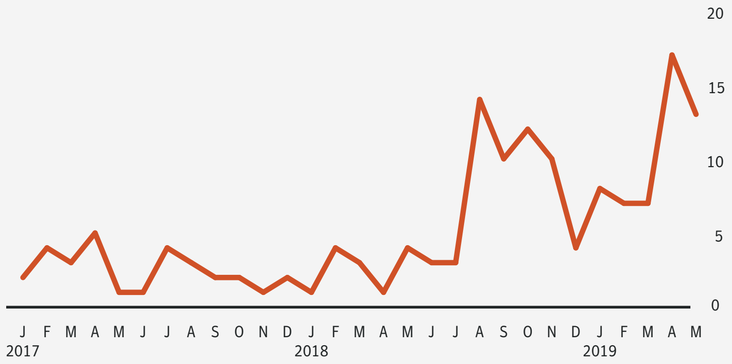
SamSam

SamSam is regarded as the original targeted threat and, for some time, was the only known cyber crime group mounting targeted ransomware attacks.

The group is heavily focused on targets in the U.S. While it has hit organizations across a range of sectors, healthcare in particular has been heavily affected, accounting for around a quarter of all attacks in 2018. SamSam has also hit a number of local government organizations, and was believed to be behind the attack on the city of Atlanta in March 2018, which saw numerous municipal computers encrypted. The clean-up costs for the attack are expected to run to over $10 million.

The group was also linked to the attack on the Colorado Department of Transportation, which resulted in clean-up costs of $1.5 million.

Figure 4. Organizations affected by SamSam attacks, January 2017 to May 2019

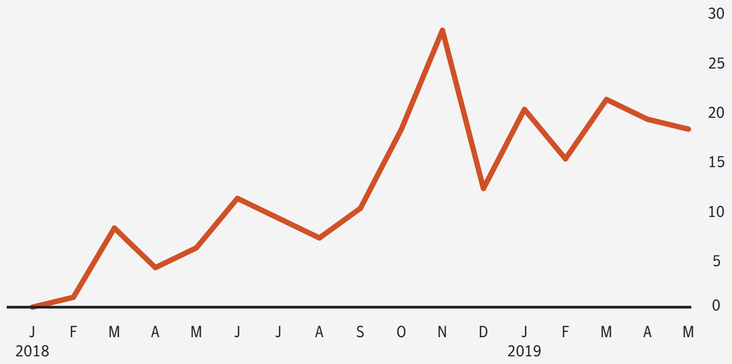


In November 2018, two Iranian nationals were indicted in the U.S. for their alleged involvement in SamSam attacks. The FBI estimated that the SamSam group had received $6 million in ransom payments to date and caused over $30 million in losses to victims. The indictment appears to have had little or no impact on SamSam activity. The number of organizations affected by SamSam attacks fell in November and December 2018, but the group's activity levels increased again in 2019.

Ryuk

Ryuk is regarded as an evolution of the older Hermes ransomware. Hermes first appeared in 2017, while the Ryuk variant began circulating during 2018. Since August 2018, Ryuk has been seen mounting targeted campaigns against enterprises, encrypting hundreds of computers and servers before demanding a ransom of between 15 and 60 bitcoins.

Figure 5. Organizations affected by Ryuk attacks, January 2018 to May 2019

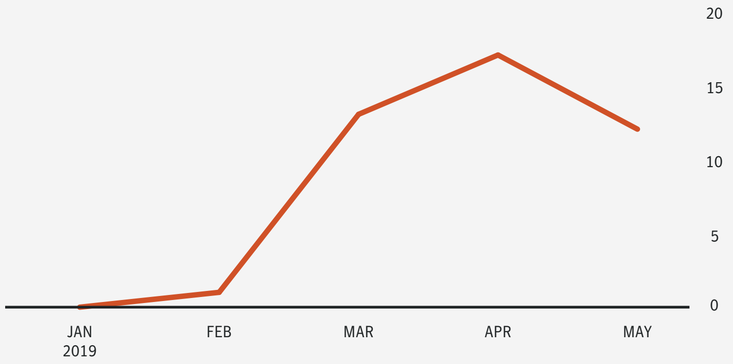


Ryuk came into the public spotlight in December 2018 when it was linked to a major ransomware attack against Tribune Publishing, which handles printing operations for numerous U.S. newspapers. Printing of several titles was disrupted by the attack.

GoGalocker

GoGalocker first appeared in January 2019 and has been used in attacks against organizations in a wide range of business sectors. While the U.S. has been the worst affected, a large number of organizations in Scandinavia have also been hit with attacks. For more details on this threat, see the "In depth: GoGalocker" section.

Figure 6. Organizations affected by GoGalocker attacks, January 2019 to May 2019



MegaCortex

MegaCortex is one of the newest targeted threats to begin operating, first appearing in May 2019, when it was used against 11 organizations. The malware has some similarities to GoGalocker, indicating that they may have common authorship. While it is possible the two groups of attackers are linked, it may also be the case that the ransomware was developed by the same third-party developer for both groups. For more details on this threat, see the "Spotlight: MegaCortex" section.

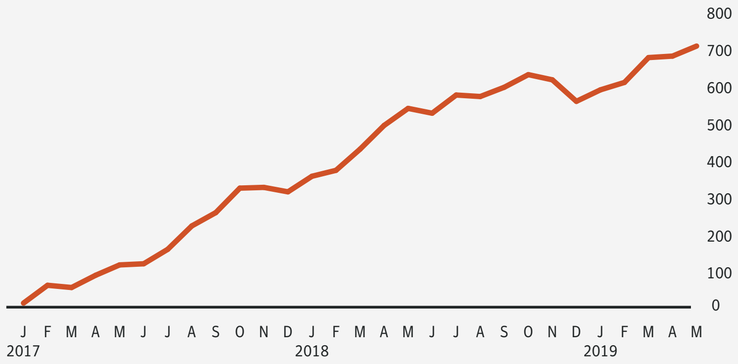
RobbinHood

RobbinHood is another new family, first appearing in May 2019.
It was reportedly used in the attack against the U.S. city of Baltimore.

Crysis (aka Dharma)

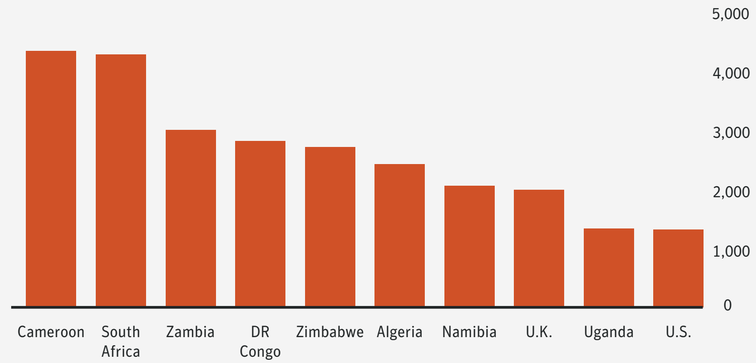
Crysis has been circulated since 2016 and is a highly prevalent threat, which is spread through multiple infection vectors. While it has been regularly involved in targeted attacks leveraging poorly secured Remote Desktop Protocol (RDP) services, it has also reportedly been spread through spam campaigns, which probably accounts for the high number of attacks relative to other threats.

Figure 7. Organizations affected by Crysis attacks, January 2017 to May 2019



One interesting feature of Crysis attacks is that organizations in Africa account for the most attacks, with eight of the top ten countries located there.

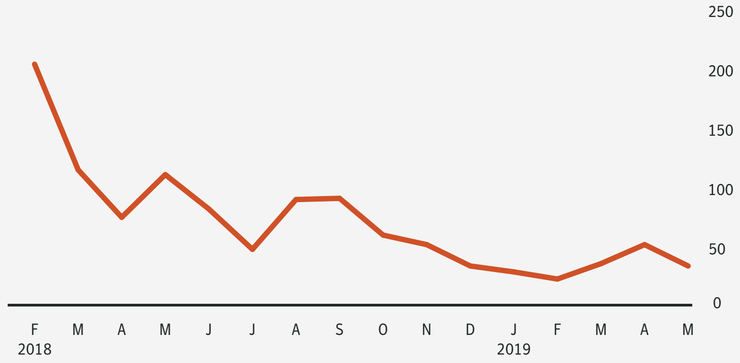
Figure 8. Number of organizations by country affected by Crysis attacks, January 2017 to May 2019



GandCrab

Like Crysis, GandCrab has been a prolific ransomware threat since it first appeared in January 2018. While it has been deployed in targeted attacks, the ransomware has also been mass distributed. This variation in attack pattern is likely due to the fact that GandCrab reputedly operates as a ransomware-as-a-service, meaning the operators rent the ransomware out to other groups for use in attacks.

Figure 9. Organizations affected by GandCrab attacks, February 2018 to May 2019



In early June 2019, GandCrab announced that it had decided to shut down its operation. The announcement came after a notable drop-off in activity in late 2018 and early 2019. The gang claimed to have seen more than $2 billion paid out in ransoms, with the operators themselves claiming to have made around $150 million a year. The veracity of these claims has yet to be established.

Infection vectors

While most ordinary ransomware families rely heavily on spam email campaigns (and up until very recently, exploit kits) for distribution, targeted threats are usually spread using different methods. Because of the relatively low prevalence of targeted ransomware attacks, the infection vector can often be difficult to establish.

Several different attack methods have been observed to date and targeted ransomware groups often take their cues from espionage groups in their methods for gaining a foothold on the victim's network.

Spear phishing

A frequently used and highly effective method for getting inside a targeted organization's network. The attackers will send emails to selected employees, often disguised as work-related correspondence. For example, someone working in the energy industry could be sent an invitation to an energy conference.

Spear-phishing attacks usually require an element of social engineering to trick the victim into opening the email. The content will need to be relevant to the recipient and contain enough of a "lure" for them to either open an attachment or follow a link within the body of the email. If the ruse works, malware will be downloaded to the victim's machine, allowing the attackers to begin moving across the victim's network.

Vulnerability exploitation

A number of targeted ransomware groups have been seen targeting vulnerable software running on public-facing servers in order to gain access to an organization's network. In most cases, the attackers exploit known vulnerabilities in unpatched software, such as JBoss or Apache web server.

Groups known to use this tactic include SamSam, which has reportedly used freely available tools to find and exploit vulnerabilities.

Poorly secured services

In some cases, attackers don't need to exploit a vulnerability in order to access a public-facing computer. There are several instances of attackers compromising poorly secured services. For example, Crysis has repeatedly been observed attacking organizations through poorly secured RDP services, taking advantage of leaked or weak credentials.

GandCrab meanwhile was recently seen scanning the internet for exposed MySQL databases that it was then infecting with malware.

Secondary infections

One possible infection vector is via other malware families. In one case involving GoGalocker, Symantec observed gambling malware on the victim's network several days prior to the attack. It is possible that this malware could have been used to deliver GoGalocker, but we have found no further evidence in support of this hypothesis.

Lateral movement

One of the key phases in any targeted ransomware attack is lateral movement. The goal of most attackers is to identify and encrypt as many computers on the victim's network as possible. The larger the proportion of infected computers, the greater the disruption. This increases the chances of the victim paying the ransom, particularly if the attackers identify and encrypt backups and important servers.

Recent targeted ransomware attacks have seen attackers deploy a wide array of tactics and tools in order to perform lateral movement. Ransomware tends to mimic the tactics used in targeted attacks, where use of custom malware is kept to a minimum. Instead, attackers tend to rely on a mix of publicly available hacking tools, commodity malware, and "living off the land" tactics—malicious use of operating system features and administration tools.

The most frequently used include:

PowerShell: Microsoft scripting tool that was used to run commands to download payloads, traverse compromised networks, and carry out reconnaissance.

PsExec: Microsoft Sysinternals tool for executing processes on other systems. The tool was primarily used by attackers to move laterally on the victim's network.

PsInfo: Another Microsoft Sysinternals tool that allows the user to gather information about other computers on the network.

Mimikatz (Hacktool.Mimikatz): Freely available tool capable of changing privileges, exporting security certificates, and recovering Windows passwords in plaintext depending on the configuration.

PuTTY: A command-line utility used to create SSH sessions.

In depth: GoGalocker

GoGalocker is one of a new breed of targeted ransomware threats to appear in early 2019. In quick succession, the ransomware was deployed in targeted attacks against a range of organizations, causing serious disruption for several of its victims.

The attackers behind GoGalocker appear to be highly skilled, capable of breaking into the victim's network and deploying a wide array of tools in order to map the network, harvest credentials, elevate privileges, and turn off security software before deploying the ransomware.

Attack preparation

Once the GoGalocker attackers gain a foothold on the victim's network, they turn their attention to mapping out the network and acquiring credentials that would permit them to access other machines and escalate their user privileges.

In order to begin this process, the attackers issue two Base64-encoded PowerShell commands designed to dynamically compile and run shellcode in memory. The attackers employ popular techniques to leverage resources in the victim's environment. These PowerShell commands issue a call on legitimate Windows resources—VirtualAlloc and CreateThread—which are functions called on by the Windows Native API and can be used to set up and run shellcode. These commands are used to download and run two pieces of shellcode on the computer:

1. **A listener shellcode:** Once executed, this shellcode opens TCP port 9899 and listens for additional code or commands.
2. **A downloader shellcode:** This shellcode acts as a downloader. Once run, a connection is made to attacker-controlled infrastructure (https://89[.]105[.]202[.]58/sMNN) and second- stage shellcode is downloaded.

Once compiled, the second-stage shellcode provides functionality similar to the commodity tool Cobalt Strike Beacon Reflective Loader, which is used to communicate (beacon) with the attacker. Symantec has seen two variants of this second-stage shellcode. Both provide the same functionality, but each connects to a different command and control server (89.105.198.21 or 89.105.202.58).

Aside from PowerShell, the attackers deploy a range of other tools on the victim's network. These include:

PuTTY: A command-line utility used to create SSH sessions.

Mimikatz: A freely available tool capable of changing privileges, exporting security certificates, and recovering Windows passwords in plaintext depending on the configuration.

Wolf-x-full: A multi-purpose tool described by its developers as "an all-in-one way to manage and gather information from your computer." Features include:

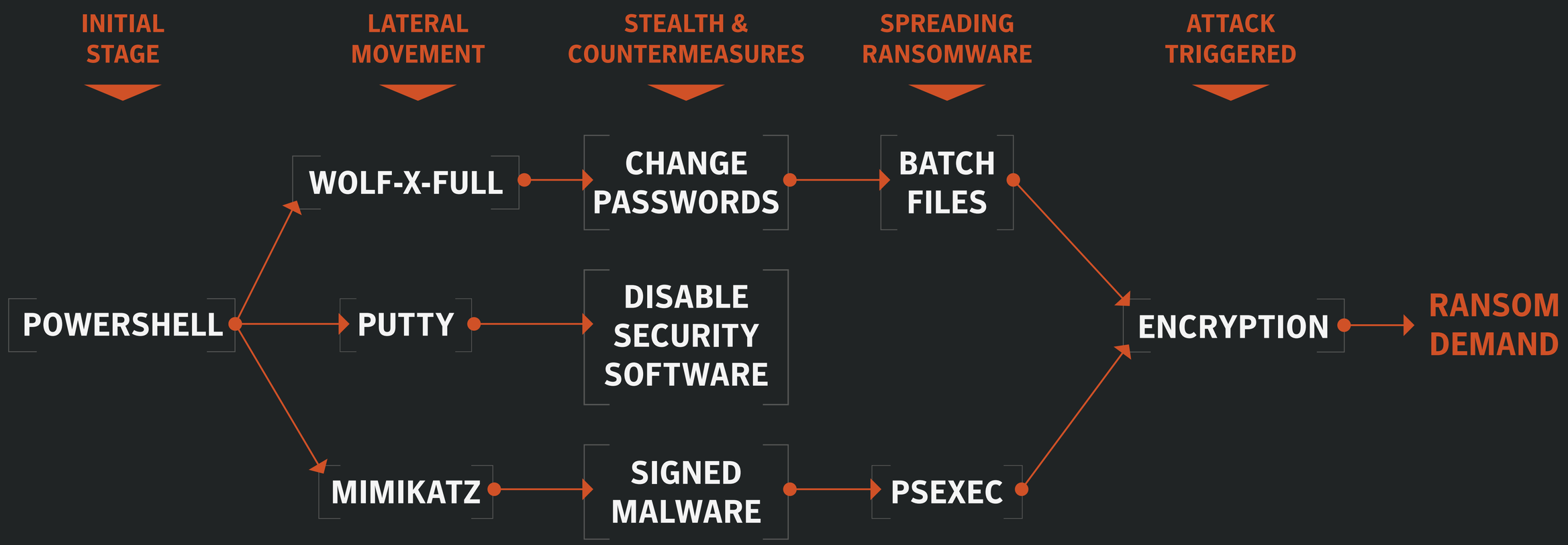
- Remote CLI access
- Enable\disable Windows User Account Control (UAC)
- Enable\disable UAC remote restrictions
- Enable\disable Windows Firewall
- Get external IP address
- View installed programs (and uninstall)
- Display local and domain groups and users, including security identifier numbers (SIDs)
- Query a range of remote machines for basic information

Used together, all these tools allow the GoGalocker attackers to both map the victim's network and steal credentials for administrator and privileged accounts. This process permits the attackers to identify and access a large number of computers in order to later simultaneously infect them with the ransomware.

GoGalocker

NEW BREED OF TARGETED THREAT

Attack Process



Disabling security software

One of the reasons the GoGalocker attackers are often so effective is that they usually disable security software before installing the ransomware. This is not because of any innate weakness or vulnerability in the security software it disables, rather that the group uses stolen administrator credentials to turn the software off or uninstall it.

The infection process

Once the attackers finish mapping the network and obtaining credentials, they turn their attention to spreading the ransomware across many computers and servers.

In several attacks, the attackers used batch files prior to execution of the ransomware. For example, in one attack, the batch files shown in Table 1 were used.

Table 1. Batch files used in a GogaLocker attack

BATCH FILE	COMMAND
copybats2.bat	start copy x[xx].bat \\[IP]\c$\windows\temp\
copyPsExec2.bat	start copy PsExec.exe \\[IP]\c$\windows\temp\
kill.bat	iisreset /stop c:\windows\temp\taskhost.exe
startbats2.bat	start psexec.exe \\[IP] -u [USER] -p [PASSWORD] -d -h -r mstdc -s -accepteula -nobanner c:\windows\temp\x[xx].bat

One of these batch files—copyPsExec2.bat—was used to copy PsExec to computers on the network. PsExec is a Microsoft Sysinternals tool used for executing processes on other systems. It is frequently used in attacks involving living off the land tactics.

In several cases involving batch files, the attackers used the aforementioned Wolf-x-full tool, in between running the files. Wolf-x-full is usually used to check if a computer was a virtual machine, gather system and network information, check who was logged into the computer, and possibly change the password policy. What the attackers were using it for in these cases is unclear.

The attackers were also seen running additional commands from a command prompt. In the example below, the attackers copy a bat file from one computer to another on the network. The file starts specified attacker-associated services and terminates a number of other services on the infected computer. They then change the local username and password on the infected computers and then start a number of attacker-selected processes and kill others. They also use PsExec.exe to execute a bat file on a list of remote computers with a hard-coded username and password. With this command it is also set to accept any EULA prompts and hide any banner that could alert the victim something was going on.

```
cmd.exe /c copy \\163.34.89.13\c$\windows\temp\kill.bat CSIDL_WINDOWS\
temp
start wmic /node:"[IP]" /user:"[USER]" /password:"[PASSWORD]" process
call create "cmd.exe /c c:\windows\temp\kill.bat"
start copy x[xx].bat \\[IP]\c$\windows\temp\
start psexec.exe \\[IP] -u [USER] -p [PASSWORD] -d -h -r mstdc -s
-accepteula -nobanner c:\windows\temp\x[xx].bat
```

Encryption

The next stage of the attack is to begin encrypting files on computers with the GoGalocker ransomware. GoGalocker encrypts all files on an infected computer with the exception of files in the C:\Windows\ directory. The file extension .locked is appended to all encrypted files, e.g. file.doc.locked. Furthermore, GoGalocker will also encrypt the Windows boot manager in order to prevent the computer from booting if restarted.

The last step the attackers take is to log off the current user. In at least one case, the attackers changed local user and administrator passwords using a net.exe command. The likely motive for this was to prevent anyone from logging in and halting the encryption process.

Interestingly, net.exe, the tool used to change the local user and administrator passwords, did not include the /domain password reset command line switch, which would have prevented the victim from being able to log into the system from an Active Directory /domain account. It is possible that the attackers believed the active directory servers would not be available. Alternatively, its absence could be an oversight on the part of the attackers.

Another interesting finding was the differing time frames between the compilation of the GoGalocker ransomware and later deployment on victim networks. The evidence to date suggests that the group appears to develop a fresh variant of the ransomware for use in each new attack. The time frame between compilation and deployment ranges from within 24 hours to several weeks.

Figure 10. Times between sample compilation and deployment

Signed malware

Another tactic the GoGalocker gang uses to avoid detection is to digitally sign its ransomware with legitimate certificates. Most of the GoGalocker samples seen by Symantec were signed with one of three certificates:

CN=ALISA LTD:

- **Origin:** https://www.virustotal.com/gui/file/eda26a1cd80aac1c42cdbba9af813d9c4bc81f6052080bc33435d1e076e75aa0/detection
- **direct download:** https://abuse.io/lockergoga/5DA173EB1AC76340AC058E1FF4BF5E1B.crt

CN=MIKL LIMITED:

- **Origin:** https://www.virustotal.com/gui/file/bdf36127817413f625d2625d3133760af724d6ad2410bea7297ddc116abc268f/detection
- **direct download:** https://abuse.io/lockergoga/3d2580e89526f7852b570654efd9a8bf.crt

CN=KITTY'S LTD:

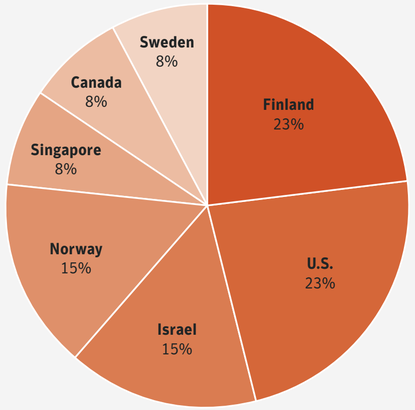
- **Origin:** https://www.virustotal.com/gui/file/47f5a231f7cd0e36508ca6ff8c21c08a7248f0f2bd79c1e772b73443597b09b4/detection
- **direct download:** https://abuse.io/lockergoga/378d5543048e583a06a0819f25bd9e85.crt

Victims

Since emerging at the beginning of 2019, GoGalocker has attacked organizations across a broad range of industry sectors, including: computer services, accountancy and auditing, consultancy, financial services, power tools, building and construction, financial services, publishing, printing, metals, and warehousing and storage.

While attacks have occurred worldwide, a high number of victims to date have been located in Scandinavia, including Finland (23 percent), Norway (15 percent), and Sweden (8 percent). Many of these attacks were directed at local companies, although some were attacks against Scandinavian offices of multinational firms. Why the GoGalocker group has focused heavily on Scandinavia remains unknown.

Figure 11. Location of organizations affected by GoGalocker attackers



Infection vector

How GoGalocker first gets onto the victim's network remains unknown. Symantec has identified three possible scenarios, although we have found no strong evidence to support any:

- **Spear phishing:** Commonly used in these kinds of targeted attacks, but no evidence to date that GoGalocker has used spear phishing.
- **Remote Desktop Protocol:** A third-party report has indicted RDP was leveraged as an infection vector, but Symantec has seen no evidence to confirm this.
- **Gambling malware:** Symantec observed gambling malware on the network of one victim, around 10 days prior to an attack. It is possible that this malware could have been used to deliver GoGalocker tools, but we have found no further evidence.

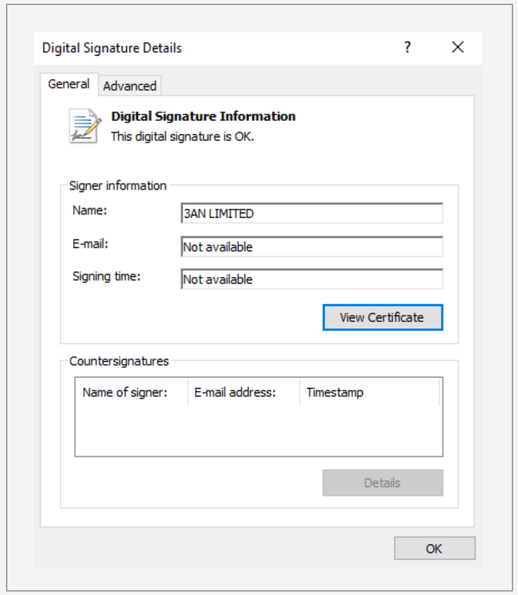
Spotlight: MegaCortex

MegaCortex is another example of the new breed of targeted ransomware threats that have begun to multiply in 2019. The ransomware first appeared in May 2019, when it was used in attacks against organizations in the U.S., South Korea, Italy, Israel, and the Netherlands.

Main executable

MegaCortex uses some of the detection evasion techniques seen in other families of targeted ransomware. For example, its main executable is signed with a valid certificate, but this certificate has already been revoked. However, if a computer hasn't updated its revoked certificate database, the certificate will still be effective.

Figure 12. Example of computer that has not updated its revoked certificate database. The signed certificate used by MegaCortex is still classed as valid



The main executable is embedded with another two DLL binaries. Both binaries are encrypted with AES-128-GCM. Once executed, MegaCortex tries to decrypt these binaries and load them dynamically by itself.

At this step, MegaCortex uses another evasion technique to prevent it from being detected in sandboxes. The malware requires a valid argument, which is a Base64 string, then combines it with another value that is calculated from the system time on the infected computer to extract an AES key and initialization vector (IV) for the next stage of decryption. The AES key and IV are generated as pseudo-code, as shown here:

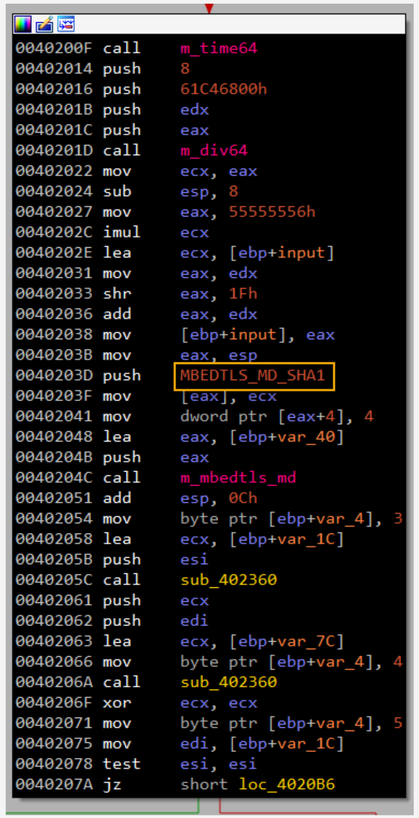
```
def get_aes_params():
  pre_key = base64_decode(argv[1])

# 0x861C46800 is number of ticks in an hour
t = time() / 0x861C46800 / 3
hash_key = sha1_hash(t)

for i in range(0x10):
  aes_key[i] = pre_key[i] ^ hash_key[i]
for i in range(0x0C):
  aes_iv[i] = pre_key[is+0x10] ^ hash_key[i]
```

Then, MegaCortex will use the AES key and IV to decrypt embedded binaries using the AES-128-GCM algorithm in the mbed TLS library.

This technique enables the attackers to create a session time for input. The ransomware could fool a sandbox into thinking it is benign unless it is run for a valid time period. For the sample analyzed by Symantec, the session time for input was three hours. However, we are also aware of other MegaCortex samples that had a one-hour session time.

Employing this technique doesn't, in any way, limit the attackers' freedom to operate, since they already know the AES key and IV and can generate an input argument any time they want.

Figure 13. How the AES key and IV are calculated from input and time value on a victim's computer



Main payloads

The first of the two binaries extracted is named payload.dll and is the main module of the ransomware. This DLL file exports two functions: start and start2.

The second binary is named injecthelper.dll. This exports the function _command@16.

After the two binaries are successfully decrypted, MegaCortex attempts to load payload.dll directly to memory before finding the address of the "start" function and calling it. The start function has the following capabilities:

- Checks if MegaCortex is running under an administrator account. If not, it attempts to elevate the main executable to administrator privileges using the API ShellExecuteEx with the parameter "runas".
- Disables Wow64 redirection
- Tries to adjust tokens:
  - SeDebugPrivilege
  - SeBackupPrivilege
  - SeRestorePrivilege
  - SeTakeOwnershipPrivilege
- Performs the pre-setup activity for encryption and loading injecthelper.dll through rundll32.exe to start encryption on the infected computer.
- After encryption is finished, it enumerates all drives and can execute the following commands (except on CD-ROM drives):
  - vssadmin.exe delete shadows /all /for=%drivepath%
  - cipher.exe /w:%drivepath%

Second stage: Pre-setup for encryption

MegaCortex prepares data for encryption by performing the following actions:

- Removes C:\\lc_vagsi.log if it is present.
- Creates an IPC shared memory region by the module interprocess in the Boost library. This shared memory has the name: lc_vagsi and is used to:
  - Work as a queue list with the full paths of files that MegaCortex has scanned on the infected computer. These files will then be encrypted.
  - Store a master AES key and IV, which are generated after scanning. This master AES key will be used to encrypt another AES key that is generated during the encryption stage to encrypt files.

- To collect files to encrypt, MegaCortex does the following:
  - Recursive scan of all logical drives and directories except %Windir% (although it will still scan %Windir%\temp).
- Filters the following file names and extensions from encryption:
  - .dll, .exe, .sys, .mui, .tmp, .lnk, .config, .manifest, .tlb, .olb
  - .bat, .cmd, .ps1
  - lc_vagsi.tsv, lc_vagsi.log in C:\\
  - desktop.ini
- Copies the first ransom note to C:\\!!!_READ_ME_!!!.txt
- Generates a random master AES key and IV (mentioned above) and a junk buffer. All three are encrypted using RSA and saved to C:\lc_vagsi.tsv.
- Stores information on encrypted files in lc_vagsi.tsv. This file is used to perform decryption.
- The RSA public key used is:
  - Public-Key: (4096 bit)
    Modulus:

```
00:ba:c1:7e:ac:19:c1:b6:0e:2d:a8:37:9f:
38:a3:25:36:66:8b:8a:d0:2d:73:74:57:a4:f2:b5:be:
a9:73:5f:8b:37:f6:9c:55:d8:39:e0:75:70:52:cc:
95:a5:7c:72:4c:ac:3a:ce:ea:b6:68:42:dd:57:71:bc:
68:7f:51:47:13:82:98:bc:fa:14:0c:12:83:18:a2:
1e:af:19:9b:92:c5:1f:e4:70:e2:87:64:5f:6f:75:
e:f2:ac:4b:bb:1c:07:dd:41:22:ac:07:9d:b4:3e:
43:4e:cc:f2:88:26:c4:00:9c:cd:7d:72:21:20:87:
b:89:05:65:af:f0:9e:a3:51:6d:a2:0b:36:a2:8a:
b8:ee:2b:49:92:99:7d:06:29:e8:4f:13:11:6a:58:
d:0b:be:d9:59:19:21:dd:12:21:c7:bb:9e:fe:65:
4d:9c:54:4c:b0:30:dd:5a:ff:fc:30:92:76:bc:d3:
9:ba:06:c4:27:27:04:47:b4:d6:16:ff:9a:36:8b:28
:d0:3a:ad:30:76:2b:1d:1b:78:89:c2:00:28:6d:
a1:c3:2e:f6:18:5c:31:6e:16:a9:2a:25:85:34:35:84:
7c:f8:4f:fa:41:f1:4e:10:f3:29:e9:f8:de:a3:
c1:b8:17:00:10:c9:75:f0:db:4a:d7:2b:90:a8:dc:
3b:82:a2:ee:c5:3d:4f:97:11:85:6c:d4:f0:5d:d4:
76:de:8c:dc:b9:e5:1d:21:e3:de:47:98:c3:7e:af:01:
28:ac:4f:2f:ff:a3:a3:e7:4e:63:79:ac:b9:c2:
87:95:55:4e:f1:b4:6f:12:bd:7c:88:35:84:8f:43:43:
a6:46:91:19:15:06:ee:d9:f8:53:8f:ea:05:7c:
12:8f:75:95:40:ea:39:ac:f1:dd:95:33:7d:e9:77:c6:
7b:04:64:1f:c8:3b:f0:ea:40:93:db:7a:91:97:
4b:57:64:91:81:68:cc:83:e4:99:ee:9a:97:0d:57:d1:
28:63:69:3c:92:36:0e:f3:1f:9f:4a:21:06:ba:
b8:01:7e:fb:9a:40:22:30:e8:bc:b9:f6:9e:e7:76:ef:
d0:01:11:14:e6:a8:50:26:54:42:a8:1a:4a:33:
0c:6f:f4:eb:43:1e:0d:fa:15:a9:2f:a7:aa:5f:25:f6:
b5:4b:a3:7a:71:35:78:80:81:93:50:da:f3:48:
1d:be:1b:79:4a:4e:b4:60:02:a3:5b:d3:6b:6e:3e:
96:4f:2a:d6:3b:a9:43:b4:b2:e2:5f:16:10:27:64:
59:c2:51:7c:36:0c:f4:2f:4c:0f:c7:fa:1f:e1:25:62:
44:0e:f6:a6:bc:54:3f:f3:da:2b:48:65:97:b0:
a6:6c:83
```

  - Exponent: 65537 (0x10001)

- Encrypts the default string “MegaCortex” with the generated master AES key and IV (using AES-128-CTR) then writes encrypted data to C:\lc_vagsi.tsv. The purpose of this step is to allow the attacker to verify whether the master AES key and IV are correct or not, if the victim makes a payment to recover their data.
- Finally, it creates another shared memory region named “Global\liblc_vagsi)” using the API CreateFileMapping before placing data related to payload.dll there. After this, it drops injecthelper.dll to %Temp%\lc_vagsi.dll and executes rundll32.exe with the arguments:
  - rundll32.exe %Temp%\lc_vagsi.dll,_command@16 Global\liblc_vagsi.
  - Now, injecthelper.dll is loaded and calls to export function _ command@16 with the input Global\liblc_vagsi
  - injecthelper.dll is a loader. It opens the shared memory region Global\ liblc_vagsi, loads data from that memory region (actually, it’s loading payload.dll, the main module of the ransomware) and calls to function start2. This creates another instance of payload.dll, which runs as a slave to perform the encryption task.

Figure 14. List of extensions and files not encrypted by MegaCortex

```
rdata:10063674 a_dll:
rdata:10063674                 unicode 0, <.dll>,0
rdata:1006367E                 align 10h
rdata:10063680 a_exe:
rdata:10063680                 unicode 0, <.exe>,0
rdata:1006368A                 align 4
rdata:1006368C a_sys:
rdata:1006368C                 unicode 0, <.sys>,0
rdata:10063696                 align 4
rdata:10063698 a_mui:
rdata:10063698                 unicode 0, <.mui>,0
rdata:100636A2                 align 4
rdata:100636A4 a_tmp:
rdata:100636A4                 unicode 0, <.tmp>,0
rdata:100636AE                 align 10h
rdata:100636B0 a_lnk:
rdata:100636B0                 unicode 0, <.lnk>,0
rdata:100636BA                 align 4
rdata:100636BC a_config:
rdata:100636BC                 unicode 0, <.config>,0
rdata:100636CC a_manifest:
rdata:100636CC                 unicode 0, <.manifest>,0
rdata:100636E0 a_tlb:
rdata:100636E0                 unicode 0, <.tlb>,0
rdata:100636EA                 align 4
rdata:100636EC a_olb:
rdata:100636EC                 unicode 0, <.olb>,0
rdata:100636F6                 align 4
rdata:100636F8 a_bat:
rdata:100636F8                 unicode 0, <.bat>,0
rdata:10063702                 align 4
rdata:10063704 a_cmd:
rdata:10063704                 unicode 0, <.cmd>,0
rdata:1006370E                 align 10h
rdata:10063710 a_ps1:
rdata:10063710                 unicode 0, <.ps1>,0
rdata:1006371A                 align 4
rdata:1006371C aDesktop_ini:
rdata:1006371C                 unicode 0, <desktop.ini>
rdata:10063734 aTemp:
```

Third stage: Encryption

At first, the slave will try to access the IPC shared memory region and pick up data from it. It retrieves:

- The full path of the files that will be encrypted
- The master AES key and IV generated in the setup stage

The encryption will then begin. MegaCortex uses native API functions to interact with target files. To encrypt each target file, MegaCortex performs the following actions:

- Appends the extension .aes128ctr to the name of the target file.
- Generates random seed data (size: 0x18 bytes). Encodes this seed data with Base64 then calculates the SHA256 from the Base64 output.
- Extracts SHA256 hash to the slave AES key and IV, which will be used to encrypt the target file (AES-128-CTR).
- Base64 of seed data with SHA1 hash of encrypted file are encrypted again by the master AES key and IV (AES-128-CTR).
- Finally, MegaCortex saves some information to the file C:\lc_vagsi.tsv for decryption purposes.

Another ransom note (!!!_READ_ME_!!!.txt) is copied to %Desktop% after the encryption process is completed.

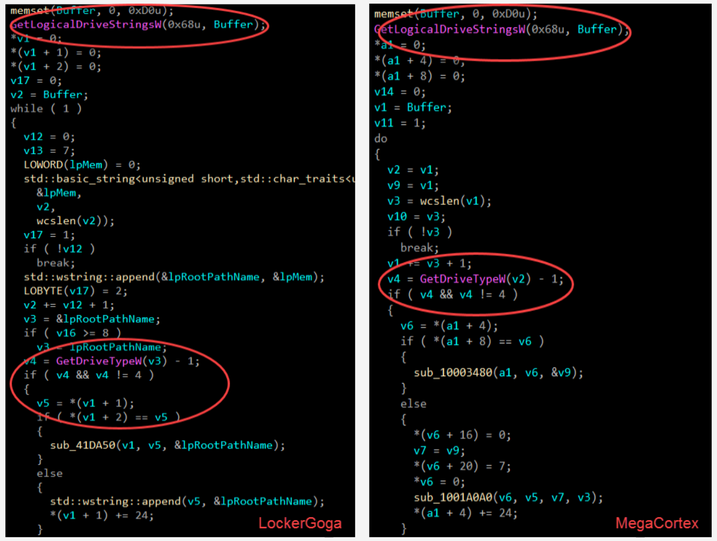
Link to GoGalocker?

Based on both MegaCortex's activity and the attributes of binary and code use, we believe there is some connection between MegaCortex and GoGalocker. We cannot confirm this connection firmly, but this coincidence is very strange.

Both MegaCortex and GoGalocker perform the following actions:

- Create a log file in C:\\
- Work using the master/slave model
- Use module interprocess in Boost library to share data and communicate between master and slave
- Use functions to enumerate logical drives before encryption (Figure 15)

Figure 15. Function used to enumerate drives in GoGalocker (left) and MegaCortex (right)



- Use native functions to work with target files:
  - NtOpenFile, NtReadFile, NtWriteFile, NtClose
- Encrypt files using AES-128-CTR
- Execute the command "cipher.exe /w" to wipe unused data after finishing encryption process

Finally, the rich header of the MegaCortex and GoGalocker executables is compiled with almost the same version of Visual Studio 2017 (minor build version 27027 and minor build version 27030 as illustrated in Figure 16).

Figure 16. Rich header data of GoGalocker (left) vs MegaCortex (right)

Additionally, based on our telemetry, we observed that there is a pattern of using Cobalt Strike malware in both GoGalocker and MegaCortex attacks. Furthermore, one of the Cobalt Strike beacons used in a MegaCortex attack connects to an IP address (185.202.174[.]44) that is also mentioned in FireEye's report about GoGalocker.

Protection

Symantec has the following protection in place to protect customers against these attacks:

File-based protection

- Hacktool.Mimikatz
- Ransom.Crysis
- Ransom.GandCrab
- Ransom.GoGalocker
- Ransom.Hermes
- Ransom.MegaCortex
- Ransom.Robbinhood
- Ransom.SamSam

Mitigation

Symantec recommends users observe the following best practices to protect against targeted ransomware attacks:

Local Environment

- Ensure you have the latest version of PowerShell and you have logging enabled.
- Restrict access to RDP Services: Only allow RDP from specific known IP addresses and ensure you are using multi-factor authentication.
- Use File Server Resource Manager (FSRM) to lock out the ability to write known ransomware extensions on file shares where user write access is required.
- Create a plan to consider notification of outside parties. In order to ensure correct notification of required organizations, such as the FBI or other law enforcement authorities/agencies, be sure to have a plan in place.
- Create a “jump bag” with hard copies and archived soft copies of all critical administrative information. In order to protect against the compromise of the availability of this critical information, store it in a jump bag with hardware and software needed to troubleshoot problems. Storing this information on the network is not helpful when network files are encrypted.
- Implement proper audit and control of administrative account usage. You could also implement one-time credentials for administrative work to help prevent theft and usage of admin credentials.
- Create profiles of usage for admin tools: Many of these tools are used by attackers to move laterally undetected through a network. A user account that has a history of running as admin using psinfo/psexec on a small number of systems is probably fine, but a service account running psinfo/psexec on all systems is suspicious.

Email

- Enable 2FA to prevent compromise of credentials during phishing attacks.
- Harden security architecture around email systems to minimize the amount of spam that reaches end-user inboxes and ensure you are following best practices for your email system, including the use of SPF and other defensive measures against phishing attacks.

Backup

- Implement offsite storage of backup copies. Arrange for offsite storage of at least four weeks of weekly full and daily incremental backups.
- Implement offline backups that are onsite. Make sure you have backups that are not connected to the network to prevent them from being encrypted by ransomware.
- Verify and test your server-level backup solution. This should already be part of your Disaster Recovery process.
- Secure the file-level permissions for backups and backup databases. Don’t let your backups get encrypted.
- Test restore capability. Ensure restore capabilities support the needs of the business.

Appendix

GoGalocker indicators of compromise

SHA256	MALWARE IDENTIFIER
8cfbd38855d2d6033847142fdfa74710b796daf465ab94216fbbbe85971aee29	Ransom.GoGalocker
c97d9bbc80b573bdeeda3812f4d00e5183493dd0d5805e2508728f65977dda15	Ransom.GoGalocker
7852b47e7a9e3f792755395584c64dd81b68ab3cbcdf82f60e50dc5fa7385125	Ransom.GoGalocker
6e69548b1ae61d951452b65db15716a5ee2f9373be05011e897c61118c239a77	Ransom.GoGalocker
bdf36127817413f625d2625d3133760af724d6ad2410bea7297ddc116abc268f	Ransom.GoGalocker
eda26a1cd80aac1c42cdbba9af813d9c4bc81f6052080bc33435d1e076e75aa0	Ransom.GoGalocker
47f5a231f7cd0e36508ca6ff8c21c08a7248f0f2bd79c1e772b73443597b09b4	Ransom.GoGalocker
e6de5029cb6020f194309eaa575007db41666658e450d234355b32e55cd56574	Ransom.GoGalocker
7bcd69b3085126f7e97406889f78ab74e87230c11812b79406d723a80c08dd26	Ransom.GoGalocker
e8c14fdcb61ac9cd261f8ea52fc2971db85144f412f0b0334555d4b5a22e3b2a	Ransom.GoGalocker
87f3a39fbea7a3a64776bb79b8b9e01c7664ca8e7b4337c6bc566635421c61dd	Trojan
88d149f3e47dc337695d76da52b25660e3a454768af0d7e59c913995af496a0f	Ransom.GoGalocker
ceec12762e66397b56dad64fd270bb3d694c78fb9cd665354383c0626dbab013	Threat Artefact
5e8369f1216b381171f1a8432548c70f2de8ee6043c80cc935e4a755b0c28a7d	Ransom.GoGalocker
c3d334cb7f6007c9ebee1a68c4f3f72eac9b3c102461d39f2a0a4b32a053843a	Ransom.GoGalocker
5b0b972713cd8611b04e4673676cdff70345ac7301b2c23173cdfeaff564225c	Ransom.GoGalocker
029b292267560038a6955b479294ee0cbdbde2c7d1966dc1f0545b86c5d53c1a	Trojan
12f09c6dc1993e727c3b1e156be4edea57084a2f5522773c610ecc4eb789adbc	Trojan
06b971a7db9469b8aef0c9f2ee951786d128bf92af7d8a3a71bbcdf497ca9555	Trojan
2c47b4f1428df8abd9ddfcd095185185e84516380a78fa60fe126e9897ccbb4b	Trojan
7a362c1a8e79865cdc992f9a8fac69c8217bc9f07edb856a3333175be7583eb1	Trojan
83448f6cdf15330fd1ebc89c4664c5652d19b6db6e8d53da5eebc599f233f1b2	Trojan
8d4f7217c15183ab5696deaa234f1b0138f696d761799660b4289ad39b608e9b	Ransom.GoGalocker
fd4b7937aa7ceb3a8df4db33f268af517e86e006250ca525f376f9724a96e6c0	Ransom.GoGalocker
a193f3b6bbc620593848de7be912c1efe7038fa5e8004c2bd44c30319dfcc8d5	Trojan
f3c58f6de17d2ef3e894c09bc68c0afcce23254916c182e44056db3cad710192	Ransom.GoGalocker
ffab69deafa647e2b54d8daf8c740b559a7982c3c7c1506ac6efc8de30c37fd5	Ransom.GoGalocker
65d5dd067e5550867b532f4e52af47b320bd31bc906d7bf5db889d0ff3f73041	Ransom.GoGalocker
14e8a8095426245633cd6c3440afc5b29d0c8cd4acefd10e16f82eb3295077ca	Ransom.GoGalocker
1dcbcd1f86c658f262c44db3dc6bf933f29177c5e828e628a149e8d4f11e7b3c	Ransom.GoGalocker
c7a69dcfb6a3fe433a52a71d85a7e90df25b1db1bc843a541eb08ea2fd1052a4	Ransom.GoGalocker
97a2ab7a94148d605f3c0a1146a70ba5c436a438b23298a1f02f71866f420c43	Ransom.GoGalocker
a84171501074bac584348f2942964c8550374c39247ec6af0f4a69756ea9fc7a	Ransom.GoGalocker

MegaCortex indicators of compromise

Command and control:

37.252.15.241

185.202.174.44/visit.js

199.189.108.71/ga.js

89.105.198.28/IE9CompatViewList.xml

89.105.198.28/push

89.105.198.28/updates.rss

SHA256

b4a65070354d2a89e84b5ddae81a954a868a714a248a48b72c832c759d85558a

f5d39e20d406c846041343fe8fbd30069fd50886d7d3d0cce07c44008925d434

b17ff8c0d83d07fca854d669d1389e8e24718ca54ed1543fdb09e9b9b39456ef

598ee9ee6ad4467ddf4b4d325cb15928fd692da8d6e1c8980d2d86d97ea2f4f9

ab654745b33aabac9c8e4ba1d0040be1c44ac50d0090b4759d4ef1aa04d55947

11f7bb37dd425150e6b095a8d1f3a347ee83e604302a4d9bb201900e74a81d73

80b9629ea3a33dc26f2ed3a2f8d3293cc3684f544011f1c4b96d4104d392497f

0858bc69e02c730a55f760f01374bdc378aaff806478d1c18f9e587d7121b56a

27253989e94640a7852c6b2c1eaa2731791bc0a421979da29af9ea9209b1d22d

07/19

Symantec Corporation
World Headquarters
350 Ellis Street
Mountain View, CA 94043
United Stated of America

+1 650 527–8000
+1 800 721–3934

Symantec.com

For specific country offices and contact numbers, please visit our website.
For product information in the U.S., call toll-free 1 (800) 745 6054.