White Paper

Symantec
A Division of Broadcom

Targeted Ransomware

By Threat Hunter Team

Table of Contents

Introduction

Targeted Ransomware Trends

Attacker Profiles
- Maze
- Sodinokibi
- BitPaymer
- WastedLocker
- Miner: Ryuk, GoGalocker, and MegaCortex

Infection Vectors
- Phishing
- Malvertising
- Vulnerability Exploitation
- Secondary Infections
- Poorly Secured Services

Credential Theft and Lateral Movement

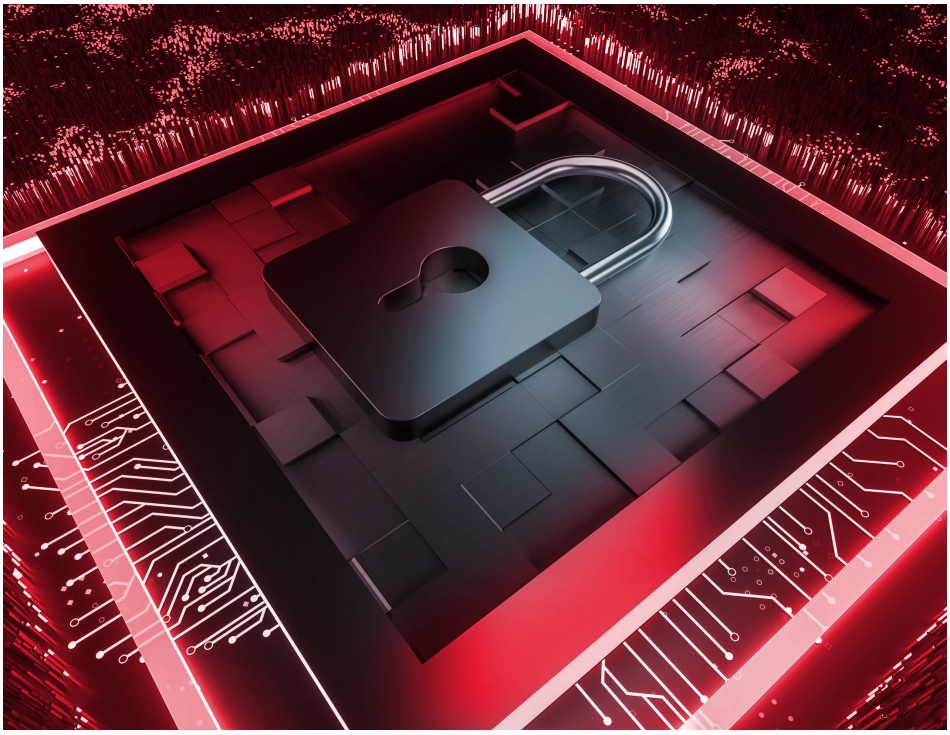
Conclusion

Protection
- File-based Protection
- AI-based Protection
- Threat Hunting
- Endpoint Detection and Response (EDR)

Mitigation

Appendix 1: Dwell Time Analysis

Appendix 2: MITRE ATT&CK® Techniques



Introduction

Over the past 18 months, targeted ransomware has moved from being a lucrative, but niche area of cyber crime to probably the most dangerous threat facing enterprises. During this period, the number of groups conducting these attacks has multiplied. Massive reported ransom payouts have created a gold rush mentality among attackers, with some veteran cyber criminals abandoning their traditional areas of operations and pivoting to targeted ransomware.

The impact of this proliferation has been amplified by the advent of ransomware-as-a-service (RaaS), where successful ransomware developers lease out their wares to other attackers in exchange for a percentage of any ransom payments.

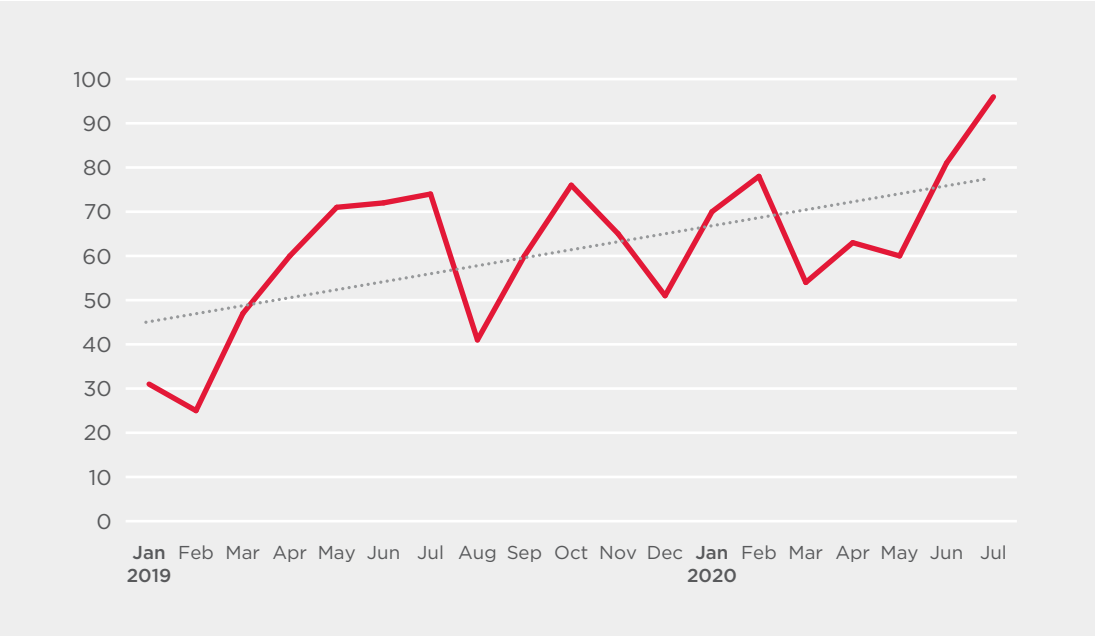
Tactics too have evolved, and attackers have found more ways of extorting victim organizations. A growing number of attackers now steal data from their targets before encrypting computers. The attackers then threaten to publish this data unless the ransom is paid. The threat of a data breach increases the pressure on victim organizations to pay. It also provides the attackers with leverage over victims who may have been in a position to restore encrypted systems from backups.

The level of threat means that organizations of all sizes should inform themselves about how these attacks can unfold, and take all possible steps to reduce the risk of a successful attack.

Targeted Ransomware Trends

The number of organizations affected by targeted ransomware attacks has grown steadily over the past year and a half. Looking at the number of verified attacks by 10 prominent targeted ransomware groups, we found that while the number of organizations attacked each month has fluctuated, the overall trend is upwards.

Figure 1: Number of Organizations Affected by Targeted Ransomware Attacks, January 2019 to July 2020

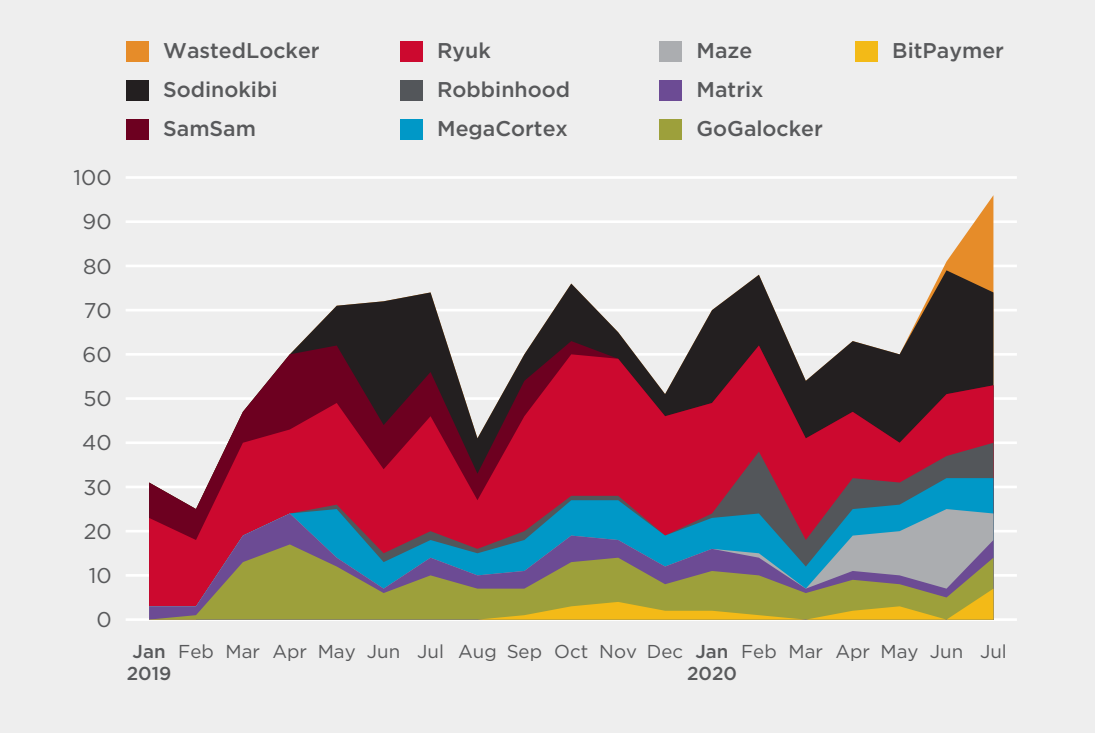


Symantec, a division of Broadcom (NASDAQ: AVGO), observed 31 organizations being attacked in January 2019. This number rose to 89 during the month of July 2020.

The real number of targeted ransomware attacks may be higher. Some ransomware families, such as Dharma (also known as Crysis) have been deployed through spam campaigns—in addition to being used in targeted attacks. There is no way to establish how many victims were infected by these targeted attacks, and how many were infected through other means.

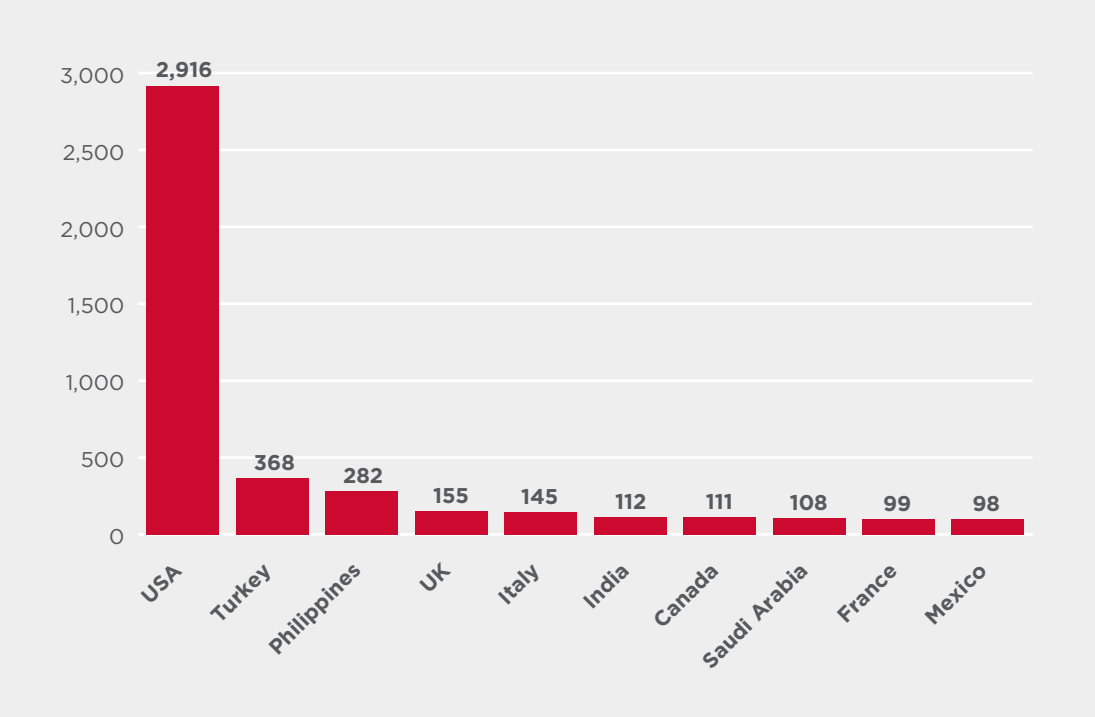
In addition to these targeted attacks, confirmed attacks from the 10 aforementioned ransomware families are probably only a representative sample of the overall number of attacks involving these threats. Most targeted ransomware operators recompile their ransomware for every new attack. This means that the variant of the ransomware used in an attack may be blocked by a generic or machine learning-generated detection signature, rather than a detection linked to that ransomware family.

Figure 2: Number of Organizations Affected by Targeted Ransomware Attacks, by Family, January 2019 to July 2020



When the attacks are broken down by ransomware family, it becomes apparent that the profusion of new actors is driving the growth in attacks. In January 2019, three of the analyzed groups were active. By July 2020, eight groups were carrying out attacks. During 2020, relatively recent arrivals on the scene such as Sodinokibi, Maze, and more recently, WastedLocker, have significantly contributed to the overall increase in attacks.

Figure 3: Number of Targeted Ransomware Infections by Country, January 2019 to July 2020



When analyzing attacks by geographical region, a different methodology needs to be employed since many victims of targeted ransomware have operations in more than one country. By counting identifiable infections from the 10 targeted ransomware families listed above, the U.S. continues to be the country that is by far the most heavily targeted by attack groups. Curiously, it is followed by Turkey and the Philippines. These countries usually do not figure so prominently in cyber crime statistics. The remainder of the top 10 countries is less of a surprise.

Attacker Profiles

Maze

Maze first appeared in May 2019, and in the intervening period has been one of the most active targeted ransomware groups. The group is best known for pioneering the tactic of exfiltrating data from victim organizations prior to encryption and threatening to release this data unless the ransom is paid. This increases the pressure on the victim to pay the ransom and provides a new pressure point that can be applied against victims capable of restoring affected systems from back-ups. This tactic was quickly copied by a range of other targeted ransomware groups including Sodinokibi, Nemty, and DoppelPaymer.

Figure 4: Organizations Affected by Maze Attacks, January 2020 to July 2020

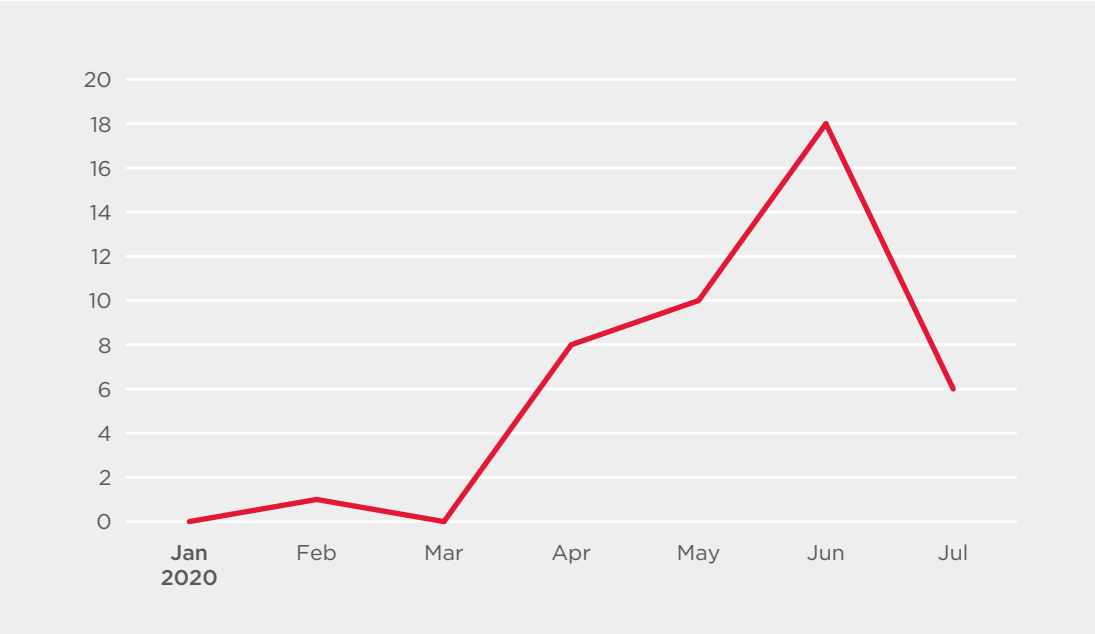
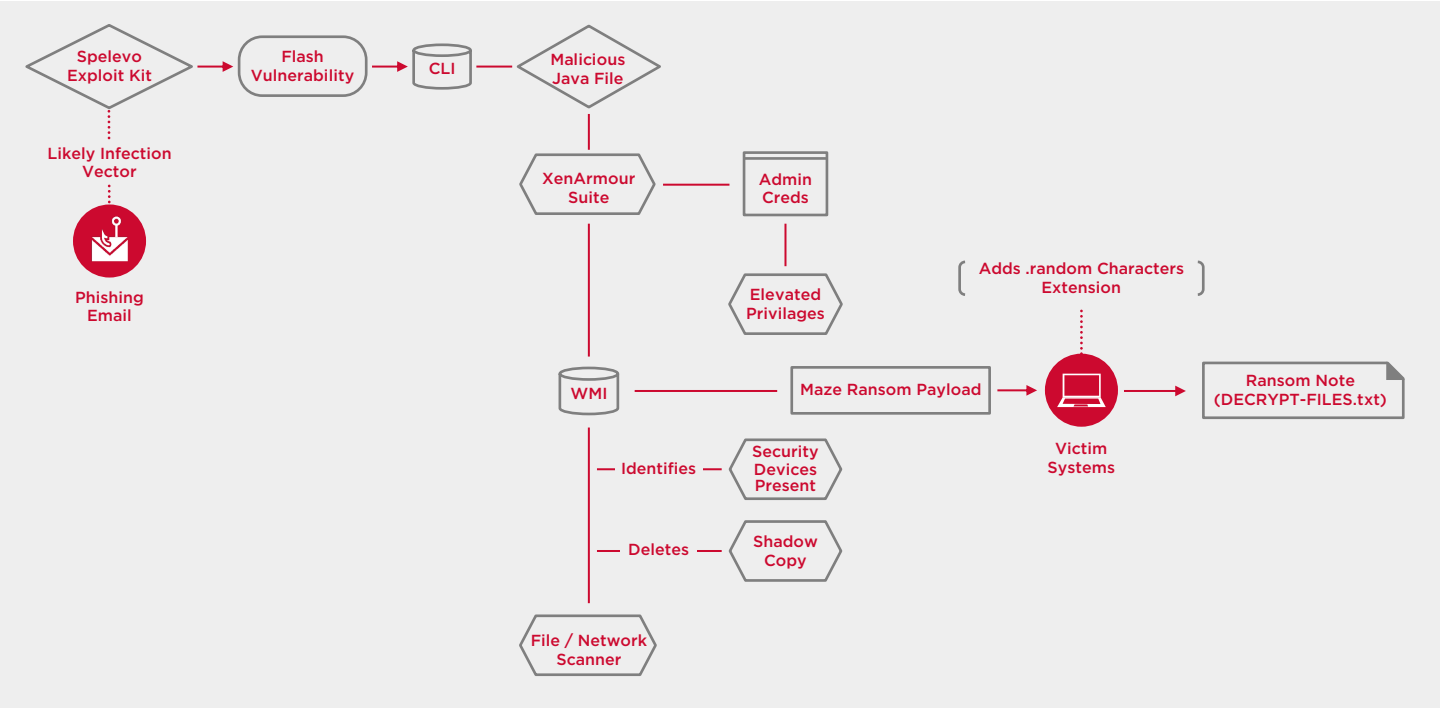


Figure 5: Maze Attack Flow



The main distribution channels for Maze are the Fallout and Spelevo exploit kits—with victims being directed to them through spam email campaigns. Once the attackers gain access to a single computer on a network, they download the commodity malware Cobalt Strike and the Metasploit Framework to move laterally across the network and enumerate machines.

The attackers scan for machines on the network running the RDP protocol and use brute-force attacks to obtain credentials and gain privileged access to servers. This access allows the attackers to identify file servers and databases, allowing them to exfiltrate data that will subsequently be used to extort the victim.

The group tends to spend a long time on the victim's network. Up to 21 days can pass between the initial intrusion and the ransomware execution.

A noteworthy feature of the Maze attacks is that the attackers check the language used on the victim's system. If the language is set to Russian, the malware does not execute.

Maze also has an unusual approach to payment, demanding two separate payments from the victim. The first payment is in exchange for an undertaking not to share data stolen from the victim. The second payment is to obtain a decryption key.

If the victim doesn't make the first payment before the deadline, Maze will post the stolen data on its own public website. It also uses social media accounts to alert the victim organization and their customers of the data breach.

According to third-party reports, the group will provide a decryption key to victims who pay, but it will still frequently sell stolen data on underground markets—even if the victim has paid the ransom.

Maze will also provide RaaS to other attackers. The group frequently posts on hacking forums and underground markets and it is also quite active on social media such as Twitter, often using it to taunt their victims.

Sodinokibi

Sodinokibi (also known as REvil) first appeared in April 2019, although its creators have been involved in the ransomware business for much longer, having been responsible for the older GandCrab ransomware which was discontinued prior to the release of Sodinokibi.

Sodinokibi, like GandCrab, operates under the RaaS business model, leasing out its tools to a select number of groups, known as affiliates, who perform the attacks. Profits are split between the Sodinokibi authors and their affiliates. It is believed that many GandCrab affiliates transitioned to become Sodinokibi affiliates.

Figure 6: Organizations Affected by Sodinokibi Attacks, January 2019 to July 2020

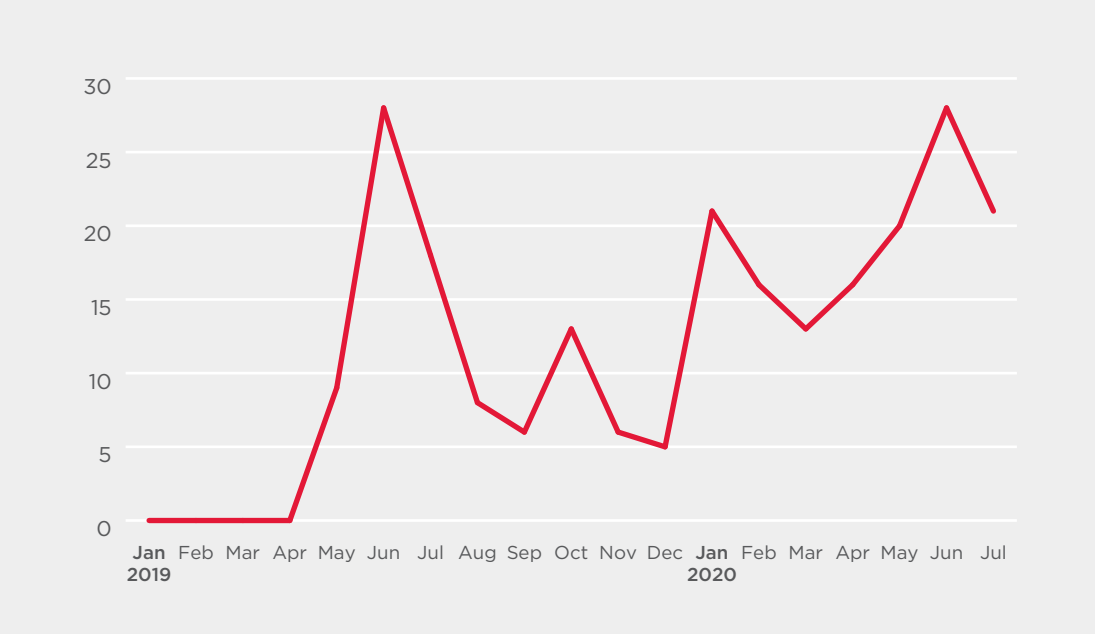
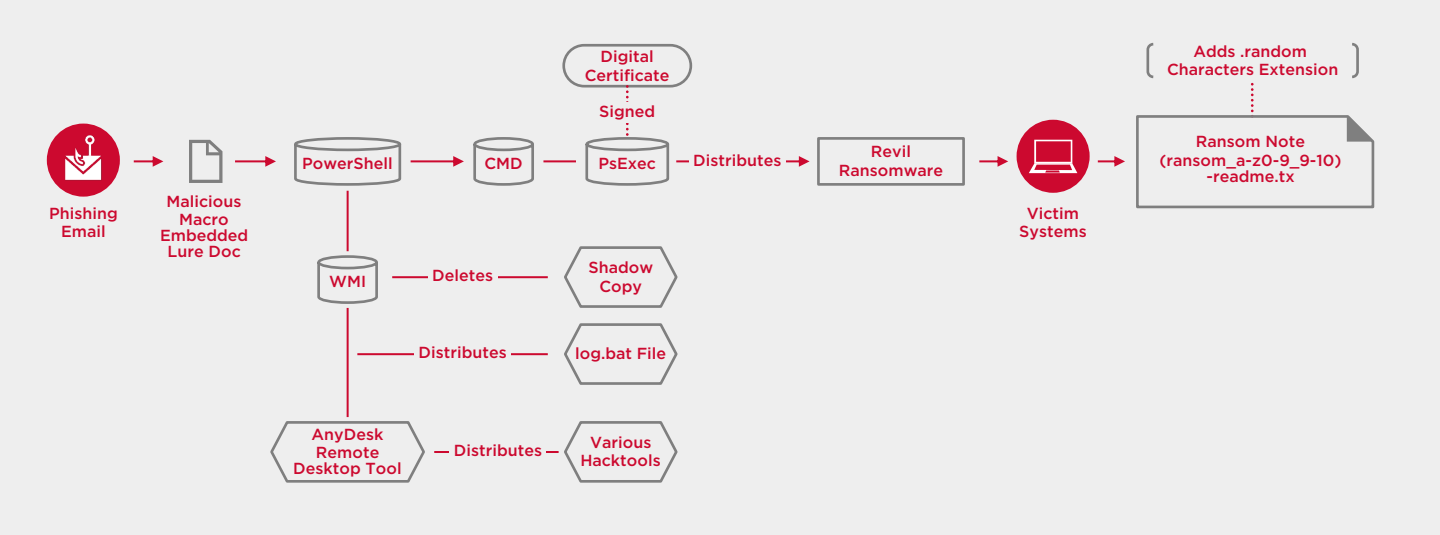


Figure 7: Sodinokibi Attack Flow



The attacks usually begin with phishing emails with attached Word documents containing malicious macros. Once on the victim's network, the attackers will spend three to eight days performing the groundwork for an attack. In common with many other targeted ransomware groups, Sodinokibi attacks tend to make extensive use of resources within the victim's environment along with publicly available tools to stage the environment before ransomware payload execution. In this case, it uses PowerShell, WMI, PsExec, and the AnyDesk remote desktop tool. The attackers also delete Windows Shadow Copies in order to hamper restoration of encrypted machines.

Sodinokibi has made a name for itself for targeting large organizations. Larger companies can afford to pay larger ransoms and often have more to lose from having their data made publicly available. The group was linked to the January 2020 attack on foreign exchange service Travelex which generated a $2.3 million ransom, far higher than the average $260,000 seen in most enterprise ransomware attacks.

Sodinokibi was quick to copy the tactic of exfiltrating data from the victim's network. The group usually posts a sample to publicly available websites such as Pastebin to prove that the data has been stolen. The attackers then apply further pressure to extort the victim by threatening to release the stolen information unless the ransom is paid. For every hour the victim does not pay, more information is publicly released, and the amount of ransom goes up.

Even if the victim pays the ransom, they may still lose their data, since Sodinokibi has also been observed selling victim data on underground forums to the highest bidder.

Another interesting feature of Sodinokibi attacks is that in some cases, the attackers have been observed scanning victim networks for credit card or point of sale (PoS) software. It is not clear at present if the attackers were targeting this software for encryption or because they want to scrape this information as a way to make even more money from this attack.

BitPaymer

BitPaymer has been linked to the Evil Corp cyber crime organization, which has subsequently begun using the WastedLocker ransomware (also profiled in this paper).

Evil Corp made a name for itself for attacks involving the Dridex banking Trojan, but during 2017 it completely overhauled its operations and moved into targeted ransomware. BitPaymer attacks began in June 2019 and continued until June 2020, after which the group appears to have transitioned to WastedLocker.

Figure 8: Organizations Affected by BitPaymer Attacks, January 2019 to July 2020

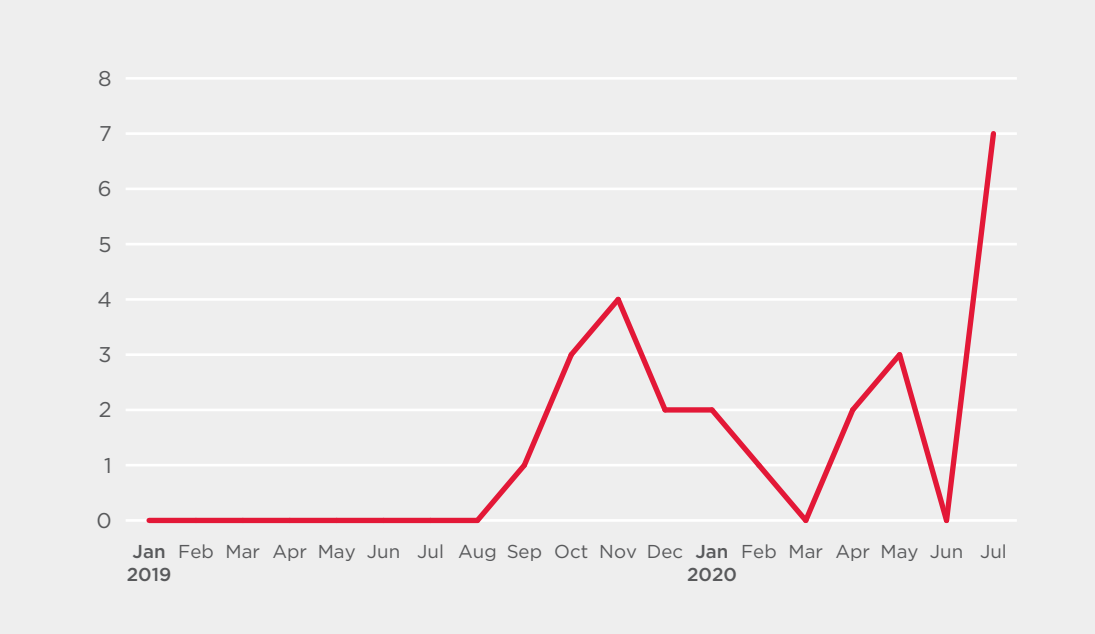
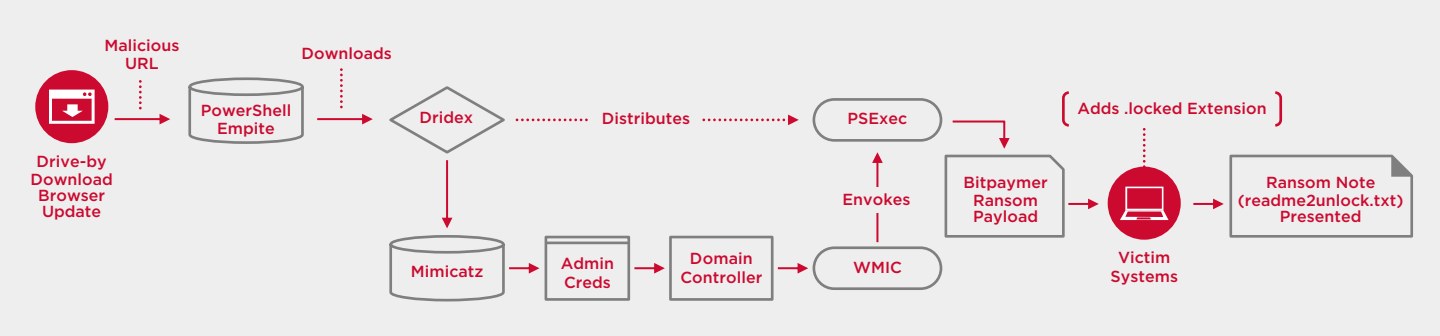


Figure 9: BitPaymer Attack Flow



BitPaymer attacks usually began by infecting the victim through phishing emails or exploit kits delivering fake browser updates. In addition to this, the group had a large pool of potential victims which had been already infected with its Dridex Trojan, providing the attackers with access to all previously compromised victims.

Dridex was not just used as an infection vector. The malware was also deployed against new victims. Dridex is modular in nature and includes credential stealing capabilities and the ability to deliver additional malware. The attackers essentially repurposed it from being their main payload to a tool used to stage the victim's environment for the ransomware attack.

Typically, BitPaymer attackers spent between five and eight days on the victim's network prior to executing the ransomware. In order to escalate privileges and move latterly across the network, the attackers leveraged many of the system and administrative tools already present in the environment, aka living off the land. This reduced any opportunity for defenders to identify malicious activity taking place, increasing the chance of a successful compromise.

Attacks frequently began with the use of PowerShell (and the PowerShell Empire framework) to download Cobalt Strike. Cobalt Strike is sold as a penetration testing tool, but is frequently used for malicious purposes.

Additionally, legitimate admin tools such as WMIC and PsExec were used to gain access, disable security software, delete backup and restoration capabilities, and disperse and execute the BitPaymer payload.

WastedLocker

WastedLocker is a new family of targeted ransomware linked to the Evil Corp cyber crime gang. It appears to have begun operating around May 2020.

Attacks begin with a malicious JavaScript-based framework known as SocGholish which masquerades as a software update. SocGholish has been found on more than 150 compromised websites, including dozens of U.S. newspaper websites.

Figure 10: Organizations Affected by WastedLocker Attacks, January 2020 to July 2020

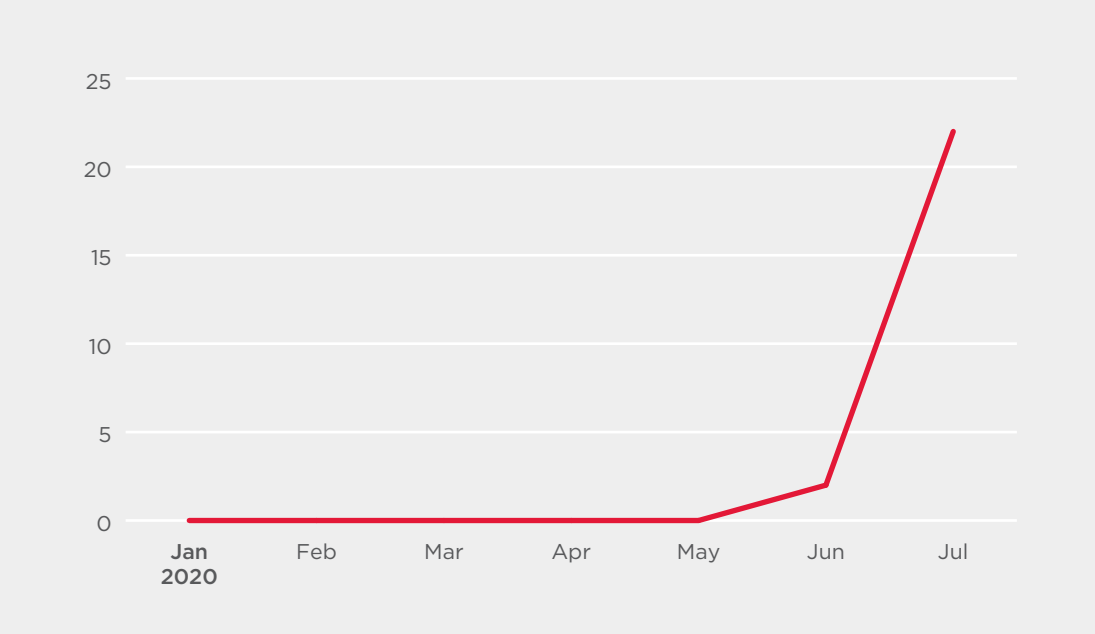
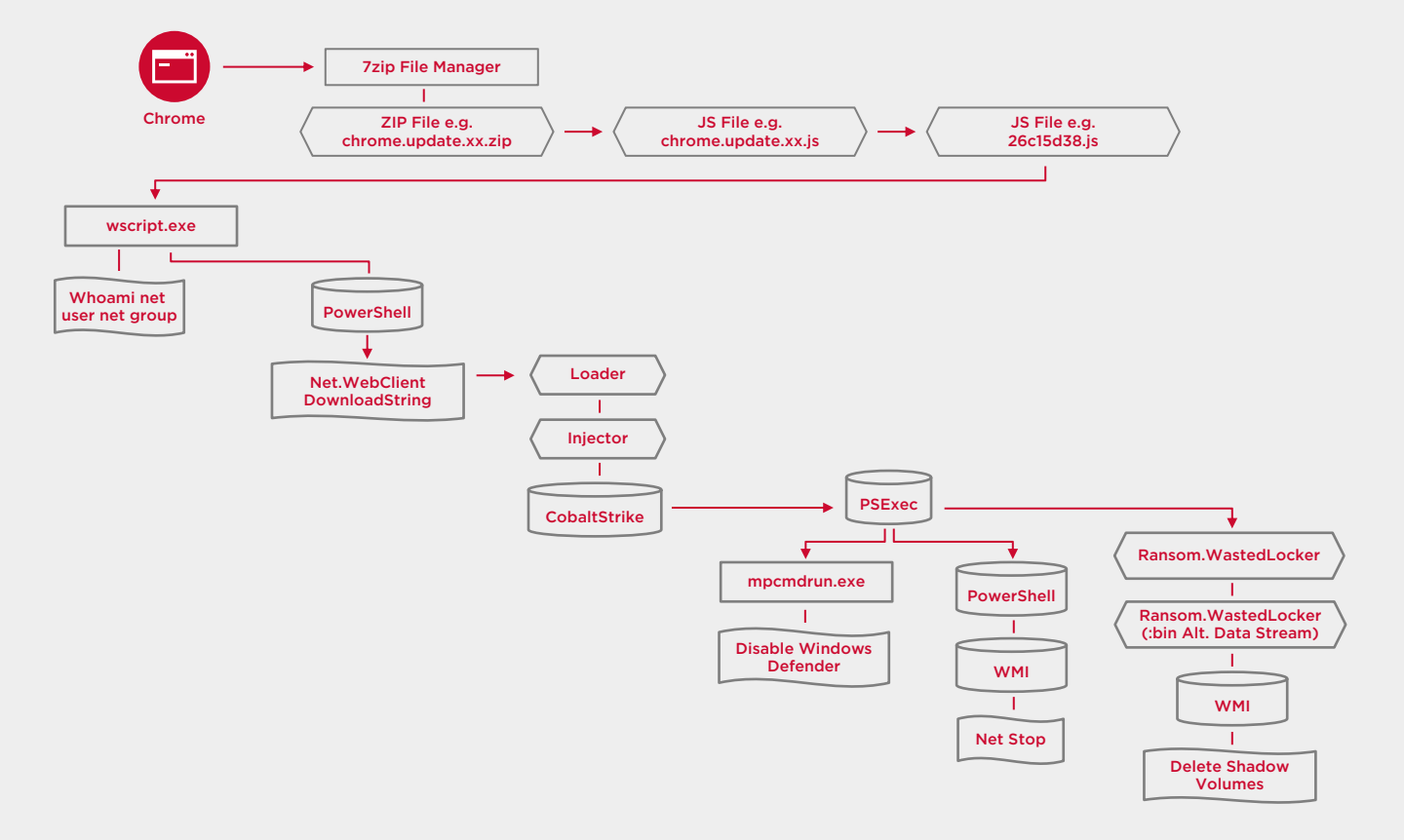


Figure 11: WastedLocker Attack Flow



Once the attackers have a foothold on the victim's network, PowerShell is used to download and execute a loader. The loader contains a .NET injector along with a loader for Cobalt Strike Beacon, which is reportedly taken from an open-source project called Donut, which is designed to help inject and execute in-memory payloads.

Cobalt Strike Beacon can be used to execute commands, inject other processes, elevate current processes or impersonate other processes, and upload and download files. The Get-NetComputer command from PowerView is renamed by the attackers to a random name. This command then searches for all the computer objects in the Active Directory database with filter conditions like *server* or *2003* or *7* (returning all Windows Server, Windows Server 2003, or Windows 7 instances). The attackers then log this information in a .tmp file.

Privilege escalation is performed using a publicly documented technique involving the Software Licensing User Interface tool (slui.exe), a Windows command line utility that is responsible for activating and updating the Windows operating system.

The attackers use the Windows Management Instrumentation Command Line Utility (wmic.exe) to execute commands on remote computers, such as adding a new user or executing additional downloaded PowerShell scripts. Cobalt Strike is also used to carry out credential dumping using ProcDump and to empty log files.

In order to deploy the ransomware, the attackers use the Windows Sysinternals tool PsExec to launch a legitimate command line tool for managing Windows Defender (mpcmdrun.exe) to disable scanning of all downloaded files and attachments, remove all installed definitions, and, in some cases, disable real-time monitoring.

PsExec is then used to launch PowerShell, which uses the win32_service WMI class to retrieve services and the net stop command to stop these services. After Windows Defender is disabled and services have been stopped across the organization, PsExec is used to launch the WastedLocker ransomware itself, which then begins encrypting data and deleting shadow volumes.

Miner: Ryuk, GoGalocker, and MegaCortex

In a 2019 paper, we found some links between the GoGalocker and MegaCortex ransomware families. Now we have found stronger evidence that they, along with Ryuk, are controlled by a single adversary which we have named Miner.

Figure 12: Organizations Affected by Ryuk Attacks, January 2019 to July 2020

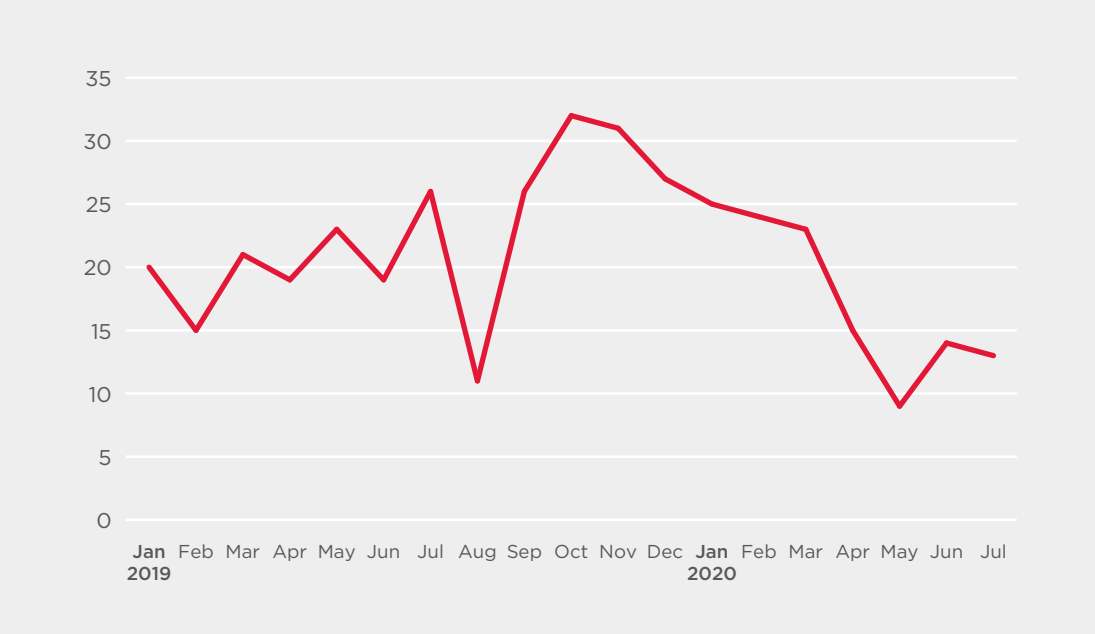
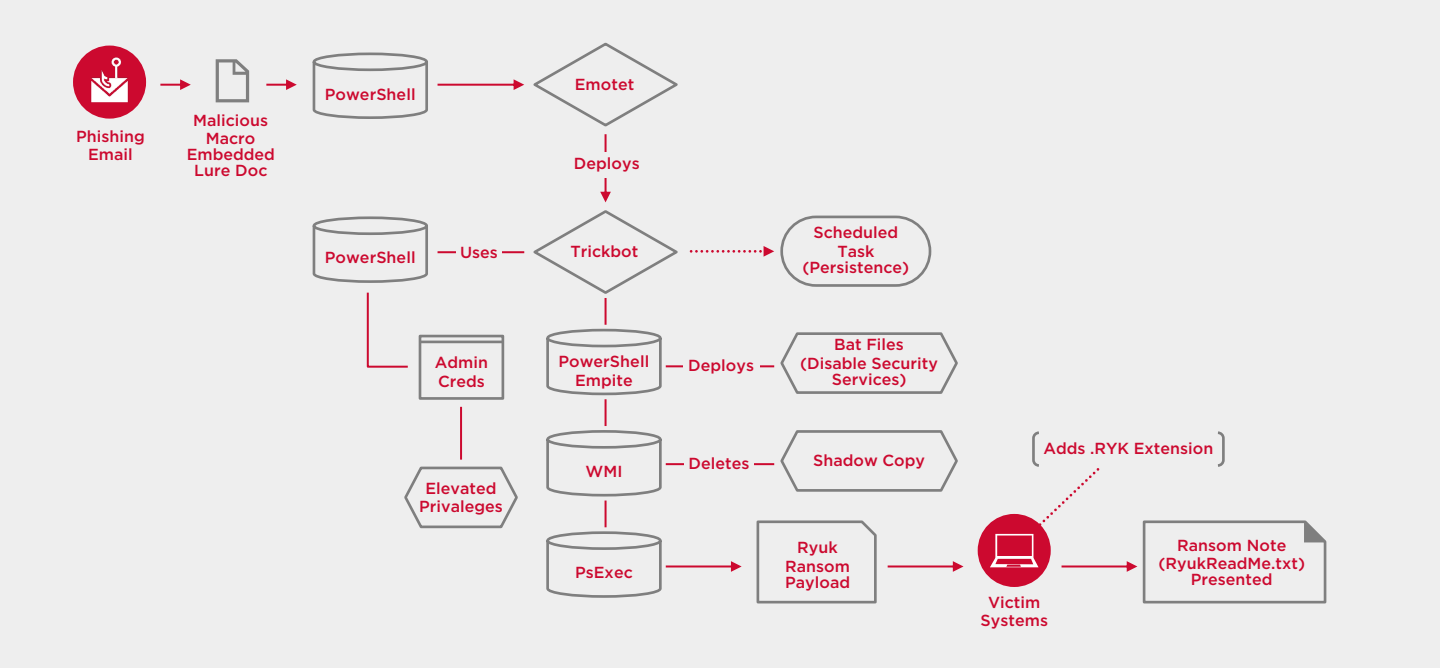


Figure 13: Ryuk Attack Flow



While Miner has used differing ransomware payloads, its overall operational methodology has remained quite consistent since it began mounting targeted ransomware attacks. While some tools have changed over time, the operating procedure has not change much.

One component seen across all operations is the use of Cobalt Strike, which runs in the memory of infected systems making detection difficult. Miner uses Cobalt Strike to download additional tools and to create a reverse shell providing the attacker with additional access. Cobalt Strike is one of the few tools consistent in all operations regardless of the ransom payload used in Miner's attack.

In some cases, Miner uses Mimikatz to obtain victim credentials, while in others, the attackers leverage capabilities found in TrickBot malware for the same purpose. In this case, Miner changed the tools used, but the tactic remained the same. The methodology and steps involved in each attack should be used to identify Miner activity rather than the tools themselves.

Figure 14: Organizations Affected by GoGalocker Attacks, January 2019 to July 2020

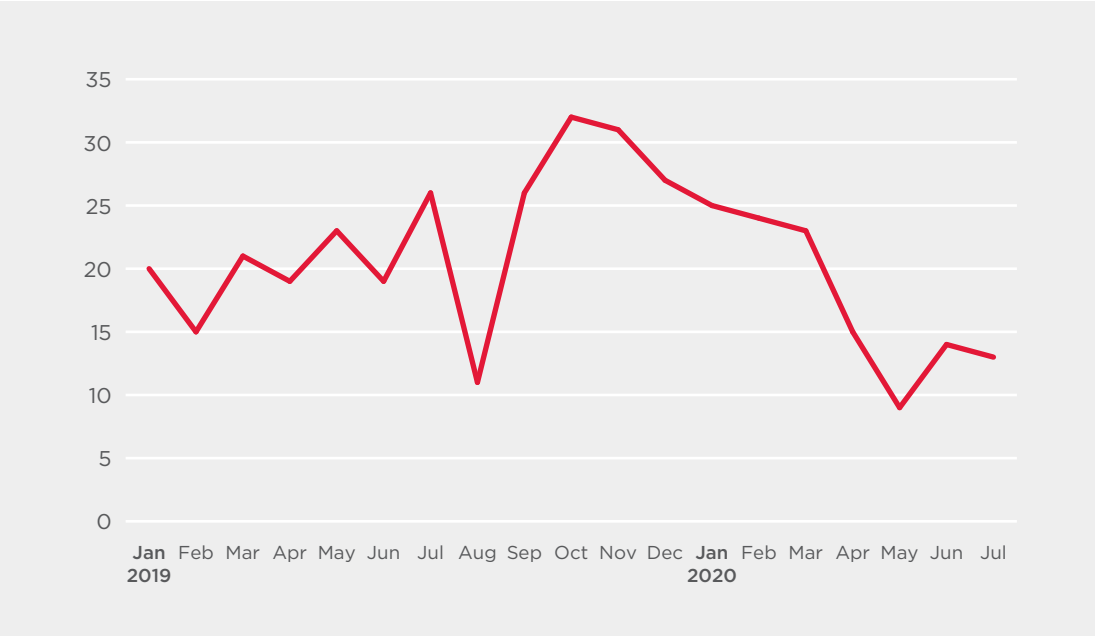
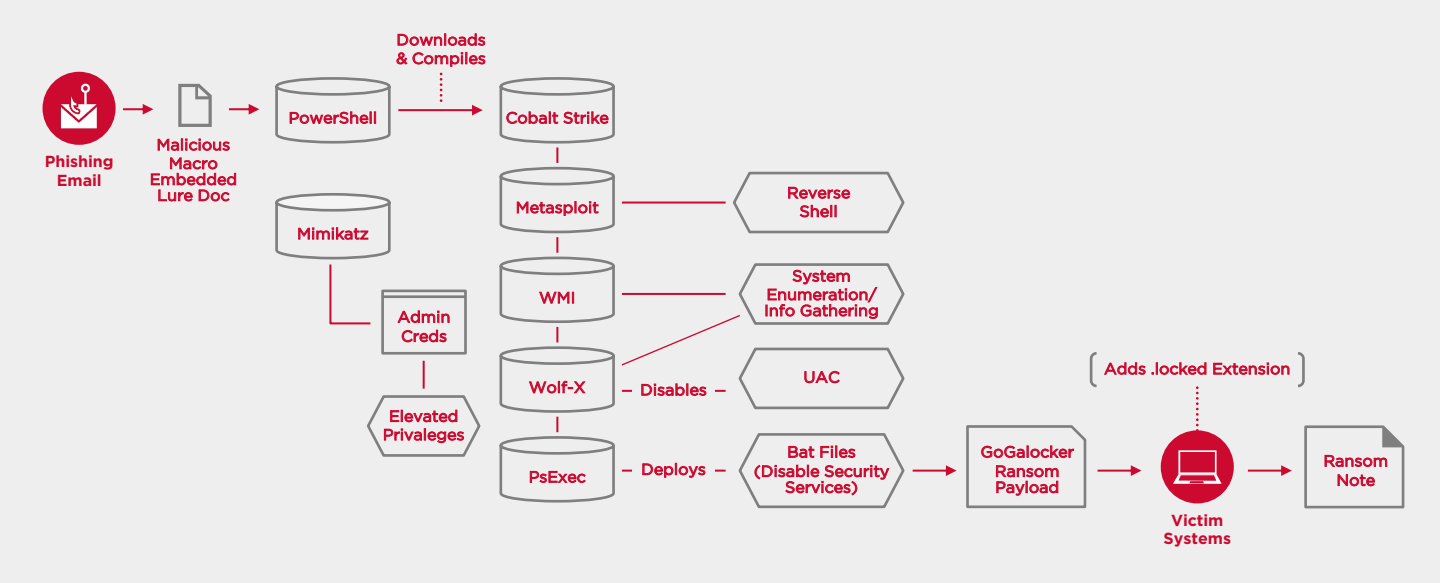


Figure 15: GoGaLocker Attack Flow



In common with many other targeted ransomware attackers, Miner makes wide use of the resources found in the victim's environment. The attacks begin with phishing emails containing malicious documents that, if opened, will infect the victim with Emotet or TrickBot malware. Emotet is designed to self-propagate across the victim's network by accessing open shares, making it a useful tool for lateral movement. TrickBot meanwhile has a modular design, and can load components pertinent to the attack underway. In this case, TrickBot is used to steal credentials in order to escalate privileges.

Publicly available malware such as Cobalt Strike and Metasploit are then used to enumerate the network for lateral movement and increase privileges. Once this step is completed, Miner gains administrative access to domain controllers. The attackers then uses batch files, deployed via PsExec, to disable and delete backup/restoration capabilities and security services throughout the environment. At this point, the network is staged and ready for the disbursement and execution of the ransomware payload.

Figure 16: Organizations Affected by MegaCortex Attacks, January 2019 to July 2020

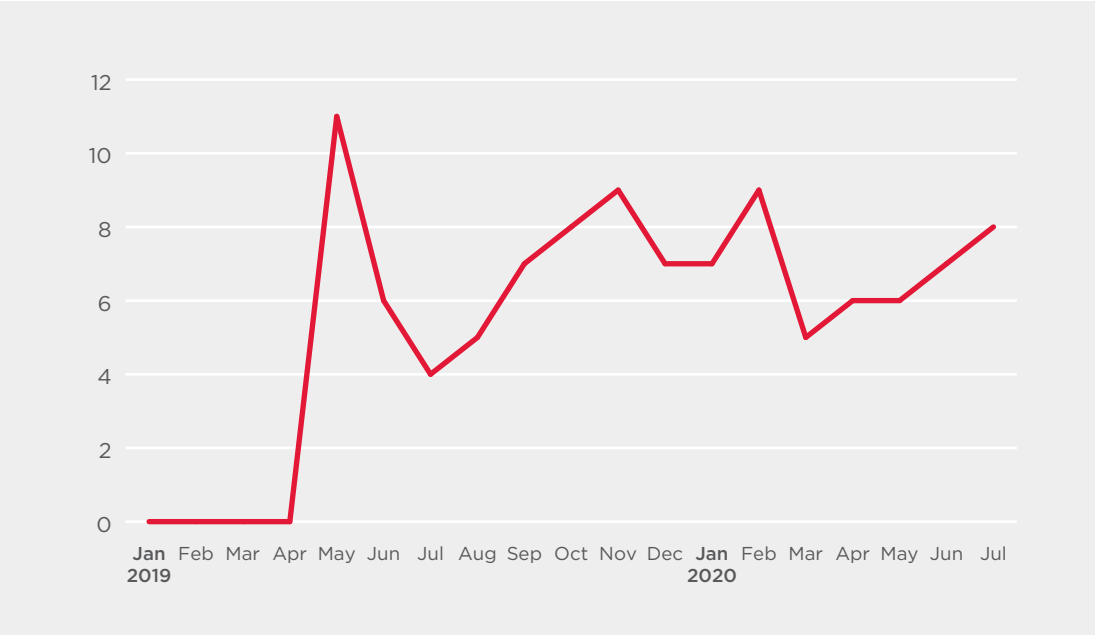
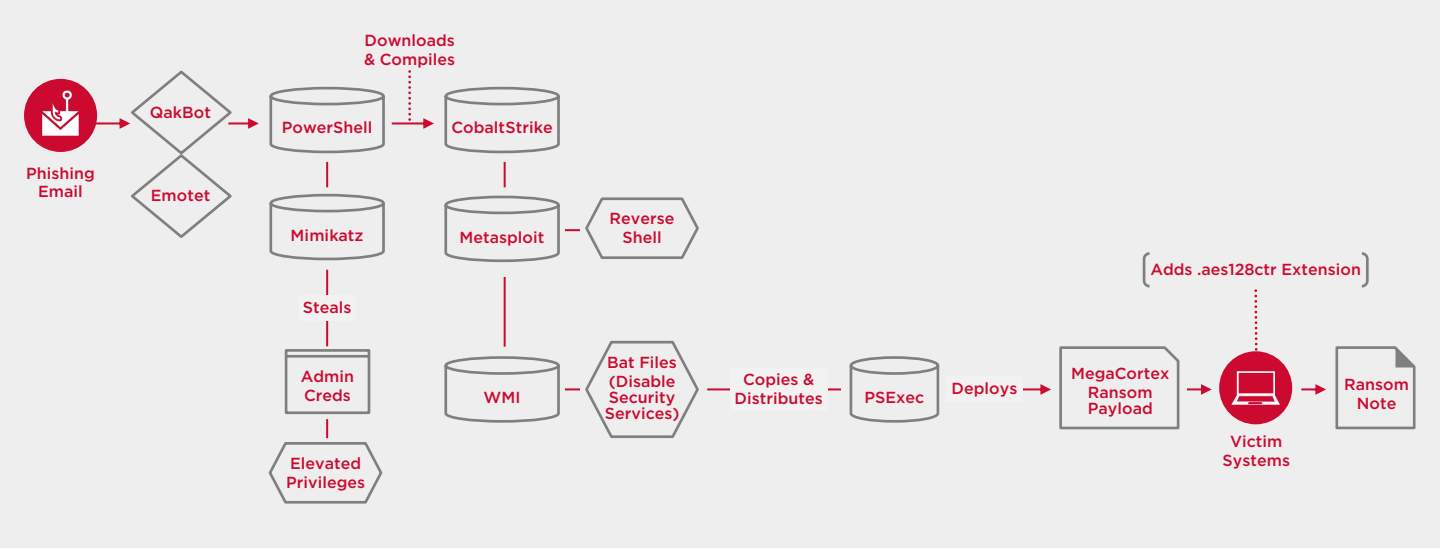


Figure 17: MegaCortex Attack Flow



Infrastructure Overlap:

Several IP addresses used by Miner to download Cobalt Strike were in the 89.105.198.XX IP space.

- 89.105.198.21 – GoGalocker attack
- 89.105.202.58 – GoGalocker attack
- 89.105.198.28 – MegaCortex attack

Bat Filename Similarities:

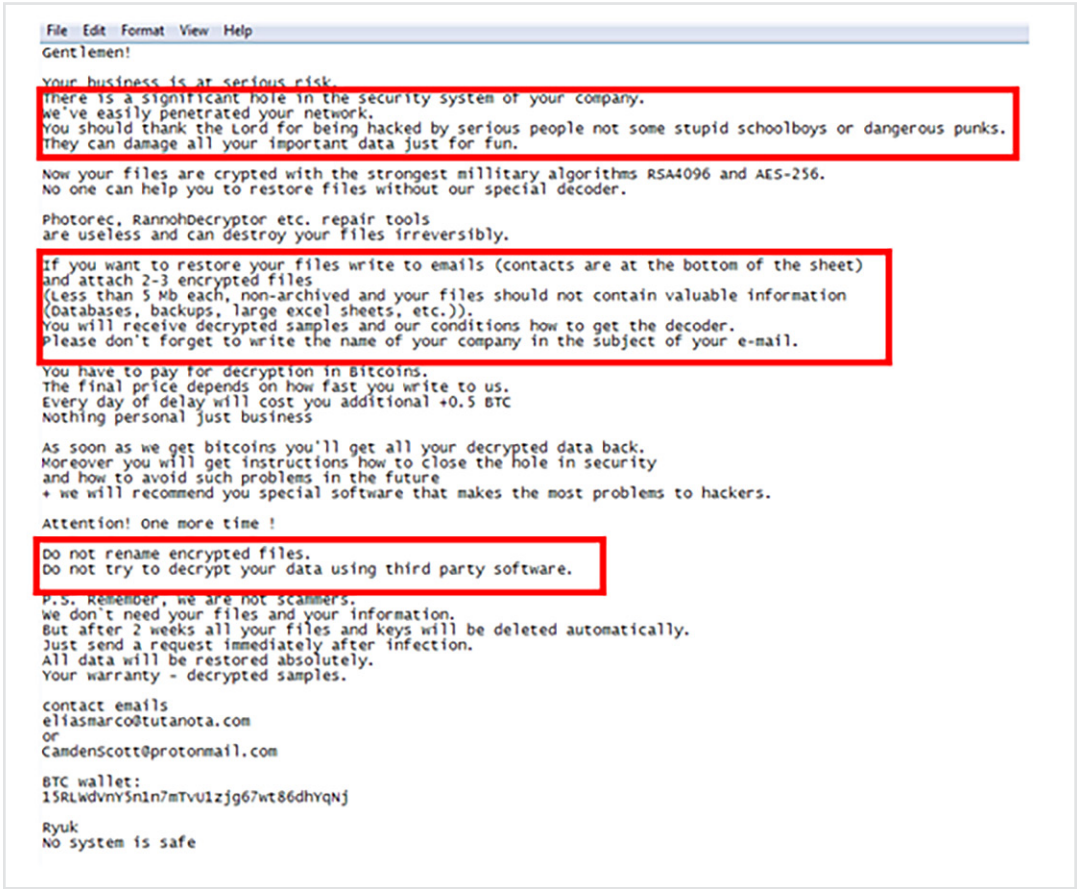
Bat files with uncommon names were used in attacks involving all three ransomware families.

- kill.bat – Used by MegaCortex, GoGalocker, Ryuk
- xaa.bat – Used by GoGalocker, Ryuk
- xab.bat – Used by GoGalocker, Ryuk
- xac.bat – Used by GoGalocker, Ryuk
- xaj.bat – Used by GoGalocker

Ransom Note Similarities:

Similarities have also been found in ransom notes

Figure 18: Ryuk Ransom Note



File Edit Format View Help

Gentlemen!

Your business is at serious risk.
There is a significant hole in the security system of your company.
We've easily penetrated your network.
You should thank the Lord for being hacked by serious people not some stupid schoolboys or dangerous punks.
They can damage all your important data just for fun.

Now your files are crypted with the strongest military algorithms RSA4096 and AES-256.
No one can help you to restore files without our special decoder.

Photorec, RannohDecryptor etc. repair tools
are useless and can destroy your files irreversibly.

If you want to restore your files write to emails (contacts are at the bottom of the sheet)
and attach 2-3 encrypted files
(Less than 5 Mb each, non-archived and your files should not contain valuable information
(Databases, backups, large excel sheets, etc.)).
You will receive decrypted samples and our conditions how to get the decoder.
Please don't forget to write the name of your company in the subject of your e-mail.

You have to pay for decryption in Bitcoins.
The final price depends on how fast you write to us.
Every day of delay will cost you additional +0.5 BTC
Nothing personal just business

As soon as we get bitcoins you'll get all your decrypted data back.
Moreover you will get instructions how to close the hole in security
and how to avoid such problems in the future
+ we will recommend you special software that makes the most problems to hackers.

Attention! One more time !

Do not rename encrypted files.
Do not try to decrypt your data using third party software.

P.S. Remember, we are not scammers.
We don't need your files and your information.
But after 2 weeks all your files and keys will be deleted automatically.
Just send a request immediately after infection.
All data will be restored absolutely.
Your warranty - decrypted samples.

contact emails
eliasmarco@tutanota.com
or
CamdenScott@protonmail.com

BTC wallet:
15RLWdVnY5n1n7mTvU1zjg67wt86dhYqNj

Ryuk
No system is safe

Figure 19: GoGalocker Ransom Note

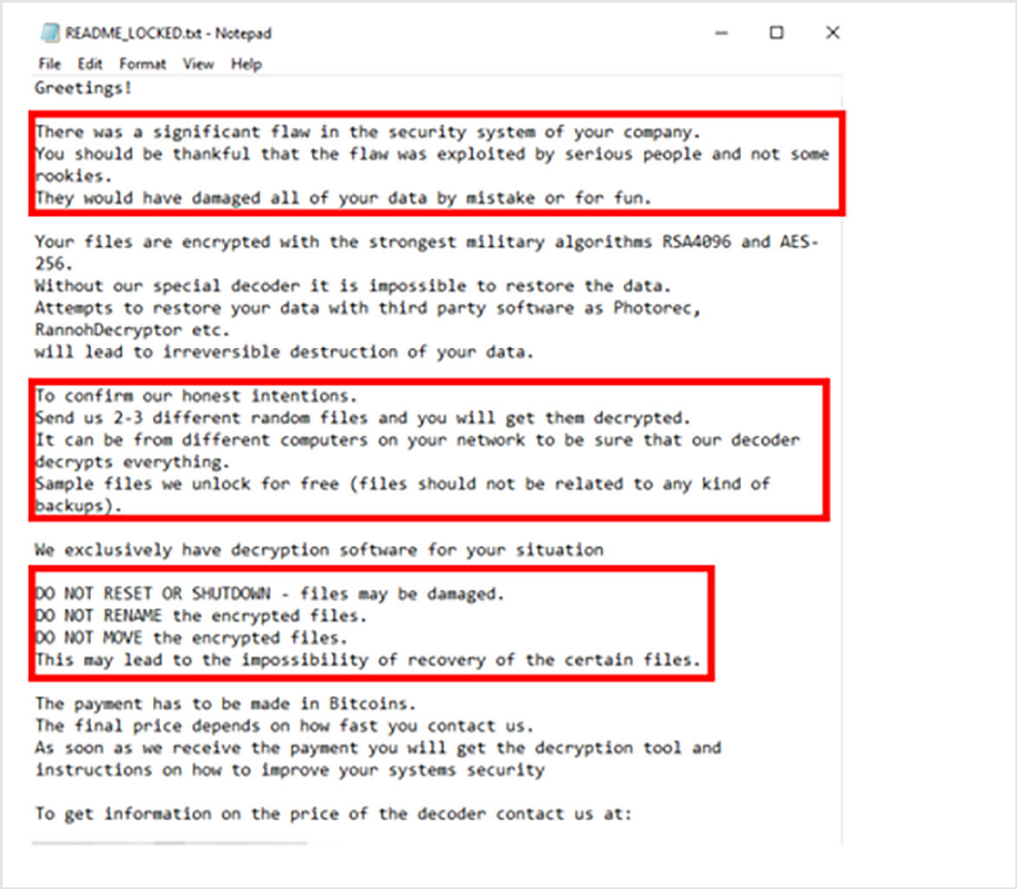
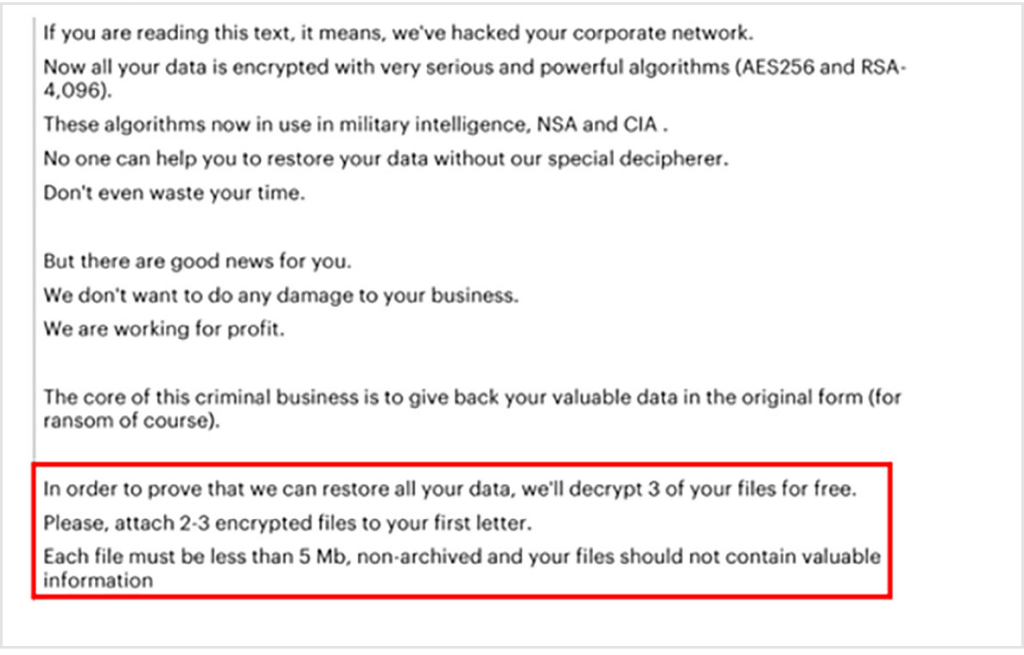


Figure 20: MegaCortex Ransom Note



Infection Vectors

Targeted ransomware groups use a diverse range of distribution methods. Because of the relatively low prevalence of targeted ransomware attacks, the infection vector can sometimes be difficult to establish. Targeted ransomware groups often take their cues from espionage groups in their methods for gaining a foothold on the victim's network.

Phishing

Phishing is one of the most widely utilized infection vectors, with emails sent to employees disguised as work-related correspondence (invoices, delivery confirmation, and so on). Some phishing campaigns may be indiscriminate, a wide-ranging trawl for victims of interest. In other cases, attackers may pre-select their victim and send spear-phishing emails to selected employees in the organization.

Spear-phishing campaigns may be tailored to the target, using subject matter relevant to the organization's business. If the recipient is tricked into opening a malicious attachment or following a malicious link, malware will be downloaded to the victim's machine, allowing the attackers to begin moving across the victim's network.

Malvertising

Hitherto not known as an infection vector for ransomware, malvertising has been leveraged during 2020 by the operators of WastedLocker. The group has been observed compromising media websites in order to serve malicious ads containing a JavaScript-based framework known as SocGholish which masquerades as a software update.

Vulnerability Exploitation

Another route on to an organization's network is exploiting vulnerable software running on public-facing servers. In most cases to date, zero-day vulnerabilities have not been used and the attackers exploited known vulnerabilities in unpatched software, such as JBoss or Apache web server. One of the primary users of this tactic was the now defunct SamSam group, which ceased operations in November 2019.

Secondary Infections

This is becoming an increasingly popular route into victim organizations. Cyber criminals are leveraging pre-existing botnets in order to gain a foothold on the victim's network. All it takes is for one computer on the network to be compromised by the botnet in order to provide a way in.

The attackers behind BitPaymer leveraged their own Dridex botnet, which was originally built to mount financial attacks, to give them a means of delivering the ransomware to organizations.

The Miner group, which is behind Ryuk, GoGalocker, and MegaCortex, has meanwhile used the Emotet botnet to mount its attacks and may have leased access from Emotet's operators.

Poorly Secured Services

Another infection vector comes from compromising poorly secured services. Crysis (also known as Dharma) has repeatedly been observed attacking organizations through poorly secured RDP services, taking advantage of leaked or weak credentials. The now defunct GandCrab group was observed scanning the internet for exposed MySQL databases that it was then infecting with malware.

Credential Theft and Lateral Movement

Targeted ransomware attacks can be broken down into four broad phases: initial compromise, privilege escalation/credential theft, lateral movement, and encryption/deletion of backups.

Lateral movement is a key phase. The higher the proportion of computers that are encrypted, the greater the likelihood of success from the attackers point of view.

Ransomware attackers tend to take their cues from espionage actors and deploy a similar range of tactics and tools when performing lateral movement. In order to reduce the risk of detection, many (but not all) will eschew custom malware and instead rely on 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 can be 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 is primarily used by attackers to move laterally on victim networks.
- **PsInfo:** Another Microsoft Sysinternals tool that allows the user to gather information about other computers on the network.
- **Windows Management Instrumentation (WMI):** Microsoft command line tool which can be used to execute commands on remote computers.
- **Mimikatz:** Freely available tool capable of changing privileges, exporting security certificates, and recovering Windows passwords in plaintext depending on the configuration.
- **Cobalt Strike:** Commodity malware that can be used to execute commands, inject other processes, elevate current processes or impersonate other processes, and upload and download files. It can also be used to perform credential dumping using ProcDump.
- **Metasploit:** Penetration testing framework that allows users to execute exploits on remote systems and deliver payloads.
- **AnyDesk:** Legitimate, publicly available remote desktop tool.
- **PuTTY:** A command-line utility used to create SSH sessions.

Conclusion

The profusion of groups carrying out targeted ransomware attacks combined with the evolution in tactics to include data theft along with encryption now means that targeted ransomware poses a significant threat to organizations. Ransom demands running into millions of dollars are now not unusual and even organizations who do not pay a ransom can sometimes face crippling cleanup costs along with reputational damage.

Defense in depth is key to blocking these kinds of attacks and knowing the attack chain utilized by most groups will help identify security priorities. Combining an EDR solution with Endpoint Protection will maximize your chances of discovering suspicious activity on your network before payloads can be deployed.

Protection

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

File-based Protection

- Ransom.Maze
- Ransom.Sodinokibi
- Ransom.BitPaymer
- Ransom.WastedLocker
- Ransom.Ryuk
- Ransom.Crysis
- Ransom.GoGalocker
- Ransom.MegaCortex
- Ransom.Robbinhood
- Hacktool.Mimikatz
- Backdoor.Cobalt (Cobalt Strike)
- Trojan.Agentemis (Cobalt Strike)

AI-based Protection

Symantec's Targeted Attack Cloud Analytics (part of Symantec's Endpoint Security Complete offering) leverages advanced machine learning to spot patterns of activity associated with targeted attacks.

Threat Hunting

Symantec's Threat Hunter team (part of Symantec's Endpoint Security Complete offering) actively analyzes Cloud Analytics alerts and investigates potential critical incidents. In June 2020, the Threat Hunter team identified dozens of early stage WastedLocker attacks and was able to notify affected organizations before the attackers could deploy their payload.

Endpoint Detection and Response (EDR)

Symantec EDR features Attack Chain Mitigation (ACM) provides enhanced early prevention capabilities. ACM focuses on behaviors rather than files and can strengthen defenses against spear phishing and use of living-off-the-land tools. For example, if Word doesn't normally launch PowerShell in the customer environment, then this should be placed in Block mode. EDR's UI allows customers to easily understand which behaviors are common and should be allowed, which are seen but should still be alerted on, and which are uncommon and should be blocked. Customers can also address gaps reactively as part of investigating and responding to incident alerts. The incident alert will show all behaviors that were observed as part of the breach and provides the capability to put this in block mode right from the incident details page.

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 that 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 to verify.
- **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 1: Dwell Time Analysis

Dwell time is the time between the attacker's initial access of the victim's environment up to the attempted execution of the ransomware payload. This provides data points on how much time is spent on the network by the attacker before encrypting the victim's data. In theory, this window of time is the last chance the victim has to identify the activity before falling victim to ransomware and provides additional data on how much time the adversary needs to spend staging the environment before the final attack phase. We analyzed attacks by five different ransomware families where we had data on dates of initial intrusion and attempted payload execution.

Ransomware	Dwell time (days)
Ryuk	14 days
BitPaymer	5 days
Maze	14 days
Sodinokibi	8 days
GoGalocker	2 days

Appendix 2: MITRE ATT&CK® Techniques

The following Mitre ATT&CK techniques have been used by targeted ransomware operators:

Group	Technique ID	Technique name	Technique use
Ryuk	T1134	Access Token Manipulation	Ryuk has attempted to adjust its token privileges to have the SeDebugPrivilege.
Ryuk	T1547	Boot or Logon Autostart Execution	Ryuk has used the Windows command line to create a Registry entry under HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run to establish persistence.
Ryuk	T1059	Command and Scripting Interpreter	Ryuk has used cmd.exe to create a Registry entry to establish persistence.
Ryuk	T1486	Data Encrypted for Impact	Ryuk has used a combination of symmetric (AES) and asymmetric (RSA) encryption to encrypt files. Files have been encrypted with their own AES key and given a file extension of .RYK. Encrypted directories have had a ransom note of RyukReadMe.txt written to the directory.
Ryuk	T1083	File and Directory Discovery	Ryuk has called GetLogicalDrives to emumerate all mounted drives, and GetDriveTypeW to determine the drive type.
Ryuk	T1562	Impair Defenses	Ryuk has stopped services related to anti-virus.
Ryuk	T1490	Inhibit System Recovery	Ryuk has used vssadmin Delete Shadows /all /quiet to to delete volume shadow copies and vssadmin resize shadowstorage to force deletion of shadow copies created by third-party applications.
Ryuk	T1036	Masquerading	Ryuk has constructed legitimate appearing installation folder paths by calling GetWindowsDirectoryW and then inserting a null byte at the fourth character of the path. For Windows Vista or higher, the path would appear as C:\Users\Public.
Ryuk	T1106	Native API	Ryuk has used multiple native APIs including ShellExecuteW to run executables,GetWindowsDirectoryW to create folders, and VirtualAlloc, WriteProcessMemory, and CreateRemoteThread for process injection.
Ryuk	T1057	Process Discovery	Ryuk has called CreateToolhelp32Snapshot to enumerate all running processes.

Group	Technique ID	Technique name	Technique use
Ryuk	T1055	Process Injection	Ryuk has injected itself into remote processes to encrypt files using a combination of VirtualAlloc, WriteProcessMemory, and CreateRemoteThread.
Ryuk	T1489	Service Stop	Ryuk has called kill.bat for stopping services, disabling services and killing processes.
Ryuk	T1016	System Network Configuration Discovery	Ryuk has called GetIpNetTable in attempt to identify all mounted drives and hosts that have Address Resolution Protocol (ARP) entries.
Maze	T1071	Application Layer Protocol	Maze has communicated to hard-coded IP addresses via HTTP.
Maze	T1059	Command and Scripting Interpreter	The Maze encryption process has used batch scripts with various commands.
Maze	T1486	Data Encrypted for Impact	Maze has disrupted systems by encrypting files on targeted machines, claiming to decrypt files if a ransom payment is made. Maze has used the ChaCha algorithm, based on Salsa20, and an RSA algorithm to encrypt files.
Maze	T1568	Dynamic Resolution	Maze has forged POST strings with a random choice from a list of possibilities including “forum”, “php”, “view”, etc. while making connection with the C2, hindering detection efforts.
Maze	T1562	Impair Defenses	Maze has disabled dynamic analysis and other security tools including IDA debugger, x32dbg, and OllyDbg.
Maze	T1070	Indicator Removal on Host	Maze has used the “Wow64RevertWow64FsRedirection” function following attempts to delete the shadow volumes, in order to leave the system in the same state as it was prior to redirection.
Maze	T1490	Inhibit System Recovery	Maze has attempted to delete the shadow volumes of infected machines, once before and once after the encryption process.
Maze	T1106	Native API	Maze has used several Windows API functions throughout the encryption process including IsDebuggerPresent, TerminateProcess, Process32FirstW, among others.
Maze	T1027	Obfuscated Files or Information	Maze has decrypted strings and other important information during the encryption process. Maze also calls certain functions dynamically to hinder analysis.
Maze		Binary Padding	Maze has inserted large blocks of junk code, including some components to decrypt strings and other important information for later in the encryption process.
Maze	T1057	Process Discovery	Maze has gathered all of the running system processes.
Maze	T1055	Process Injection	Maze has injected the malware DLL into a target process.
Maze	T1082	System Information Discovery	Maze has checked the language of the infected system using the “GetUSerDefaultUILanguage” function.
Maze	T1049	System Network Connections Discovery	Maze has used the “WNetOpenEnumW”, “WNetEnumResourceW”, “WNetCloseEnum” and “WNetAddConnection2W” functions to enumerate the network resources on the infected machine.
Maze	T1047	Windows Management Instrumentation	Maze has used “wmic.exe” attempting to delete the shadow volumes on the machine.
RobbinHood	T1059	Command and Scripting Interpreter	RobbinHood uses cmd.exe on the victim’s computer.

Group	Technique ID	Technique name	Technique use
RobbinHood	T1486	Data Encrypted for Impact	RobbinHood will search for an RSA encryption key and then perform its encryption process on the system files.
RobbinHood	T1562	Impair Defenses	RobbinHood will search for Windows services that are associated with antivirus software on the system and kill the process.
RobbinHood	T1070	Indicator Removal on Host	RobbinHood disconnects all network shares from the computer with the command net use * /DELETE /Y.
RobbinHood	T1490	Inhibit System Recovery	RobbinHood deletes shadow copies to ensure that all the data cannot be restored easily.
RobbinHood	T1489	Service Stop	RobbinHood stops 181 Windows services on the system before beginning the encryption process.
SamSam	T1059	Command and Scripting Interpreter	SamSam uses custom batch scripts to execute some of its components.
SamSam	T1486	Data Encrypted for Impact	SamSam encrypts victim files using RSA-2048 encryption and demands a ransom be paid in Bitcoin to decrypt those files.
SamSam	T1070	Indicator Removal on Host	SamSam has been seen deleting its own files and payloads to make analysis of the attack more difficult.
SamSam	T1027	Obfuscated Files or Information	SamSam has been seen using AES or DES to encrypt payloads and payload components.
GoGalocker	T1531	Account Access Removal	GoGalocker has been observed changing account passwords and logging off current users.
GoGalocker	T1486	Data Encrypted for Impact	GoGalocker has encrypted files, including core Windows OS files, using RSA-OAEP MGF1 and then demanded Bitcoin be paid for the decryption key.
GoGalocker	T1562	Impair Defenses	GoGalocker installation has been immediately preceded by a “task kill” command in order to disable anti-virus.
GoGalocker	T1070	Indicator Removal on Host	GoGalocker has been observed deleting its original launcher after execution.
GoGalocker	T1570	Lateral Tool Transfer	GoGalocker has been observed moving around the victim network via SMB, indicating the actors behind this ransomware are manually copying files form computer to computer instead of self-propagating.
GoGalocker	T1553	Subvert Trust Controls	GoGalocker has been signed with stolen certificates in order to make it look more legitimate.
GoGalocker	T1529	System Shutdown/ Reboot	GoGalocker has been observed shutting down infected systems.

SED-TR-WP103 October 7, 2020