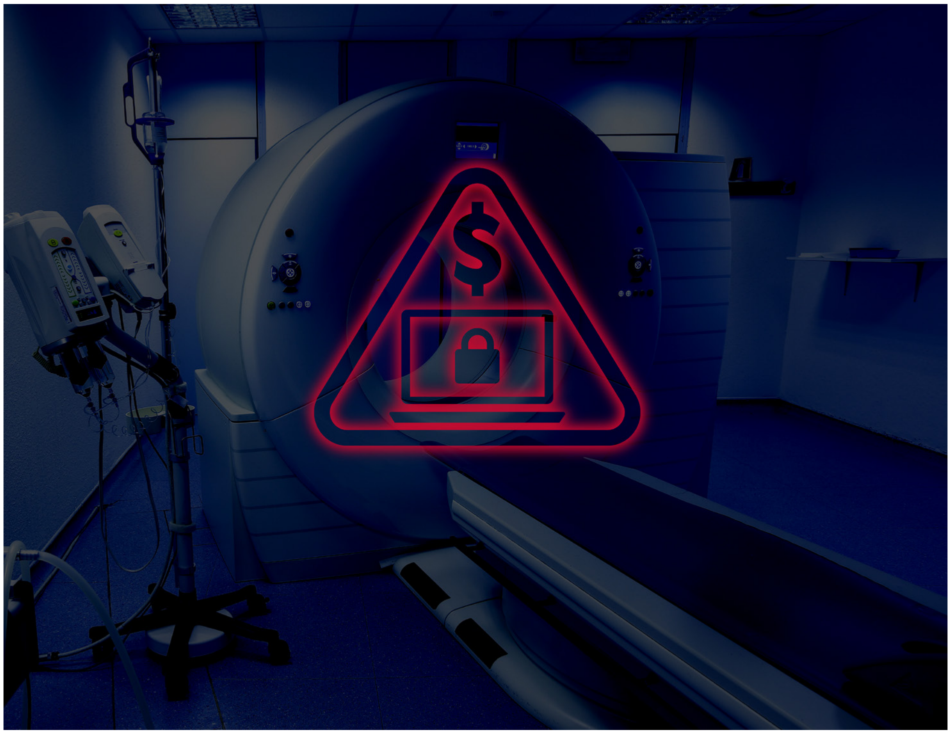
White Paper

Symantec
A Division of Broadcom

The Ransomware Threat

By Threat Hunter Team

Table of Contents



Introduction

Ransomware continues to pose a major threat for enterprises and other large organizations, with targeted ransomware attacks in particular proving to be highly lucrative for cyber criminals. Major ransomware attacks prompting multi-million dollar ransom payouts have attracted a growing number of malicious actors into the ransomware space.

Over the past year, ransomware attackers have grown increasingly ambitious and have mounted a number of high-profile, extremely destructive attacks. The attack against Colonial Pipeline in the U.S. in May 2021 caused significant disruption and prompted concerns about the nation's fuel supplies. In the same month, an attack on Ireland's national health service, the Health Service Executive, forced it to cancel thousands of appointments. In the middle of a global pandemic, staff had to keep paper records as computers were kept offline until the network was cleaned up.

While these attacks paint a picture of ransomware gangs operating with impunity, the disruption they caused did have a political impact, with U.S. President Joe Biden urging his Russian counterpart Vladimir Putin to rein in ransomware attackers, many of whom are believed to be located in Russia.

The glare of publicity surrounding such high-profile attacks and subsequent law enforcement operations is believed to have contributed to the disappearance of some of the more active ransomware threats during 2021, include Darkside, Sodinokibi (aka REvil), and Egregor.

While the departure of any threat is always a welcome development, it should not be assumed that ransomware activity will diminish. Frequently, attackers who have departed the scene will re-emerge with a new toolset, while new attackers will emerge trying to take the market space occupied by departing players. Any change in the threat landscape means that there's a period of uncertainty where network defenders aren't aware of who the big players are going to be and what tactics they are going to use.

Two trends are a particular source of concern. Although the phenomenon of ransomware-as-a-service (RaaS) is not new, its increasing adoption as part of the operations of most major ransomware developers has contributed to the proliferation of targeted ransomware attacks. Not only does RaaS prompt more attacks, but it also multiplies the number of tools, tactics, and procedures (TTPs) being employed to deliver ransomware. Each ransomware threat could be delivered by one of multiple different threat actors, many of whom will use differing TTPs. RaaS has also lowered the entry barriers for less skilled actors to enter the arena, adding to the number of attackers.

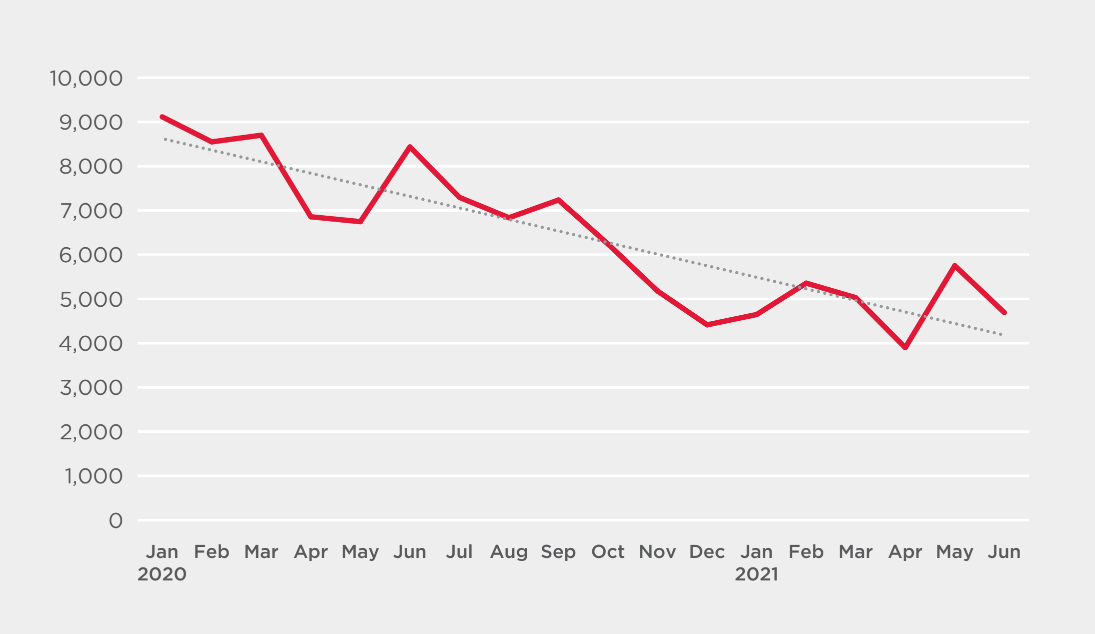
Secondly, a growing a number of ransomware operators are collaborating with other malware developers, most notably financial fraud botnets, to gain access to victims. Major botnets often have a vast reach and can potentially offer ransomware gangs a deep pool of potential victims from which to fish from.

Ransomware groups are now sophisticated threat actors, capable of building relationships with other attackers in order to further their reach and employing an evolving array of tools and tactics in order to make their attacks more effective. Successfully defending against ransomware attacks now requires defense in depth from organizations, along with a deep understanding of how these attacks unfold.

Ransomware Trends

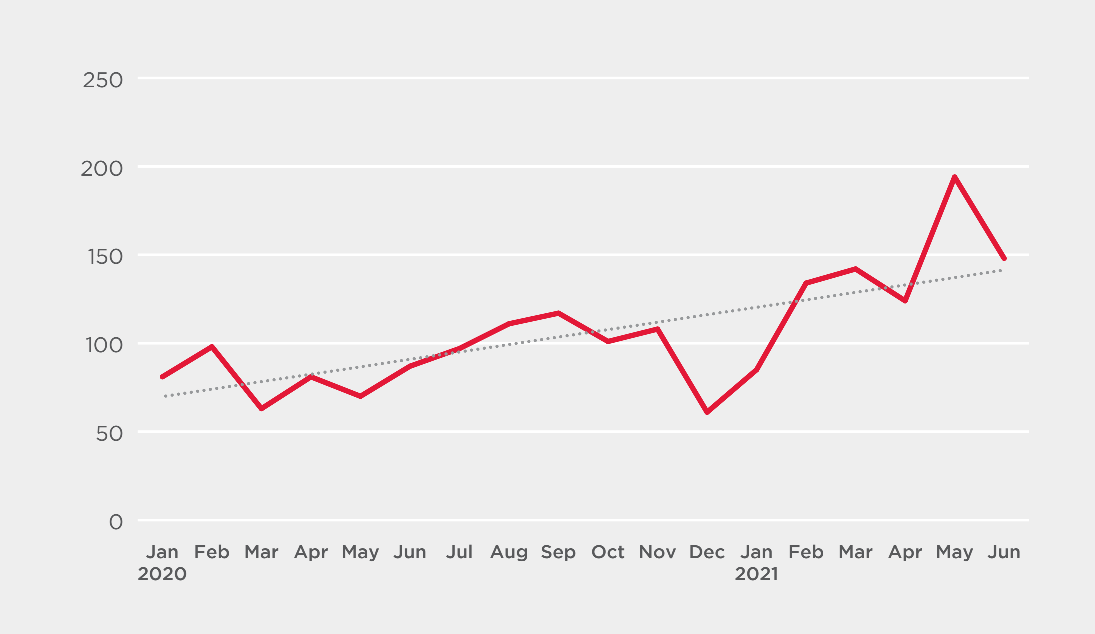
Over the past number of years, there has been a marked shift in the ransomware threat landscape and that trend has continued in recent times. In the past 18 months, the total number of ransomware attacks detected and blocked by Symantec has almost halved, from 9,116 in January 2020 to 4,692 in June 2021.

Figure 1: All Ransomware Detections January 2020 to June 2021



While any reduction in ransomware activity is to be welcomed, the overall decline in numbers is accounted for by the ongoing decline of relatively unsophisticated, indiscriminate attacks. A growing number of threat actors are now focusing on targeted ransomware attacks, where a single organization at a time is attacked and the attackers attempt to encrypt as many computers as possible on the network in the hope of extracting a high-value ransom. Although relatively small in number, these attacks are far more damaging to organizations than indiscriminate attacks, where usually only a small number of computers may be affected.

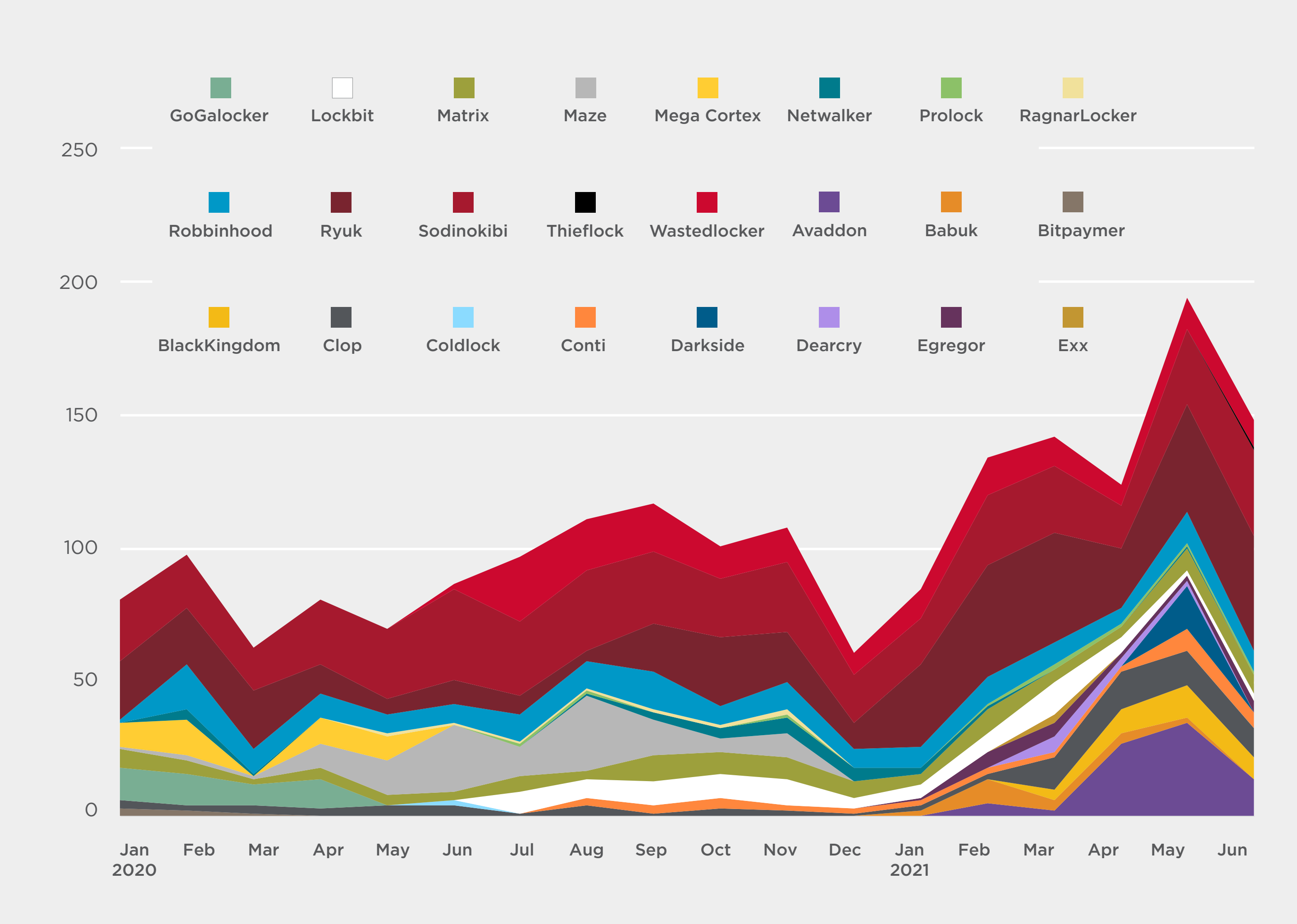
Figure 2: Number of Organizations Affected by Targeted Ransomware Attacks, January 2020 to June 2021



The statistics for targeted attacks tell a different story, with the number of organizations affected by targeted ransomware attacks up by 83% over the past 18 months, from 81 in January 2020 to 148 in June 2021. The real number of targeted ransomware attacks is much higher. Some ransomware families have been deployed via spam campaigns in addition to being used in targeted attacks. There is no way of establishing how many victims of these threats were infected by targeted attacks and how many were infected through other means, meaning they cannot be counted among targeted attacks.

In addition to this, confirmed attacks from known targeted ransomware families are probably only a representative sample of the overall number of attacks involving these threats. Many targeted ransomware attacks are halted before payload deployment, meaning they may not be identified as ransomware. In addition, 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.

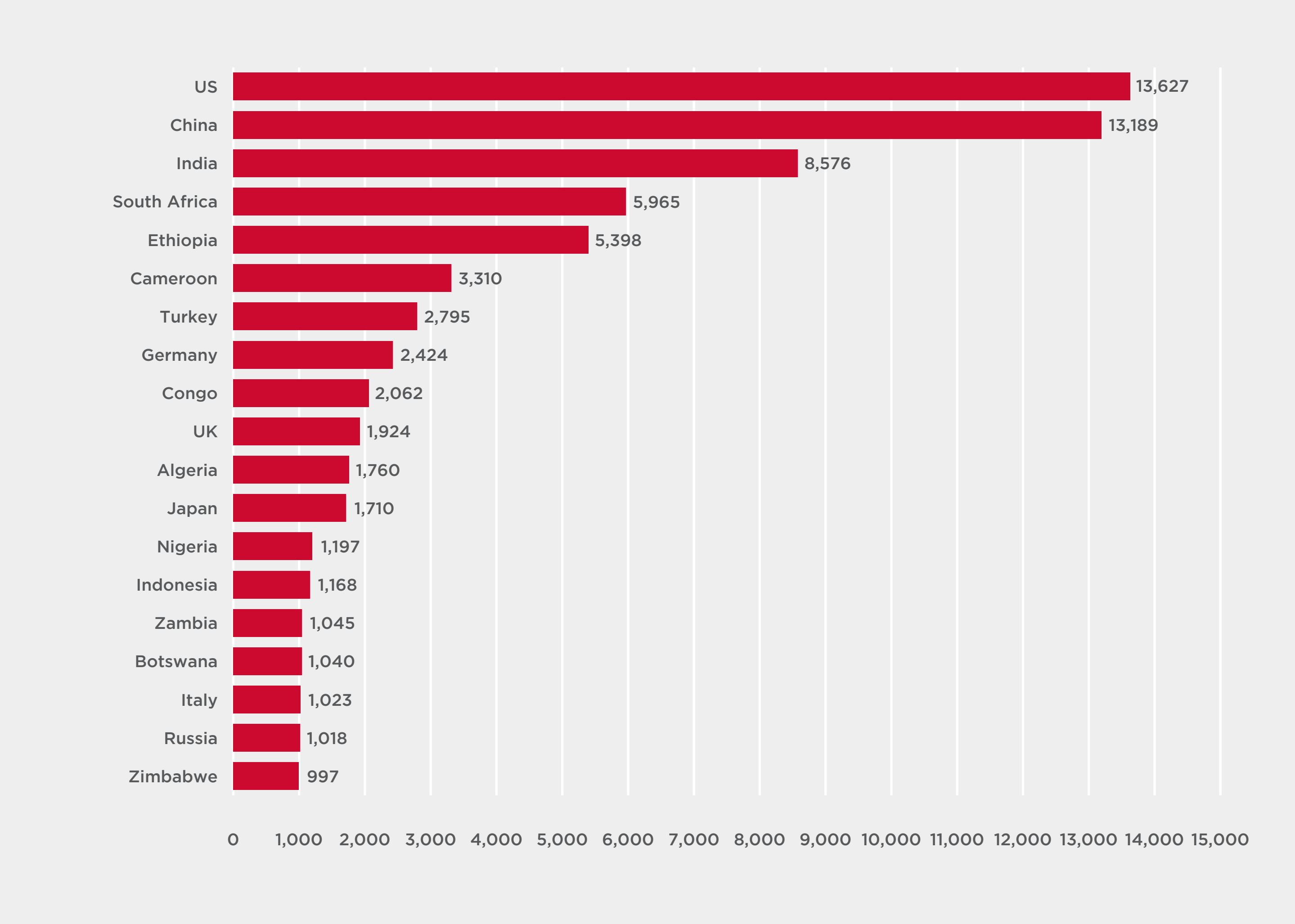
Figure 3: Number of Organizations Affected by Targeted Ransomware Attacks, by Family, January 2020 to June 2021.



When targeted attacks are broken down by ransomware family, two trends become apparent. Firstly, the profusion of new threats has continued and is contributing to the overall increase in attacks. Of the 24 groups analyzed, nine were active in January 2020, but 13 were active in June 2021. Secondly, a small number of prolific threat actors such as Ryuk, Sodinokibi, and, more recently, Avaddon, have accounted for a large proportion of attacks.

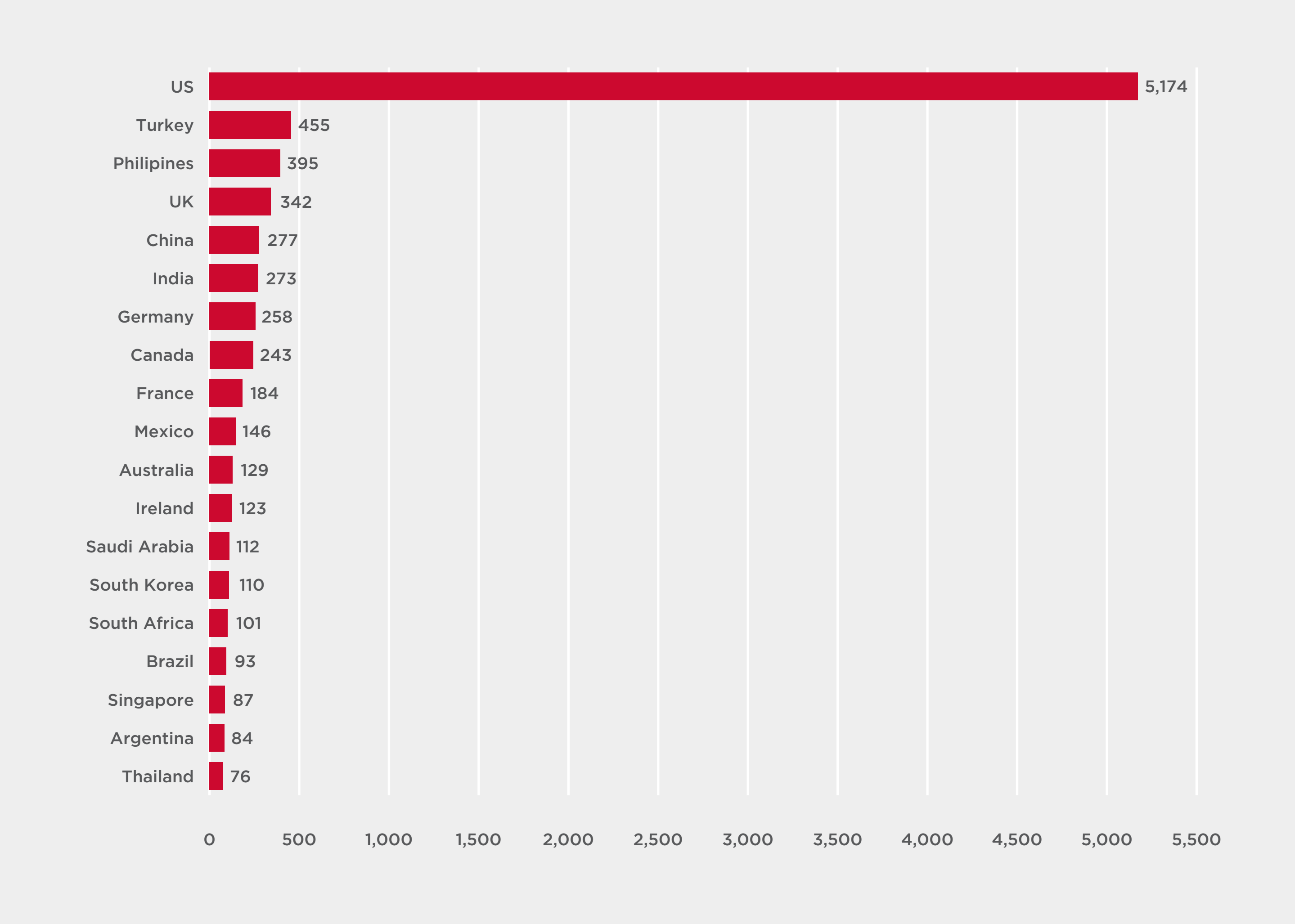
Again, it should be stressed that these statistics should be treated as a representative sample of attacks blocked by Symantec. The majority of attacks are likely to be blocked at the pre-ransomware deployment stage or before they can be associated with any particular family of ransomware.

Figure 4: Overall Number of Ransomware Detections by Country, January 2020 to June 2021



Another key trend emerges when examining the location of ransomware victims. While the U.S. is the most frequently attacked country, ransomware attacks in general are quite commonplace worldwide, with a notable number of African countries appearing in the top 20 over the past 18 months. The presence of Africa on the list is largely accounted for by the fact that it appears to be a particular focus for attackers mounting indiscriminate ransomware attacks, such as through spam email campaigns or exploits of known vulnerabilities.

Figure 5: Number of Targeted Ransomware Detections by Country, January 2020 to June 2021



A very different picture emerges when analyzing only targeted ransomware attacks. The U.S. is by far the most affected country, with more than 11 times more attacks over the past 18 months than the next most affected country (Turkey).

The concentration of victims in the U.S. is not surprising. As a large, affluent nation with a highly developed business sector, it is naturally a prime target for targeted ransomware attacks. Several ransomware gangs are on record as saying they mostly, if not exclusively, targeted organizations in the U.S.

While it may be a surprise that Turkey and the Philippines also figure prominently, it is consistent with previous years' statistics, where both also featured in the top five.

It should be noted that unlike targeted ransomware stats listed earlier that counted the number of organizations, this statistic represents a count of computers on which a targeted ransomware family was detected. 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.

Compounding the Threat: Ransomware-as-a-Service

A key factor in driving the threat posed by ransomware was the advent of ransomware-as-a-service (RaaS). While a successful targeted ransomware attack can be devastatingly effective, one of the drawbacks it has for the attacker is that it can be quite labor intensive. The various steps involved in a typical attack, including credential theft, privilege escalation, lateral movement, data exfiltration, deletion of backups, and payload deployment often require active participation on the part of the attacker. Consequently, the number of attacks a ransomware actor can perform is limited by their available workforce.

Successful ransomware authors realized that they could boost their revenues by recruiting other attackers, known as affiliates, and provide them with access to their tools in exchange for a cut of the ransom payment. This business model is now highly developed and most of the high-profile targeted ransomware developers operate some kind of RaaS program.

The available evidence suggests that there are varying types of affiliate relationships, but the basic template currently involves ransomware authors offering access to the ransomware itself, hosting for breached data, and handling of ransom negotiations. In some cases, it's been reported that ransomware developers provide an entire playbook for affiliates. However, often affiliates will use their own TTPs. Symantec has frequently seen actors using the same TTPs but different payloads over time. There is also some evidence of actors being affiliated to more than one ransomware developer at the same time (see Case Study: Shifting allegiances among affiliates).

While some ransomware developers appear to solely work under the RaaS business model, others are more hands-on and will continue to mount attacks themselves. The nature of what's required from affiliates may also vary. Several have been observed advertising for "access brokers", suggesting that they're simply looking for a means of entry to potential victim networks and will to carry out the rest of the attacks themselves.

The advent of affiliates makes the ransomware threat landscape more complex for network defenders, since each ransomware threat could be delivered by one of multiple different threat actors, many of whom will use differing TTPs.

Case Study: Shifting Allegiances Among Affiliates

Most ransomware affiliates appear not to be exclusively tied to a single ransomware developer. When a ransomware developer goes offline or retires, many of their affiliates will move to another RaaS operator.

For example, when the Leafroller (aka REvil) group suddenly took its Sodinokibi ransomware operation offline in early July 2021, it appears that some of its affiliates moved to rival operations. Following Sodinokibi's disappearance, attacks involving LockBit have increased notably, and Symantec found evidence that at least one former Sodinokibi affiliate was now using LockBit. This attacker used consistent TTPs to deliver Sodinokibi to victims until July of 2021, at which point the payload switched to LockBit.

Attacks from this actor begin with a file named mimi.exe, which is an installer that drops a number of password-dumping tools. Immediately prior to the ransomware being launched, a large number of commands are executed to disable various services, block access to Remote Desktop Protocol (RDP), delete shadow copies etc. This actor consistently names their ransomware payload as "svhost.exe" and this practice has been maintained following their transition to LockBit.

Ransomware Threat Actors

Miner

Aliases: Wizard Spider

Ransomware families: Ryuk, Conti, GoGalocker (inactive), MegaCortex (inactive)

Active since: 2014

Miner is believed to be active since at least June 2014 when it began using the Dyre banking Trojan in financial fraud campaigns. Dyre became inactive in November 2015, but a new financial Trojan known as Trickbot appeared in September 2016. It was subsequently linked to the Miner group because Trickbot and Dyre appeared to share common authorship.

Trickbot was originally developed as a financial Trojan capable of performing man-in-the-browser (MitB) attacks to intercept online transactions when victims are using online banking applications. It has since been repurposed for use as a credential stealer and acting as a distribution channel for other malware.

Miner also introduced new malware known as BazarLoader and BazarBackdoor in April 2020. Like Trickbot, BazarLoader is spread through spam email campaigns and can deliver the second-stage BazarBackdoor payload. Unlike Trickbot, the Bazar family appears to have been primarily developed for malware distribution.

During 2018, the group branched out into targeted ransomware, using the Ryuk ransomware. Ryuk is based on the older Hermes ransomware family, which it appears to have acquired from the original developer.

Ryuk attacks have frequently employed both Trickbot and the Emotet botnets as infection vectors. 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, the attackers gain administrative access to domain controllers. The attackers then use batch files, deployed via PsExec, to disable and delete backup/restoration capabilities and security services throughout the environment.

During 2019, Miner began using two new ransomware families, GoGalocker (aka LockerGoga) and MegaCortex. Both shared code with Ryuk and analysis by Symantec found that there was overlap in the command and control (C&C) infrastructure used by all three ransomware families. Attacks involving GoGalocker and MegaCortex ceased in early 2020.

Miner was then linked to the Conti ransomware, which first appeared in December 2019. There has been some speculation that Conti was created specifically for use by affiliates, under the RaaS model, but this remains unconfirmed.

Both Ryuk and Conti have been distributed using very similar TTPs. A May 2021 investigation by Symantec found significant overlap in tools used to deliver both. The attacks involved extensive use of variants of Cobalt Strike. In some cases, the infection vector appears to be via the IcedID malware, which delivers malware known as Longlist, which in turn is used to install Cobalt Strike.

Case Study: Social Engineering Element in BazarLoader Attacks

A recent attack campaign involving the Miner group's BazarLoader malware saw the attackers employ a degree of social engineering in order to push malware on to the victim's network. The campaign targeted a number of large organizations during July 2021 and began with the appearance of a malicious Excel file on one computer on the victim's network.

While the initial infection vector was not confirmed in all cases, in one organization the attack began when a spear-phishing email was sent to an employee. The email alleged that the recipient had been involved in a recent car accident and a claim had been made against their motor insurance. They were given a number to call for further information. The email was convincing enough for the employee to call the number. The subsequent phone call directed them to a URL. This URL led to the download of a malicious Excel file.

The tactic of using a phone call to get the target to download a suspicious file is a bid to avoid detection. A suspicious attachment or link in an email from an unknown sender is likely to either be automatically blocked by security software or raise the suspicions of the recipient. A URL that is manually entered by an end-user may not be as likely to raise red flags.

The attackers created a new directory on the compromised computer and copied Certutil to it under a new name:

CSIDL_COMMON_APPDATA\epvv2e\epvv2e.exe

This masquerading technique was previously used in the Kaseya attack and is intended to hide malicious use of Certutil.

Certutil is used to download a malicious DLL file. This was identified as BazarLoader. Symantec did not observe the attackers successfully deploying a payload. However, the association of these TTPs with previous ransomware attacks suggests a strong possibility of early-stage ransomware activity, most likely involving Ryuk.

Leafroller

Aliases: REvil

Ransomware families: Sodinokibi (inactive), Gandcrab (inactive)

Active since: 2018

Leafroller conducted targeted ransomware attacks using the Sodinokibi ransomware between April 2019 and July 2021. The group is known to work with affiliates, using the RaaS model. Like many ransomware groups, Leafroller and its affiliates routinely steal victim data prior to encryption and then post a sample to publicly available websites. The attackers then attempt to apply further pressure to extort the victim by threatening to post sensitive information if they don't pay the ransom.

Prior to creating Sodinokibi, the group was involved in attacks involving an older strain of ransomware Gandcrab, having acquired its source code from the original developer. Some of the affiliates it shared Gandcrab with continued with the group when it transitioned to Sodinokibi.

Leafroller is known for targeting high-profile organizations to maximize the amount of ransom they can extort. One of its most notable victims was Travelex, a foreign exchange service, which was attacked in January 2020 and generated a $2.3 million ransom for the ransomware operators.

Leafroller also has a reputation for frequently trialing new TTPs. During 2020, it was observed scanning victim networks for credit card or point of sale (POS) software. It was not clear if the attackers were targeting this software for encryption or data theft. In July 2021, Sodinokibi was used in a novel ransomware supply chain attack involving Kaseya software (see Case Study: Ransomware supply chain attack).

Less than two weeks after the Kaseya attack, infrastructure and websites belonging to Leafroller went offline. Both dark net and clear net infrastructure associated with the group was affected, including ransom negotiation websites, data breach websites, and C&C servers. The reason for the group's disappearance remains unclear. However, at the time of writing, there has been no evidence of new Sodinokibi activity.

Hispid

Aliases: EvilCorp, Indrik Spider, TA505

Ransomware families: BitPaymer (retired), DoppelPaymer, WastedLocker, Hades, Phoenix Locker

Active since: 2011

Hispid are veteran cyber crime actors, active since approximately 2011. The group was originally involved in financial fraud, having been responsible for the Dridex banking Trojan. At its height, Dridex was one of the most prolific cyber crime threats, being distributed in massive spam runs that went to millions of email addresses.

At some point around 2017, the group shifted its focus to targeted ransomware, introducing the BitPaymer ransomware family. It later introduced a second ransomware family known as DoppelPaymer which was based around the same code, albeit with some minor differences. It has been reported that DoppelPaymer was developed for use by affiliates, but Symantec has not been able to confirm this.

In a similar fashion to how Miner continued to use Trickbot, Hispid continued to use Dridex for a time after its move to ransomware, repurposing the malware for use as a precursor tool in ransomware attacks.

In December 2019, two Russian nationals were indicted on multiple charges in the U.S. relating to the group's activities. A $5 million reward was offered for information leading to their arrest or conviction.

In May 2020, Hispid retooled and introduced a new family of ransomware known as WastedLocker. Attacks began with a malicious JavaScript-based framework known as SocGholish which masquerades as a software update. An investigation by Symantec in June 2020 found SocGholish on more than 150 compromised websites, including dozens of U.S. newspaper websites.

Once the attackers had a foothold on the victim's network, PowerShell was used to download and execute a loader. The loader contained a .NET injector along with a loader for Cobalt Strike Beacon.

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 was renamed by the attackers to a random name. This command then searched for all the computer objects in the Active Directory database.

Privilege escalation was 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 used 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 was also used to carry out credential dumping using ProcDump and to empty log files.

In order to deploy the ransomware, the attackers used 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 was then used to launch PowerShell, which used the win32_service WMI class to retrieve services and the net stop command to stop these services. After Windows Defender was disabled and services had been stopped across the organization, PsExec was used to launch the WastedLocker ransomware itself, which then began encrypting data and deleting shadow volumes.

In March 2021, the group introduced a new variant of ransomware dubbed Hades, which had significant code overlap with WastedLocker. It is likely that Hispid developed the Hades ransomware in response to sanctions imposed by the U.S. Treasury Department's Office of Foreign Assets Control (OFAC) in 2019, which prohibited victims from making payments to the threat group.

At the time of writing, the group is reportedly regularly renaming its ransomware due to fears that victims will not pay lest they violate U.S. sanctions. Hades was later rebranded as Phoenix Locker and, as of June 2021, was reportedly using the name PayloadBin, which is already associated with the Babuk group, presumably to fool victims into thinking they'd been infected by another actor.

Thysanura

Aliases: Avaddon

Ransomware families: Avaddon

Active since: 2019

Active since at least 2019, Thysanura is known for mounting targeted ransomware campaigns against large organizations. The group frequently compromises victims using remote access login credentials—such as RDP and Virtual Private Networks (VPN).

Thysanura operates on a RaaS model, which is advertised on Russian-language cyber-crime forums. The group uses multiple extortion tactics to pressure victims into paying.

As well as encrypting files, it will also threaten to leak information stolen from victims and in January 2021, it began telling victims that didn't pay a ransom that it would hit them with distributed denial of service (DDoS) attacks. To date, it has yet to be confirmed if the group has ever followed through on this threat.

After the attackers gain access to a victim's network, they map the network and identify backups for deletion and/or encryption. The following tools are used by attackers using Avaddon to compromise victims:

- PowerShell
- WMIC.exe (WMI -Windows Management Instrumentation)
- Svchost.exe (Service host system process)
- Taskhost.exe (Host protocol)

On June 11, 2021, the group announced it was shutting down its operation and released the decryption keys for its victims. The gang sent news outlet Bleeping Computer almost three thousand decryption keys, after which the security firm Emsisoft produced a free, public decryption tool. At the time of writing, it remains unclear as to whether the group's departure is permanent.

Syrphid

Aliases: LockBit

Ransomware families: Lockbit

Active since: 2019

The LockBit ransomware first appeared in September 2019 when it was initially known as ABCD, after the file extension it was using on encrypted files. In January 2020, Syrphid expanded its operations by shifting to a RaaS business model through the creation of an affiliate program.

Attackers using LockBit are known to compromise organizations using brute-force attacks against web servers running an outdated VPN service. It has also been reported to use mass vulnerability scanning, phishing, and credential stuffing as vectors. It also reportedly buys access to already-compromised servers on underground forums.

In some cases, the attackers will brute forced administrator credentials in order to traverse the network. They have also been known to use post-exploitation frameworks, for privilege escalation and lateral movement.

Before encrypting files, Syrphid will attempt to identify sensitive data on the target network and export it to an external hosting service. Affiliates use a unique build of the ransomware for each victim organization.

Attacks involving Lockbit increased markedly in July 2021 and there is some evidence to suggest that Syrphid was attempting recruit former Sodinokibi affiliates (see Case Study: Shifting allegiances among affiliates).

Snakefly

Aliases: Clop

Ransomware families: Clop

Active since: 2019

Snakefly is known for developing the Clop ransomware and frequently leverages distribution channels owned by Hispid (aka Evil Corp). The group has been linked to some high-profile incidents, including an attack on the University of Maastricht in 2019.

The group's attacks generally begin with a malicious email that is sent from a previously compromised account to make it more convincing. This email contains an HTML attachment that redirects to a compromised website that then delivers a document containing a malicious macro that drops the Get2 loader. This then downloads the SDBot malware or other remote access tools (RATs) to assist the attackers in moving laterally across the network, exfiltrate data, and download the Clop ransomware.

Some of the ransomware payloads have a signed certificate that can help them appear legitimate and potentially bypass security measures. Once Clop is executed, it searches for security products to delete. It has been seen by a third party deleting or stopping security products from Malwarebytes, ESET, and Microsoft. The ransomware encrypts files and adds a .clop extension to infected files, before placing a ransom note on the machine.

It is also known to exfiltrate data from victims prior to encryption and threaten to release it unless a ransom is paid. Like most ransomware groups these days, the group also runs a Clop data leaks website where it publishes data stolen from victims who have refused to pay a ransom.

Coreid

Aliases: Darkside

Ransomware Families: Darkside, BlackMatter (unconfirmed)

Active since: 2020

Coreid was, for a brief period of time, one of the most prolific targeted ransomware threats and was used in a number of ambitious attacks, most notably the May 2021 attack on Colonial Pipeline that disrupted fuel supplies to the East Coast of the U.S.

Coreid operated under a RaaS model, working with affiliates to conduct ransomware attacks and takes a share of the profits. Like most ransomware actors, attacks linked to Coreid steal victims' data and the group then threatens to publish it to further pressure victims into paying the ransom demand.

Once on a victim's network, attackers using Darkside generally begin exfiltrating data, credentials, and other sensitive information. The attackers also attempt to move laterally across the network to gain access to the domain controller (DC). Once on the DC they exfiltrate sensitive information and also used PowerShell to download the DarkSide binary.

The attackers are known to create a shared folder using the company's name on the DC itself, and copy the Darkside binary to it. Subsequently, the attackers use BITSAdmin to distribute the ransomware binary from the shared folder to other computers on the network.

Coreid affiliates use TOR to communicate with victims and manage administration of the ransomware. Coreid reportedly encourage their affiliates to request Monero in ransomware demands, presumably due to that cryptocurrency's high level of anonymity.

Coreid appeared to become inactive following the Colonial attack after some of its infrastructure was taken offline.

In late July 2021, media reports linked Coreid to a new ransomware threat named BlackMatter. The ransomware is believed to use the same encryption routines as used by Darkside. In an interview with Recorded Future, BlackMatter's developer denied the link, saying "we are familiar with the Darkside team from working together in the past but we are not them, although we are intimate with their ideas." However, Blockchain analysis firm Chainalysis also found financial links between the two threats and concluded that BlackMatter was created by Coreid. Symantec's assessment is that it is too early yet to make a definitive attribution on BlackMatter.

Hornworm

Aliases: RagnarLocker, Viking Spider

Ransomware Families: RagnarLocker

Active since: 2020

Hornworm is associated with the RagnarLocker ransomware. RagnarLocker first appeared in early 2020 and was the subject of an FBI flash alert in November 2020. The FBI reported that it had encrypted computers on a large corporation's network and demanded an $11 million ransom, threatening to release 10 TB of stolen data if the ransom wasn't paid. Since then, it has mounted ransomware attacks against a range of other organizations in the United States.

In a bid to avoid detection, RagnarLocker is reported to be deployed as a full virtual machine on each infected computer. In some cases, the payload was delivered in an MSI package, which includes a working installation of an old Oracle VirtualBox (Sun xVM VirtualBox version 3.0.4) and a virtual disk image file (VDI) named micro.vdi— an image of a stripped-down version of the Windows XP SP3 operating system, called MicroXP v0.82. The image includes a 49 kB ransomware payload. While Hornworm may have pioneered this tactic, Symantec has since observed attackers using other payloads also attempt to run them from virtual machines.

RagnarLocker appends encrypted files with the extension .RGNR_<ID>, where <ID> is a hash of the computer's NETBIOS name. The attackers, identifying themselves as RAGNAR_LOCKER, leave a .txt ransom note on computers, with instructions on how to pay the ransom and receive a decryption key. The group is known to frequently change obfuscation techniques and has VMProtect, UPX, and custom packing algorithms.

Hornworm reportedly exfiltrates data from victim organizations prior to encryption and threatens to release this data unless a ransom is paid. It uses a dedicated data leak website for this purpose, hosted on Tor.

Case Study: Hornworm Collaboration with FIN8

Hornworm may have established a relationship with the FIN8 cyber-crime gang. In early 2021, FIIN8 was seen deploying the RagnarLocker ransomware onto machines it had compromised in a financial services company in the U.S., the first time Symantec had seen FIN8 installing ransomware on machines it has compromised.

BADHATCH malware, which is known to be used by the FIN8 group, was launched on computers at the organization via PowerShell in January 2021. Multiple PowerShell scripts were downloaded from the abused legitimate sslip[.]io service, which is known to be used by FIN8. PowerShell was also used to download unknown content from a WMI object. FIN8 uses PowerShell to deploy malicious tools onto victim machines.

A keylogger was also deployed and executed. In February 2021, three-and-a-half weeks after suspicious activity was first seen on the network, the open-source tool Rclone was used to exfiltrate data. Just under one month later, in mid-March, the RagnarLocker ransomware was dropped on the network by another tool known as Safebitsloader.

While it is possible that the FIN8 and RagnarLocker activity on this network was carried out separately by two different actors, several things indicate that this wasn't the case. This includes that both BADHATCH and Rclone were downloaded from the same IP address, and both the ransomware and PowerShell scripts were downloaded to the same directory (%WINDIR%\temp) on infected computers.

Leaftier

Aliases: Babuk

Ransomware Families: Babuk

Active since: 2021

First finding public attention in early 2021, Leaftier is notable for its heavy focus on data breach extortion. The group initially operated under an RaaS business model and used double extortion tactics, stealing data from victims as well as encrypting files. However, Leaftier later announced that it was foregoing encryption and focusing only on data theft as a way to extort money from victims.

Babuk was found to have a high degree of similarities with another ransomware threat called Vasa Locker. A Vasa sample analyzed by McAfee shared approximately 86% of the same codebase as Babuk and was compiled one month before the first release of Babuk. It is likely that the actors behind Babuk and Vasa Locker are one and the same, or have strong links to one another.

In late April 2021, Leaftier announced that it was closing its affiliate program and moving to an extortion model that did not rely on encrypting victim computers. The group said it would instead focus on demanding ransoms for information stolen from its victims.

In May 2021, Leaftier announced the development of a platform for “independent leaks” which would be a data leak website for other actors to use. At the same time the group rebranded, changing the name on its new leak website (Payload.bin) from Babuk to Payload Bin.

In early July 2021, it was reported that Leaftier had seemingly returned to using ransomware to target corporate networks. The gang began using a new version of its Babuk ransomware (Babuk v.2.0) and moved to a new data leak website.

Leaffolder

Aliases: Maze, Egregor

Ransomware Families: Maze, Egregor

Active since: 2019

The first evidence of Leaffolder activity dates from May 2019, with the appearance of the Maze ransomware. Leaffolder 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. The tactic was quickly copied by a range of other targeted ransomware groups.

Maze’s main distribution channels were the Fallout and Spelevo exploit kits, with victims being directed to them via 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 in order to move laterally across the network and enumerate machines.

In October 2020, Leaffolder announced that it was shutting down the Maze ransomware operation. The group was subsequently linked to a new ransomware operation known as Egregor, which appeared shortly after Maze was retired. Many former Maze affiliates migrated to using Egregor.

Affiliates of Egregor were subject to a law enforcement operation in February 2021. Egregor is believed to have become inactive since this occurred.

Canthroid

Aliases: UNC2447

Ransomware: Thieflock

Active Since: 2021

Canthroid first appeared in early 2021 when it began performing targeted ransomware attacks using Thieflock. It as operates an RaaS program.

To date, it is known for compromising victims using the exploit of a zero-day vulnerability in Sonicwall VPN (CVE-2021-20016). The vulnerability was patched in February 2021, but Canthroid has continued to attack organizations using unpatched versions of the software. Successful exploit allows the attacker to create their own credentials and join the target's network.

Once inside the network, the group has been observed using SoftPerfect Network Scanner, a publicly available tool used for discovery of hostnames and network services. It is also known to use SombRAT, a custom remote access tool which allows the attackers to download further tools and maintain communications with a C&C server.

Prior to encryption, the group is known to exfiltrate data from the target's network. The attackers are reported to use pCloud, an encrypted cloud storage service.

Tools, Tactics, and Procedures

Most ransomware attacks are a multi-staged process and targeted ransomware attacks in particular usually involve a large number of steps and a significant level of interaction on the part of the attackers. An array of tools, tactics, and procedures (TTPs) are employed to infiltrate the victim's network, steal credentials, elevate privileges, move laterally across the network, and deploy a ransomware payload on multiple computers.

Knowing the TTPs used by ransomware attackers allows network defenders to better understand how their organizations could be compromised and can provide some guidance on prioritization of defensive measures. For example, the Windows tools such as PsExec are frequently abused by attackers and reducing the number of accounts with administrator privileges whilst increasing protection on administrator accounts may mitigate the risk of a successful attack.

Table 1: Most Frequently Seen Ransomware TTPs, April 2021 – June 2021

TTP	Percentage of Ransomware Investigations
Cobalt Strike	41%
PsExec	33%
Netscan	15%
Mimikatz	15%
Adfind	15%
Weirdloop	11%
IcedID	11%
SystemBC	7%
ProcDump	7%
Nsudo	7%
Disable Defender	7%
Delete Shadow Copies	7%
WMI	4%
rclone	4%
Qakbot	4%
BITSAdmin	4%

By examining the results of recent ransomware investigations where precursor tools were found, Symantec was able to obtain a picture of which were the most commonly used TTPs in ransomware attacks. While the most frequently employed tool was the commodity malware Cobalt Strike (seen in 41% of investigations), a large proportion of the list was taken up by freely available, dual-use tools or operating system features, such as PsExec and WMI.

- **Cobalt Strike:** An off-the-shelf tool that can be used to execute commands, inject other processes, elevate current processes, or impersonate other processes, and upload and download files. It ostensibly has legitimate uses as a penetration testing tool but is invariably exploited by malicious actors.
- **PsExec:** Microsoft Sysinternals tool for executing processes on other systems. The tool is primarily used by attackers to move laterally on victim networks.
- **Netscan:** SoftPerfect Network Scanner, a publicly available tool used for discovery of hostnames and network services.
- **Mimikatz:** Freely available tool capable of changing privileges, exporting security certificates, and recovering Windows passwords in plaintext depending on the configuration.
- **Adfind:** A free tool that can be used to query Active Directory.
- **Weirdloop:** Weirdloop, CobaltStrike HTTPS Stager loader used in some attacks involving Ryuk during 2021.
- **IcedID:** Botnet malware that was originally developed as a financial Trojan but is now frequently working in collaboration with ransomware attackers.
- **SystemBC:** Commodity malware which can open a backdoor on the infected computer and use the SOCKS5 proxy protocol to communicate with a C&C server.
- **ProcDump:** Microsoft Sysinternals tool for monitoring an application for CPU spikes and generating crash dumps, but which can also be used as a general process dump utility.
- **Nsudo:** Open-source system management tool that can be abused to elevate privileges.
- **Windows Management Instrumentation (WMI) (wmic.exe):** Microsoft command-line tool that can be used to execute commands on remote computers.
- **Qakbot:** Botnet malware that was originally developed as a financial Trojan.
- **BITSAdmin:** A Microsoft command-line tool that can be used to create download or upload jobs and monitor their progress.

Case Study: Ransomware Supply Chain Attack

While targeted ransomware attacks have proved to be highly lucrative for attackers, it hasn't stopped them from continuously refining tactics. The major innovation of 2020 was the practice of stealing data prior to encrypting computers on the network and then threatening 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.

In July 2021, attackers using the Sodinokibi ransomware experimented with a new tactic: delivering ransomware through a supply chain attack. The attack involved the exploitation of a zero-day vulnerability (CVE-2021-30116) in Kaseya VSA software, which was used to compromise victim organizations via multiple Managed Service Providers (MSPs) who use the software.

The ransomware is believed to have infected at least 1,500 organizations worldwide. Much of the process appeared to be automated and the ransomware was to trigger simultaneously across multiple organizations, presumably to give victims no forewarning of the attack. The attack may have been timed to coincide with the 4th of July holiday weekend in the U.S., where many organizations may be lightly staffed.

The attackers used the exploit to deliver a malicious script and an ASCII PEM named agent.crt to Kaseya VSA clients. The dropper masqueraded inside the ASCII PEM file, which was decoded using Certutil after attempts to disable Microsoft Defender. It dropped two resources, an old, but legitimate copy of Windows Defender (MsMpEng.exe) and a custom malicious loader. The dropper wrote the two files to disk and executed MsMpEng.exe which then side-loaded and executed the custom loader's export (mpsvc.dll).

It remains to be seen whether the attack is the beginning of a new trend. The nature of the attack meant that it may have been somewhat less effective than "traditional" targeted ransomware attacks. The automated nature of the attack meant that the attackers had to forego some of the standard steps taken in such attacks, such as the exfiltration of data and the deletion of backups.

Leafroller, the group behind Sodinokibi, went offline less than two weeks after the attack. The reason for this disappearance remains unclear and it is unknown if it was a coincidence or linked in any way to the Kaseya attack.

Several weeks after the attack Kaseya said that it had acquired a universal decryptor for the ransomware. The company said that it had acquired the decryptor from a «trusted third party» and was now sharing it with affected customers.

Following the attack, the attackers reported demanding $70 million for a universal decryptor, $5 million for a decryptor for each MSP, or $40,000 for each encrypted computer. Kaseya said that it could neither confirm nor deny whether it had paid a ransom to obtain the decryption tool.

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.

Secondary Infections

Over the past twelve months, this has quickly become one of the most prevalent means of access for ransomware groups. Generally speaking, it involves malware that is distributed using mass-mailing botnets, since it provides ransomware groups with a large pool of potential victims. Trojans that were once used for financial fraud, such as Trickbot, have recently been used mainly as distribution channels for other malware, most notably ransomware.

In some cases, ransomware attackers already control the botnets, such as the Miner group, which owns the Trickbot botnet. Trickbot has been seen as a precursor to attacks by Ryuk, which is attributed to Miner. Similarly, Hispid have leveraged their own Dridex botnet, which was originally built to mount financial attacks, to give them a means of delivering the ransomware to organizations.

Other actors have since attempted to replicate this attack pattern, seeking collaborations with established botnet operators. The most notable of these is the use of IcedID by at least one affiliate operator of the Conti ransomware (see Case Study: IcedID and Conti collaboration).

Case Study: IcedID and Conti Collaboration

Several recent investigations by Symantec into attacks involving the Conti ransomware found a consistent attack chain in multiple attacks, suggesting that at least one attacker using Conti had begun to collaborate with the IcedID botnet.

The first evidence of malicious activity in targeted organizations was the presence of IcedID on the target's network. IcedID was then used to deliver malware known as Longlist, which in turn is used to install Cobalt Strike. Other tools used in the attack included the publicly available credential dumping tool LaZagne and Adfind, a free dual-use tool that can be used to query Active Directory.

While IcedID is widely distributed malware, its presence along with these other tools is likely to suggest a ransomware attack in preparation.

Phishing

Phishing is one of the most widely utilized infection vectors, with emails sent to employees disguised as work-related correspondence (invoices, delivery confirmation etc.). 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 was 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 onto 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. More recently, the Canthroid group is known for compromising victims using the exploit of a zero-day vulnerability in Sonicwall VPN (CVE-2021-20016), while the Proxylogon Exchange Server vulnerability was also leveraged by several actors to perform ransomware attacks.

Poorly Secured Services

Another infection vector comes from compromising poorly secured services. Crysis (aka 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.

Protection

How Symantec Solutions Can Help
The Symantec Enterprise Business provides a comprehensive portfolio of security solutions to address today's security challenges and protect data and digital infrastructure from multifaceted threats. These solutions include core capabilities designed to help organizations prevent and detect advanced attacks.

Symantec Endpoint Security Complete
Symantec Endpoint Security Complete (SESC) was specifically created to help protect against advanced attacks. While many vendors offer EDR to help find intrusions, as does Symantec, there are gaps. We call these gaps blind spots and there are technologies in SESC to eliminate them.
LEARN MORE

Privileged Access Management (PAM)
PAM is designed to prevent security breaches by protecting sensitive administrative credentials, controlling privileged user access, proactively enforcing security policies and monitoring and recording privileged user activity.
LEARN MORE

Symantec Web Isolation
Symantec Web Isolation eliminates web threats and solves the challenge of providing access to unknown, uncategorized and potentially risky web sites by creating a remote execution environment between an agency's enterprise systems and content servers on the web.
LEARN MORE

Symantec Secure Web Gateway (SWG)
SWG delivers high-performance on-premises or cloud secure web gateway that organizations can leverage to control or block access to unknown, uncategorized, or high-risk web sites.
LEARN MORE

Symantec Intelligence Services
Symantec Intelligence Services leverages Symantec's Global Intelligence Network to deliver real-time threat intelligence to several Symantec network security solutions including Symantec Secure Web Gateway, Symantec Content Analysis, Symantec Security Analytics, and more.
LEARN MORE

Symantec Content Analysis with Advanced Sandboxing
Within the Symantec Content Analysis platform, zero-day threats are automatically escalated and brokered to Symantec Malware Analysis with dynamic sandboxing for deep inspection and behavioral analysis of potential APT files and toolkits.
LEARN MORE

Symantec Security Analytics
Symantec Security Analytics delivers enriched, full-packet capture for full network traffic analysis, advanced network forensics, anomaly detection, and real-time content inspection for all network traffic to arm incident responders for quick resolution.
LEARN MORE

Mitigation

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

Local Environment:

- Monitor the use of dual-use tools inside your network.
- 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 (MFA).
- Implement proper audit and control of administrative account usage. You could also implement one-time credentials for administrative work to help prevent theft and misuse 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.
- Use application whitelisting where applicable.
- Locking down PowerShell can increase security, for example with the constrained language mode.
- Make credential dumping more difficult, for example by enabling credential guard in Windows 10 or disabling SeDebugPrivilege.
- MFA can help limit the usefulness of compromised credentials.
- **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.

Email:

- Enable MFA to prevent the 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.

Symantec™
A Division of Broadcom

For product information and a complete list of distributors, visit our website at: broadcom.com