White Paper

The Ransomware Threat Landscape: What to Expect in 2022

Threat Hunter Team

Table of Contents

Introduction

Ransomware was the dominant cyber-crime trend of 2021, with no signs of that changing in 2022. The big names on the ransomware landscape may change, as takedowns, improved security, and new arrivals force existing families to adapt, but activity remains at a high level. Big names like Ryuk, REvil/Sodinokibi, and Darkside have declined or disappeared over the last while, but newer names like Hive and AvosLocker have come to the fore instead.

While the most active names, and the tactics, tools, and procedures (TTPs) used by ransomware developers and their affiliates may alter, ransomware is unlikely to disappear or decline dramatically due to its sheer profitability. Ransomware is only likely to disappear if something more profitable and easier to execute for cyber criminals comes along, which doesn't seem likely at the moment.

Changes in the area of cyber insurance - such as insurance firms refusing to cover ransomware attacks - or increased regulation of cryptocurrencies are two external factors that could impact the profits ransomware actors can make. Any change in the world of cryptocurrency that may impact ransomware authors seems unlikely, but we have seen some cyber insurance companies become stricter about ransomware pay-outs, which makes that an area to watch. Many companies rely on insurance pay-outs to pay ransoms and recover from ransomware attacks.

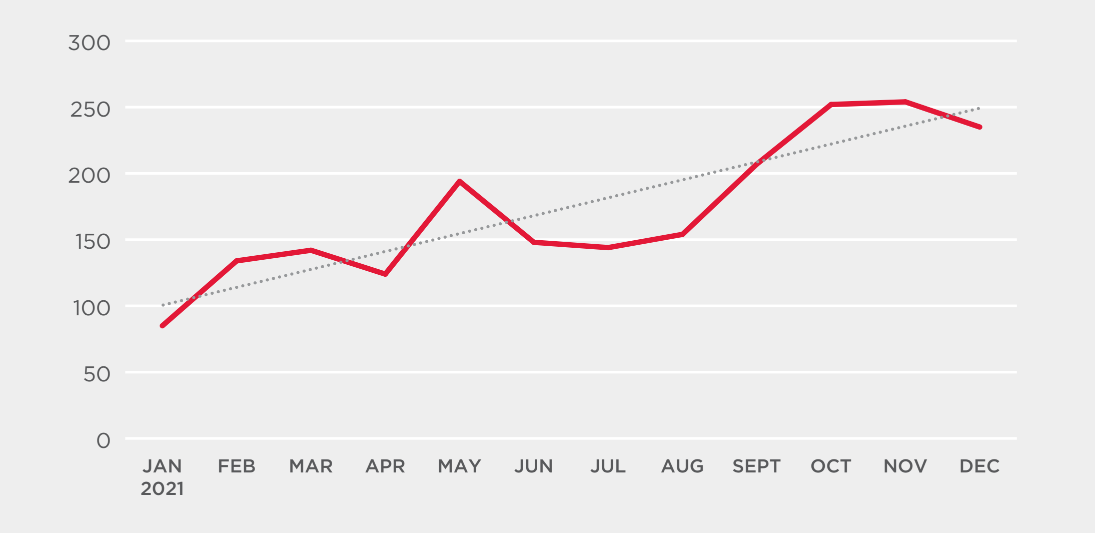
Some of the main findings in this paper include:

- Targeted ransomware attacks trended upwards in 2021, almost trebling between the first and final quarter of 2021.
- The list of TTPs used by ransomware actors continues to evolve. While hacktools and commodity malware are frequently leveraged by ransomware actors, dual-use tools and living-off-the-land tactics also continue to remain popular as ransomware actors endeavor to keep their activity undetected until they can deploy their ransomware payload.
- The main ransomware families on the scene constantly change, often due to the impact of takedowns, sanctions, or increased scrutiny from law enforcement. New actors like Pinion (Hive) and Sirex (AvosLocker) are now very active, while Miner (Conti) also remains a strong presence on the ransomware scene.
- The return of the Emotet botnet in late 2021 has the potential to have a major impact on the ransomware landscape in 2022.

Ransomware Trends

The number of organizations being bit by targeted ransomware trended upwards in 2021, as can be seen in *Figure 1*.

Figure 1: Number of Targeted Ransomware Attacks, Jan to Dec 2021

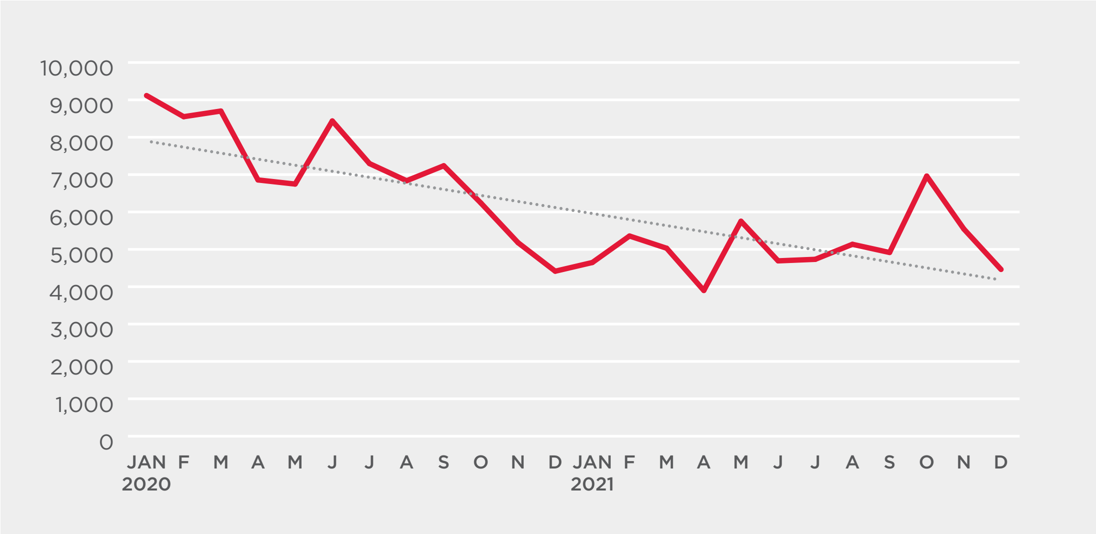


We noted in last year's Ransomware Threat Landscape whitepaper that the number of targeted ransomware attacks jumped by 83% between January 2020 and June 2021. We can see that this growth continued in the second half of 2021, with more than 250 targeted ransomware attacks recorded in both October and November 2021. Between January 2021 and November 2021, the number of targeted ransomware attacks almost trebled from 85 to 254, increasing by just under 200%.

It is important to note too when looking at the figures around targeted ransomware, which can seem small, that 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 blocked before the payload is deployed, meaning they may not be identified as ransomware. Also, 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.

While the number of targeted ransomware attacks has trended upwards over the last couple of years, the total number of ransomware attacks detected by Symantec, a division of Broadcom, has been in decline, as can be seen in *Figure 2*. This is likely a reflection of the decline in the popularity of mass-mailing spam ransomware campaigns, with the focus of most cyber criminals in this space now on targeted ransomware. It is by no means an indication that the danger posed by ransomware is declining in any way. With attackers increasingly focusing on targeted ransomware, the danger for large organizations has likely only increased.

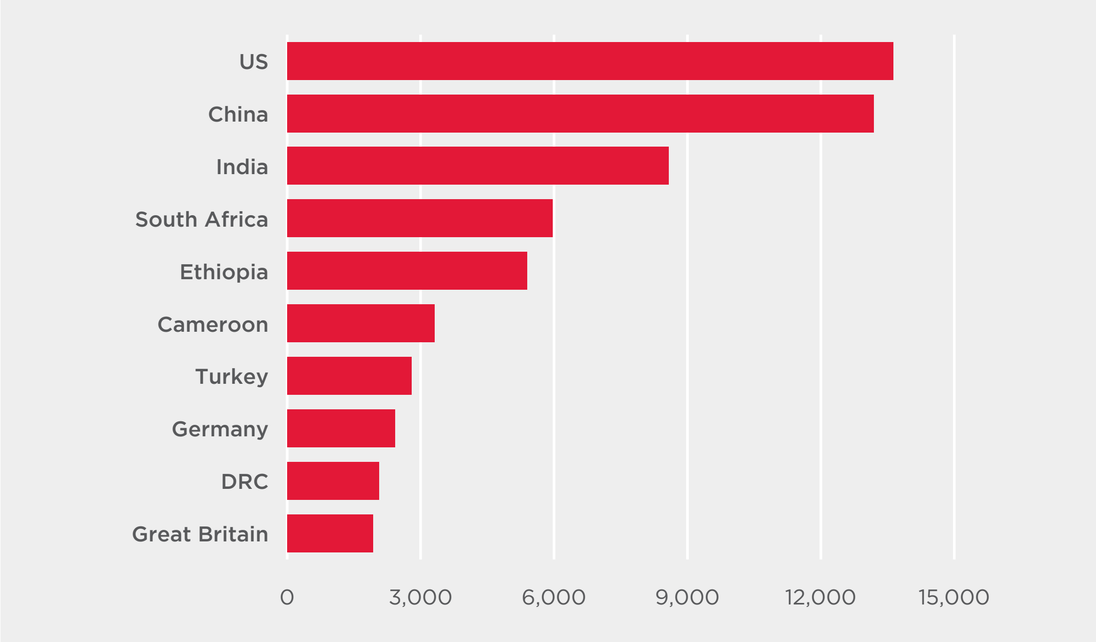
Figure 2: All Ransomware Detections, Jan 2020 to Dec 2021



The difference between indiscriminate ransomware attacks and targeted ransomware attacks can be seen when we look at the overall number of ransomware detections by country (*Figure 3*), compared to the number of targeted ransomware detections by country (*Figure 4*).

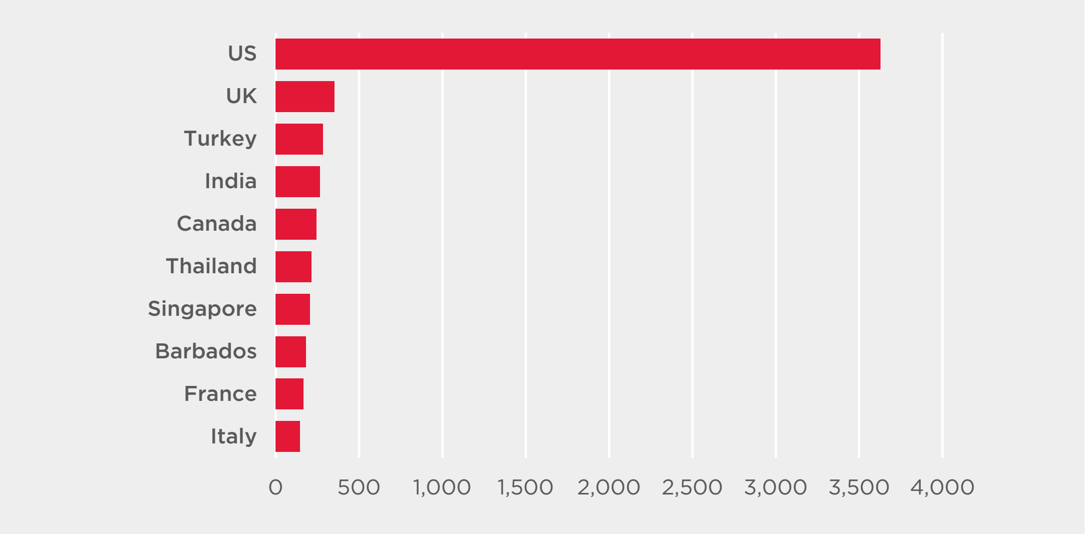
While the U.S. is the most targeted country in both cases, the overall number, which tends to be dominated by indiscriminate, mass-spamming ransomware attacks, lists countries such as the Democratic Republic of Congo (DRC), Ethiopia, and other countries that do not appear in the targeted ransomware list.

Figure 3: Overall Number of Ransomware Detections by Country, Jan to Dec 2021



The targeted ransomware list is more dominated by richer countries, including the UK, France, and Italy. Once again, the U.S. is at the top of the list, with it seeing more than 10 times as many targeted ransomware attacks as the next nation on the list (the UK). This is unsurprising considering the U.S. is a rich nation with a large business sector, and many targeted ransomware gangs have claimed to exclusively target U.S.-based companies.

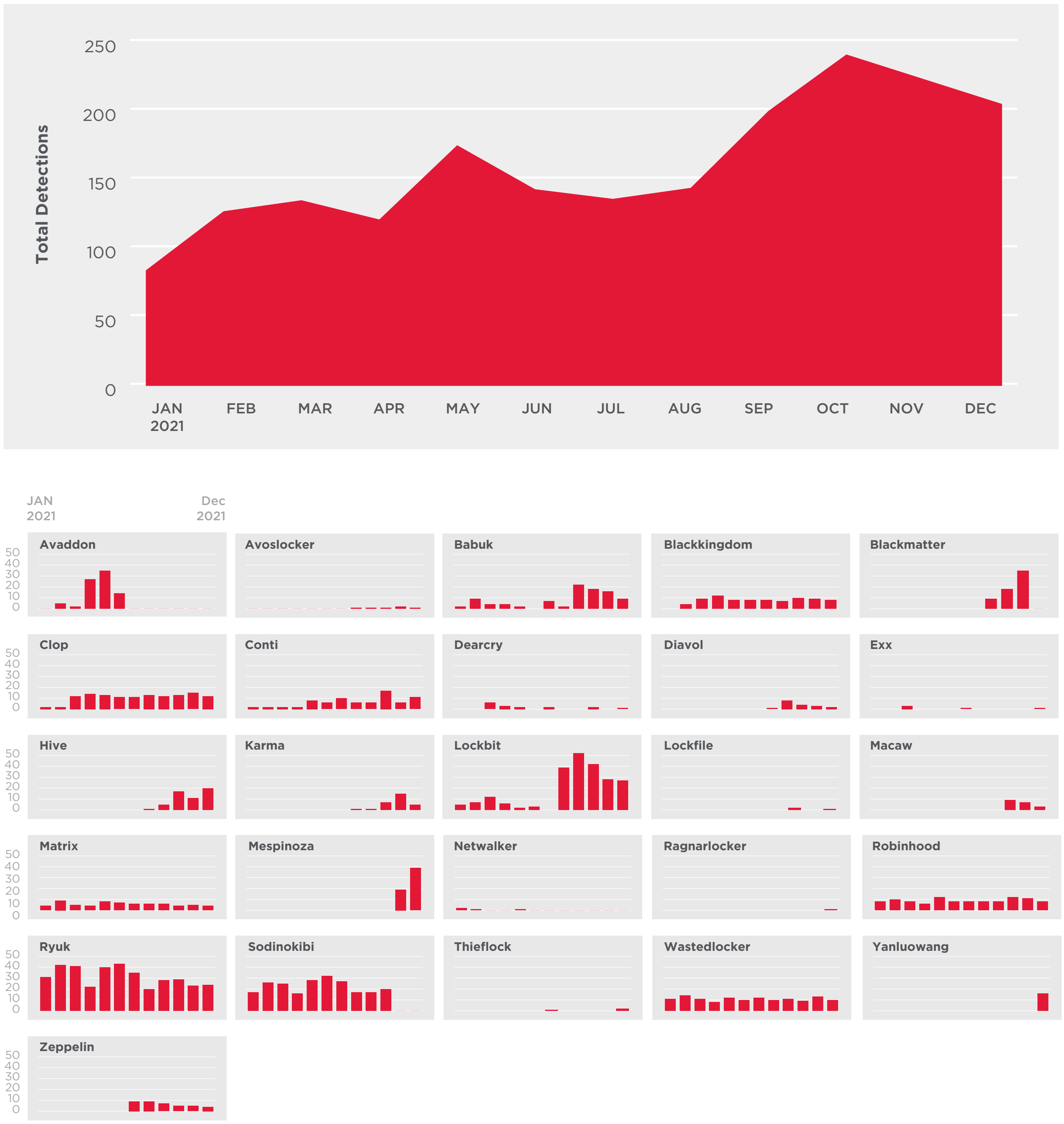
Figure 4: Targeted Ransomware Detections by Country, Jan to Dec 2021



The presence of a small country like Barbados in the top 10 in *Figure 4* might raise eyebrows, but this is a count of computers on which a targeted ransomware family was detected, rather than a count of organizations. Many victims of targeted ransomware have operations in more than one country.

While overall activity and impacted countries are valuable information, what many people want to know is the most active ransomware families they need to be aware of now. The ransomware landscape is ever evolving, and ransomware families that were once dominant have become inactive – sometimes due to takedowns and at other times because operators have decided to “retire” a particular family – while new ransomware families have come to prominence.

Figure 5: Targeted Ransomware Attacks by Family, Jan to Dec 2021



While some families, such as Conti and LockBit, were active for much of 2021, many of the now-most-dominant ransomware families only appeared in the final half or even the final quarter of 2021. Mespinoza, AvosLocker, Hive, and Zeppelin are all ransomware families that are very active and highly dangerous at the moment, with all of these families seeing an uptick in activity in the second half of 2021, underlining the fast-changing nature of the ransomware landscape.

More information about these active threats can be found in the Ransomware Threat Actors section of this whitepaper.

Again, it should be stressed that these statistics should be treated as a representative sample of attacks blocked by Symantec products. 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.

Case Study

REvil Takedown a Sign of Things to Come?

Infamous ransomware gang REvil/Sodinokibi (aka Leafroller) was forced offline in October 2021 when control of its infrastructure was seized in a multi-country operation. REvil had initially gone offline in July 2021, when its main spokesperson "Unknown" also appeared to disappear from the internet, but the ransomware came back online in September.

The July shutdown of REvil occurred shortly after the high-profile REvil ransomware attack that hit IT management software company Kaseya. However, while that disappearance was temporary, signs are that this October takedown may have a more lasting impact. Media reports said that the U.S. Federal Bureau of Investigation (FBI), U.S. Cyber Command, the Secret Service, and a number of international governments were responsible for the coordinated action against REvil in October.

This action was followed in January 2022 by announcements from Russia that 14 alleged members of the REvil ransomware gang had been arrested by authorities in that country, in what was a highly unusual move by Russian law enforcement. Russian law enforcement said they made the arrests after they received information about the ransomware gang from authorities in the U.S. The White House said that among those arrested in those raids was the person responsible for the Colonial Pipeline ransomware attack that occurred in May 2021. While that attack was linked to the Darkside ransomware, the developers of Darkside – Coreid – are believed to have been associates of the REvil gang.

High-profile ransomware attacks in 2021, such as those targeted at Colonial Pipeline, Kaseya, and also U.S. food production giant JBS Foods, appear to have made governments much more willing to take a strong stance against the cyber-criminal gangs that are involved in ransomware attacks.

Also in 2021, we saw the takedown of the Emotet botnet in January, though it may now have returned, and the Netwalker ransomware infrastructure was also seized and arrests made in that same month.

Tactics, Tools and Procedures

Most targeted ransomware attacks are a multi-stage process that see the attackers take many steps and deploy an array of TTPs before deploying the ransomware payload. An awareness of the TTPs commonly employed by ransomware attackers is key for organizations seeking to defend their networks from being infiltrated by ransomware attackers, as spotting this pre-ransomware activity can allow defenders to stop an attack before it detonates.

Attackers employ these TTPs for a variety of actions, including to infiltrate the victim's network, steal credentials, elevate privileges, move laterally across the network, and deploy their ransomware payloads.

The pre-ransomware tools we saw used most often in attacks during 2021 can be seen in *Table 1*. It is notable that a Windows operating system tool like PsExec was the tool seen in the most investigations (34%) between April and December 2021. While commodity malware like Cobalt Strike also features strongly in the list of tools used by ransomware attackers, the large number of living-off-the-land and dual-use tools leveraged points to the continuing popularity of living-off-the-land tactics among ransomware attackers as they endeavor to keep their activity on victim networks hidden until the ransomware payload is deployed. They do this by leveraging legitimate processes and tools that are less likely to trigger security software or look suspicious to users on the network.

Table 1: Most Frequently Seen Pre-ransomware Tools, April – December 2021

Tool	Percentage of Investigations
PsExec	34%
Cobalt Strike	18%
Mimikatz	11%
VssAdmin	10%
NetScan	7%
Bitsadmin	4%
AdFind	5%
Nsudo	5%
PowerShell	5%
MSIExec	4%
WEIRDLOOP	3%
IcedID	3%
Disable Defender	3%
WMI	4%
rclone	3%
NetworkShare	2%
PAExec	2%
RaccoonStealer	2%
PasswordRevealer	2%
Netsh	2%
ProcDump	2%
ScreenConnectInstaller	2%
SystemBC	2%
Delete Shadow Copies	1%
Qakbot	1%

In the ransomware whitepaper we shared with customers in September 2021, we listed a number of the tools we saw leveraged in ransomware attacks. Almost all of those tools are still relevant now, but we have also seen some additional tools leveraged in more recent attacks. These include:

- **VssAdmin**: Legitimate Windows process that can be used to manage - or delete - shadow copies on Windows machines.
- **MSIExec**: Legitimate Windows installer that can be abused by attackers to load malicious payloads onto victim machines.

- **NetworkShare**: Command attackers can issue in order to spread their malicious payload to other machines on the same network.
- **PAExec**: Allows users to launch Windows programs on remote Windows computers without needing to install software on the remote computer first. Like PsExec, it is primarily used by attackers to move laterally on victim networks.
- **RaccoonStealer**: An information-stealer-for-hire that its operators rent to other cyber criminals for a fee. It can be used to steal a variety of information from infected machines, but is most likely used by ransomware attackers to steal credentials to allow for privilege escalation and lateral movement.
- **PasswordRevealer**: Hacktool that shows the passwords hidden behind asterisks on machines it is installed on.
- **Netsh**: Windows command-line utility that allows a user to configure and display the status of various network communications server roles and components. Has been used in LockBit and Mespinoza/Pysa attacks.
- **ScreenConnectInstaller**: An installer for ScreenConnect (now known as ConnectWise), a legitimate remote access tool that has been frequently exploited by malicious actors to provide access to victim machines. Has recently been used in attacks leveraging the Yanluowang and Noberus (ALPHV/BlackCat) ransomware.

The tools which feature in our statistics and which also appeared in our September ransomware whitepaper are listed below.

- **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.
- **PowerShell**: Legitimate tool that can be used for a variety of malicious purposes, including executing commands directly from memory, and injecting malware into other legitimate processes. Because PowerShell has many legitimate uses it provides an ideal way for attackers to hide their malicious activity.
- **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**: Cobalt Strike 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 used in collaboration with ransomware attackers.
- **SystemBC**: Commodity malware that can open a backdoor on the infected computer and use the SOCKS5 proxy protocol to communicate with a command-and-control (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.
- **Rclone**: An open-source command-line utility that can legitimately be used to manage content in the cloud, but has been seen being abused by ransomware actors to exfiltrate data from victim machines.
- **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.

Knowing the TTPs used by ransomware attackers allows defenders to better understand how their organizations could be compromised and can provide some guidance on prioritization of defensive measures.

New and Updated Ransomware Threat Actors

Many of the main ransomware threat families were detailed in our September 2021 ransomware whitepaper. However, the nature of the ever-changing cyber-crime landscape, and in particular the ransomware landscape, means that several new ransomware families have become prominent since then. Some of the currently most active ransomware families are detailed in this section.

New Actor Profiles:

Birdwing

Aliases: Pysa, Mespinoza

Ransomware families: Pysa

Active since: 2018

Birdwing develops the Mespinoza/Pysa ransomware, which has been used in attacks on victims in a large number of sectors and countries, though most of its victims have been in the U.S. It is not entirely clear if Birdwing deploys the ransomware itself, or if it operates a ransomware-as-a-service (RaaS) model, where affiliates deploy the ransomware on its behalf for a cut of the profits.

Active since at least October 2018, Birdwing's activity has ramped up in recent times, with the FBI issuing an alert about the group in March 2021. Birdwing ransom notes contain the phrase "Protect Your System Amigo", which may be what Pysa stands for.

Birdwing typically gains unauthorized access to victim networks by compromising Remote Desktop Protocol (RDP) credentials and/or through phishing emails. The group carries out reconnaissance on compromised systems, likely to determine whether there is enough valuable data to justify launching a full-scale attack, and it searches for keywords such as "clandestine", "fraud", "ssn", and more, likely to find sensitive files that would have an impact if leaked. The cyber actors use Advanced Port Scanner and Advanced IP Scanner to conduct network reconnaissance, and proceed to install open-source tools, such as PowerShell Empire, Koadic, and Mimikatz. Other open-source tools like PsExec, PowerShell, and netsh have been seen being deployed in Birdwing attacks as well. Security products, including Windows Defender, are also generally deactivated before the ransomware is deployed, and shadow copies are deleted from victim systems so that data cannot be restored from them.

Palo Alto said that in a Birdwing attack it observed a new backdoor it dubbed Gasket being downloaded to maintain access to the network. Gasket also referenced a capability called "MagicSocks" that uses the open-source Chisel project to create tunnels for continued remote access to a network. The attackers created a standalone version of the MagicSocks tool that they used in addition to Gasket to tunnel traffic. Symantec researchers also observed a malicious script named p.ps1 being deployed by attackers via PsExec approximately 24-hours before ransomware was deployed on victim machines during a Birdwing attack. Birdwing uses various methods to exfiltrate files from victim networks. The FBI reported it had been seen using the free open-source tool WinSCP, while both Symantec and Palo Alto researchers observed Birdwing attackers use IP-based URLs containing the same URI pattern to exfiltrate victim data, e.g. URIs /upload-wekkmferokmsdderiuheoirhuiewiwnijnfrer?token=<base64 token value>&id=<unique number for organization>&fullPath=<path on disk of file exfiltrated>. In some Birdwing attacks, stolen data has been uploaded to the Mega.nz file-sharing site.

Once the data is exfiltrated, the data on infected networks is encrypted by the ransomware. In several instances Birdwing has downloaded its payload with the file name svchost.exe, most likely in an effort to disguise the ransomware as the generic Windows host process by giving it the same name. When the ransomware is executed, a detailed ransom message is generated and displayed on the victim's login or lock screen.

Symantec researchers observed a Pysa ransomware attack in late October 2021 when the attackers spent just three or four days on the network before deploying the ransomware payload, which is a relatively short dwell time for ransomware attackers.

Sirex

Aliases: AvosLocker

Ransomware families: AvosLocker

Active since: 2021

Sirex first appeared in June 2021. It is a ransomware operator that uses affiliates to carry out attacks using its AvosLocker ransomware for a cut of the profits. It offers not only the malware, but also help in managing the communication with the victim, and hosting of the data stolen during the operation.

AvosLocker is generally spread via spam email campaigns or malvertising, however, as Sirex operates as an RaaS and the ransomware is distributed by affiliates, the TTPs used to carry out AvosLocker ransomware attacks may vary. Attackers using AvosLocker have also been seen exploiting known vulnerabilities in Microsoft Exchange Server to gain initial access to victim networks. Once the ransomware executes, the ransom note GET_YOUR_FILES_BACK.txt is created. The ransomware then encrypts the user's files and appends the .avos extension to them. The link given in the ransom note guides victims to a Tor website that requests the ID that was also in the note. If not paid, the ransom increases after a certain time, and the group also threatens to reveal publicly that the victim organization has been hacked.

If a file is currently being accessed by another process when the payload detonates, the ransomware ends the process and proceeds with the content encryption. The ransomware reads the file's content, encrypts it, and writes the content in the encrypted file with a unique signature. This signature is used to identify whether the file is encrypted or not. It also encrypts the network share drive.

Analysis by Malwarebytes concluded that AvosLocker was an unremarkable family of ransomware, which did "not distinguish itself much from other ransomware (apart from being unusually noisy)." However, there are no weaknesses in its encryption, so it is impossible to recover encrypted data without the decryption key.

In September 2021, Sirex updated its website to create a system to allow it to auction off the data of hacked companies that refuse to pay ransom demands, rather than just dumping it online for free.

Pinion

Aliases: Hive

Ransomware families: Hive

Active since: 2021

Pinion is notable for not seeming to exclude any sectors from its attacks, as many ransomware operators often claim to do, with it known to have attacked multiple victims in the healthcare sector, for example. These attacks do not seem to be mistakes because the ransomware is human-operated and designed to take input from the command-line, indicating the attackers are both aware of the environment they are in and tailoring their attacks for maximum impact.

In an attack on non-profit U.S. healthcare provider Memorial Health Systems (MHS) in August 2021, attackers using the Hive ransomware claimed to have stolen data belonging to as many as 200,000 patients. The attack also led to the cancellation of surgeries and the curtailment of healthcare operations. Unlike in similar ransomware attacks where the ransomware actors have provided a decryption key free of charge after hitting a healthcare provider, Pinion didn't do this, with MHS reportedly paying a ransom of close to $2 million.

Pinion operates as an RaaS, with affiliates carrying out attacks using the Hive ransomware for a cut of the profits. Hive is used in double-extortion ransomware attacks, where victim information is stolen as well as their files being encrypted.

Pinion and the affiliates leveraging its ransomware use multiple mechanisms to compromise business networks, including phishing emails with malicious attachments to gain access and RDP to move laterally once on the network. Attackers using Hive have also been seen leveraging Cobalt Strike and the legitimate ConnectWise tool for persistence on infected networks.

The ransomware seeks processes related to backups, anti-virus/anti-spyware, and file copying, and terminates them to facilitate file encryption. It adds the .hive extension to encrypted files and then drops a hive.bat script into the directory, which enforces an execution timeout delay of one second in order to perform a clean-up after the encryption is finished by deleting the Hive executable and the hive.bat script. A second file, shadow.bat, is dropped into the directory to delete shadow copies, including disc backup copies or snapshots, and then delete the shadow.bat file. During the encryption process, encrypted files are renamed with the double final extension of *.key.hive or *.key.*. The ransom note, HOW_TO_DECRYPT.txt, is dropped into each affected directory and states that if the *key.* file is modified, renamed, or deleted, the encrypted files will no longer be able to be recovered.

The ransom note contains a "sales department" link, accessible through a Tor browser, that allows victims to contact the actors through a live chat. Some victims also reported receiving phone calls from Hive actors requesting payment for their files, according to the FBI. The note also informs victims that their data will be published on a data leaks website if they do not pay the ransom.

There are also Hive variants capable of encrypting Linux and FreeBSD systems.

Dryxiphia

Aliases: Yanluowang

Ransomware families: Yanluowang

Active since: 2021

Dryxiphia, which was discovered by Symantec researchers, was first observed attempting to carry out a ransomware attack using the Yanluowang ransomware in September 2021. The attack targeted a large enterprise organization and was spotted after researchers noted suspicious use of AdFind, a legitimate command-line Active Directory query tool that is regularly abused by ransomware attackers. Days after the suspicious AdFind use was seen on victim machines the attackers attempted to deploy the Yanluowang ransomware.

Following our initial discovery of Yanluowang, Symantec researchers then found evidence that it had also been used by a threat actor mounting targeted attacks against U.S. corporations since at least August 2021. The attacker used a number of TTPs that were previously linked to Canthroid (Thieflock) ransomware attacks, suggesting that they may have been a Thieflock affiliate who shifted allegiances to the new Yanluowang ransomware family.

Yanluowang appears to be quite a newly developed ransomware, and it is unclear at the moment whether it is being rented out for use by affiliates as part of an RaaS operation or if Dryxiphia is carrying out most attacks directly. The ransomware has primarily been deployed against organizations in the financial sector.

Also notable is that, in its ransomware note, Dryxiphia warns victims not to contact law enforcement or ransomware negotiation firms. If the attackers' rules are broken the ransomware operators say they will conduct distributed denial of service (DDoS) attacks against the victim, as well as make "calls to employees and business partners." The criminals also threaten to repeat the attack "in a few weeks" and delete the victim's data. This follows a recent trend we have seen of ransomware attackers making further threats if victims attempt to involve any third parties in ransomware negotiations.

Batfly

Aliases: Nemty, Karma

Ransomware families: Karma, Nemty, JSWorm, Nefilim, Fusion, Milihpen, Gangbang

Active since: 2019

Batfly is responsible for the well-known Nemty and Karma ransomware strains, as well as being involved in the development of various other ransomware variants, including Nefilim, Gangbang, and Milihpen, since 2019. Batfly's first publicly observed activity was under the moniker JSWorm in April 2019. Nemty was first spotted in August 2019, and it went through numerous different versions. Both Nemty and Karma are named as those are the extensions they add to encrypted files.

When Nemty first appeared it was available for purchase on cyber-crime forums and the ransoms demanded were modest by current standards, equating to approximately $1,000. In the early days of Nemty's operations Batfly was very active about releasing new versions of it to fix bugs and make improvements. Some of these were necessitated due to the work done by security researchers and companies, while some were spurred on by critiques from the users of the underground cyber-crime forums where Batfly was initially selling access to Nemty.

Batfly was also one of the earlier ransomware developers to carry out double-extortion attacks, where the attackers steal data for extortion purposes as well as encrypting it, operating a data leaks website since August 2019. Nemty was distributed through email spam campaigns, exploit kits, and by brute-forcing RDP endpoints, as well as at one point being distributed via the Trik botnet.

In March/April 2020, Batfly rebranded its ransomware to Nefilim and announced it would be "going private". This meant it was no longer freely available to purchase on ransomware forums and that its developers would only work with trusted affiliates, which is typically how RaaS offerings operate now.

The Milihpen variant appeared in January 2021. Written in C++ it retained the main functionality, execution flow, crypto scheme and data leak site addresses of earlier variants, while Gangbang, which appeared in February 2021, was identical to Milihpen. Karma appeared in May 2021 and researchers concluded it was most likely from the same developers as Nemty due to code similarities between Karma, Gangbang, and Milihpen. The similarities included the exclusion of folders, file types, and the debug messages used. However, several changes had also been made, including Karma using Salsa20 encryption, while it also creates a new thread for the enumeration and the encryption, possibly to achieve a more reliable outcome. The size of the ransoms demanded by Karma is not known, but the ransomware seems to be primarily deployed against large organizations with revenues of more than $1 billion.

Batfly's older 'Corporate Leaks' data leaks website went dormant around the same time that Karma and its data leaks website appeared, indicating that, for now anyway, Karma appears to be the main focus for Batfly.

Pollen

Aliases: Zeppelin, VegaLocker

Ransomware families: Zeppelin, Buran, VegaLocker

Active since: 2019

Active since 2019, Pollen initially used the VegaLocker ransomware, which targeted Russian speakers and was spread via malvertising on an online Russian advertising network. At the time it was indiscriminate in its targeting, and over the course of 2019 multiple new versions of VegaLocker appeared - Jamper, Storm, Buran - with some offered for sale on underground forums.

However, a change in Pollen's approach occurred when it launched the Zeppelin ransomware in November 2019, with the ransomware being used to target carefully chosen organizations in the technology and healthcare sectors in the U.S. and Europe. Another feature of Zeppelin that marks it out from earlier versions of Pollen's ransomware is that it is designed to quit if it is running on machines in Russia or other Commonwealth of Independent States (CIS) countries.

Pollen sells Zeppelin on underground forums, allowing buyers of the malware to decide how they wish to use it rather than distributing it through the more typical, controlled RaaS programs we generally see ransomware developers operating now. Pollen is also notable for not operating a data leaks website, unlike most ransomware actors these days. Zeppelin is also notable for long periods of inactivity, with many believing it had been retired at the end of 2020 before Pollen returned to offer a new version of the ransomware for sale in mid-2021.

Cyber criminals using Zeppelin generally use common initial attack vectors like RDP, VPN vulnerabilities, and phishing, while it has also been seen being distributed via compromised websites or temporary C&C infrastructures that are active only during distribution. More recent Zeppelin variants also include a sleep function that lasts for 26 seconds in an attempt to bypass dynamic analysis engines and sandboxes.

Symantec researchers observed a Zeppelin ransomware attack in November 2021 that abused a local network share as a staging server for the ransomware payload and a malicious PowerShell script named w.ps1. Prior to the ransomware being deployed, a number of behaviors were observed, including:

- Credential dumping using comsvcs
- Disabling security services
- Deletion of volume shadow copies
- Inhibiting system recovery using BCDEdit
- Remote compiling and execution using CVTRES

PsExec was used to execute w.ps1 and copy the ransomware payload to all computers on the network. In this attack, encrypted files were given the file extension .v-society.9BF-C5F-9E3 and the ransom note stated that "VICE SOCIETY" was responsible.

Because Zeppelin can be relatively easily bought on underground forums it is likely to be distributed by a larger than normal number of cyber-crime actors, making it more challenging to develop a picture of a typical Zeppelin attack as the TTPs used are likely to vary greatly.

Case Study

Noberus: Rust-coded Ransomware Wants to Keep Negotiations Private

Noberus (aka ALPHV/BlackCat) was first seen on a victim organization on November 18, 2021, with three variants of Noberus deployed over the course of the one attack. Noberus is interesting because it is coded in Rust, and this is the first time we have seen a professional ransomware strain that has been used in real-world attacks coded in this programming language.

Noberus carries out the now-typical double-extortion ransomware attacks we are accustomed to seeing, and deploys commonly seen ransomware tools like PsExec and PowerShell in its attacks. It also appears to leverage the legitimate ConnectWise tool to deploy its payload. It also carries out various other commonly seen pre-ransomware actions, such as disabling Window Defender and deleting shadow copies.

One interesting thing that Noberus does is run commands to collect system information via WMIC, in order to collect Universally Unique Identifiers (UUIDs) from each machine. These are then used to generate the 'access token' that makes up part of the unique Tor address victims are instructed to visit. Victims need to have this unique address in order to enter into negotiations with the attackers. It is likely the attackers did this in order to stop their negotiations being infiltrated by others, such as security researchers or journalists.

Leaked negotiation transcripts largely arise from the fact that the preferred means of ransom negotiation is a chat site with a unique URL for each victim. While it makes it easy for victims to contact the attackers, it does mean that anyone with the URL can view the conversation and even post themselves. Ransom negotiation URLs are often contained within the ransomware payload and can be found if a sample is uploaded to services such as VirusTotal, which means that even if the victim doesn't want to publicize the negotiation, it may be accessible to third parties. The creation of these unique access keys during the attacks prevents this from happening.

Negotiations being leaked or infiltrated is something that appears to have aggravated ransomware attackers recently, with more than one ransomware group having threatened to halt negotiations if victims bring in a professional negotiator or if information about the attack is leaked to the media.

Conti (aka Miner) said that it would immediately leak victim data if transcripts or screenshots of ransom negotiations were publicly shared. Meanwhile, the Grief ransomware said it would delete decryption keys if victims hired a professional negotiator, while RagnarLocker said it would leak victim data if law enforcement was contacted.

Miner

No sign of activity abating

Aliases: Wizard Spider

Ransomware families: Diavol, Conti, Ryuk, GoGaLocker (inactive), MegaCortex (inactive)

Active since: 2014

One of the most active ransomware developers of recent years, Miner showed no signs of intending to slow down its activity as 2021 came to a close. Conti remains one of the most active targeted ransomware families, with the Australian Cyber Security Center (ACSC) as recently as December 2021 issuing a warning about attacks using this ransomware. The ACSC said there were "multiple instances" of Australian organizations being impacted by Conti ransomware in November and December 2021.

Elsewhere, it has been reported that attackers associated with Conti were involved in the return of the Emotet botnet in the last quarter of 2021 (*See Case Study*). However, it is not clear if this was Miner, or an affiliate user of Conti.

Meanwhile, in more recent months, Miner has been associated with a new ransomware called Diavol, which appears to be becoming increasingly active. Fortinet researchers linked it to Miner in July, when it said the ransomware was used in an attack during which Conti was also deployed on the same network. There are also some similarities between the two pieces of malware, as well as between the TTPs used. Diavol uses "nearly identical" command-line parameters to those of Conti and they are used for the same functionality, namely to log files, encrypt local drives or network shares, and scan specific hosts for network shares. Both Diavol and Conti also feature asynchronous I/O operations when queuing the file paths for encryption.

Miner has remained consistently active during a time of great disruption on the ransomware landscape. If the group now also has the Emotet botnet in its arsenal it is likely that attacks using ransomware developed by this group will continue to increase in 2022.

Coreid

Link to notorious FIN7 cyber-crime group

Aliases: Darkside

Ransomware families: Darkside, BlackMatter

Active since: 2020

Coreid is most famously associated with the Darkside ransomware, which was used to carry out the May 2021 attack on Colonial Pipeline. Intense attention from both media and law enforcement following this attack led to Coreid retiring Darkside, with the group claiming it had lost access to its servers and cryptocurrency wallets following law enforcement action.

However, in July 2021, the BlackMatter ransomware, which is widely believed by experts to be associated with Coreid, appeared. BlackMatter used the same encryption routines as Darkside, while blockchain analysis firm Chainalysis also found financial links between the two ransomware families. The U.S. government issued a warning about BlackMatter in October 2021, saying it had been used in multiple targeted attacks aimed at critical infrastructure organizations in the country. However, at the start of November, BlackMatter posted a message saying it would be ceasing operations due to "certain unsolvable circumstance associated with pressure from the authorities." This likely means that arrests had made continuing to run the ransomware difficult. Its disappearance just over four months after it became active underlines the volatile nature of the ransomware landscape.

While initially tracked by Symantec researchers as a standalone group, in the second half of 2021, research by CrowdStrike linked Coreid to the infamous FIN7 (aka Carbon Spider) cyber-crime group, stating that they were one and the same and that FIN7 was behind both the Darkside and BlackMatter ransomware strains. FIN7 is a prolific cyber-crime group that has been active since at least 2016. Initially known for installing malware on point-of-sale systems in the retail and hospitality industries, according to CrowdStrike the group shifted its focus in 2020 and started carrying out some ransomware attacks using the REvil ransomware. CrowdStrike says that FIN7 was responsible for developing both the Darkside and BlackMatter ransomware strains, and for running the affiliate programs for both ransomware.

The fact that a well-known and prolific cyber-crime gang like FIN7 made the decision to focus its attention on ransomware shows the influence of ransomware on the cyber-crime landscape at the moment – it is the primary vehicle which sophisticated cyber criminals are using to make money. Now that the group has been forced to retire both Darkside and BlackMatter it will be interesting to see if they appear with a new ransomware strain, or if law enforcement pressure has had an irreversible effect on the group's activity.

Hispid

Group debuts two new ransomware strains

Aliases: EvilCorp, Indrik Spider, TA505

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

Active since: 2011

Hispid is a well-established cyber-crime group that has been active for around 10 years. The group was initially associated with financial fraud, being responsible for the Dridex banking Trojan, before it turned its attention to ransomware in 2017. Sanctions were imposed on Hispid 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. The group is known to frequently rebrand its ransomware, likely in an effort to circumvent these sanctions and receive payment from U.S.-based companies.

In the second half of 2021, Hispid was seen operating two new ransomware strains. The Grief ransomware appeared in June, and in October it claimed responsibility for a ransomware attack that hit the U.S. National Rifle Association (NRA). Also, in September 2021, Grief posted a statement on its data leaks website threatening to delete its victim's decryption keys if victims hired a negotiation firm.

Meanwhile, in October 2021, another new ransomware, Macaw, was launched by Hispid. An attack using Macaw led to significant disruption at U.S. broadcasters Olympus and Sinclair Broadcast Group, leading to TV broadcasts being cancelled and newscasters reporting stories using paper and whiteboards. The attackers reportedly demanded ransoms of $28 million and $40 million off the victims.

It is likely we will see further new Hispid rebrands in 2022, as the group continues to try and evade the sanctions against it.

Case Study

Exmatter: Data Exfiltration Tool Used in BlackMatter, Conti Attacks

Exmatter is a custom data-exfiltration tool that was discovered by the Symantec Threat Hunter team in October 2021. It is designed to steal specific file types from a number of selected directories and upload them to an attacker-controlled server prior to deployment of the ransomware itself on the victim's network. This is the third time a custom data-exfiltration tool appears to have been developed by ransomware operators, following the earlier discovery of the Ryuk Stealer tool and StealBit, which is linked to the LockBit ransomware operation.

While Exmatter was initially spotted being used in a BlackMatter ransomware attack, it was also subsequently used in an attack where Conti was deployed in December 2021. This indicates that Exmatter is likely to be the product of a ransomware affiliate rather than Coreid or Miner (the ransomware developers behind BlackMatter and Conti, respectively).

Once executed, the tool attempts to exfiltrate files from a local machine according to some hardcoded rules. It will search a number of specified directories for the following file types: .doc, .docx, .xls, .xlsx, .pdf, .msg, .png, .ppt, .pptx, .sda, .sdm, .sdw, or .csv. It attempts to prioritize any files for exfiltration by using LastWriteTime. Multiple variants of Exmatter have been observed, indicating that the actor behind it is continually refining the tool in order to expedite exfiltration of a sufficient volume of high-value data as quickly as possible.

Once it has finished exfiltrating data from victim machines, Exmatter runs a command to remove any trace of itself.

Vectors

It can often be hard to establish the initial infection vector used in ransomware attacks. However, some of the known vectors commonly used by targeted ransomware actors include:

- Email – phishing and spam campaigns
- Vulnerability exploitation
- Botnets

The initial access vectors used by ransomware attackers are relevant because if a ransomware actor discovers a vector that gives them extensive access to victim networks it could allow them to execute highly disruptive and costly attacks. It can also allow them to become a dominant figure on the ransomware landscape if they discover a way to infiltrate victim networks that other ransomware actors do not have access to, such as knowledge of a zero-day vulnerability or access to a particularly powerful botnet.

Email Used to Deliver SquirrelWaffle Loader

SquirrelWaffle is a malware loader that first appeared in September 2021, and which was described by some researchers as a potential successor to Emotet - before the latter's reappearance (*see Case Study*). Email is a known tool for delivering ransomware threats, and SquirrelWaffle is primarily spread via spam campaigns and used to deliver Qakbot and Cobalt Strike, which are commonly seen pre-ransomware tools.

The spam emails delivering SquirrelWaffle generally contain hyperlinks to malicious Zip archives that include a malicious .doc or .xls attachment. In a campaign analyzed by Cisco Talos, the actors used the DocuSign signing platform to trick the recipients into enabling macros on malicious documents.

If the victim enables macros on the document, SquirrelWaffle is fetched, which leads to the eventual download of Qakbot and Cobalt Strike onto victim machines. All communications between SquirrelWaffle and its C&C servers are encrypted, while the malware also contains an IP address block list that is populated with notable security research firms as a way to evade detection and analysis. It was noted by Cisco Talos researchers when it appeared on the scene that SquirrelWaffle's "distribution campaigns, infrastructure, and [C&C] implementations feature several interesting techniques that are similar to those seen from other more established threats."

Qakbot and Cobalt Strike are classic pre-ransomware tools. Symantec researchers spotted a campaign in October 2021 that deployed many of the same tactics as those seen in SquirrelWaffle activity. The same paths and file names were used in this campaign as were used in a SquirrelWaffle campaign Netskope blogged about, but we did not see the SquirrelWaffle loader being deployed. In this campaign Qakbot was used to deliver Cobalt Strike, and while ransomware was not observed being delivered, that is believed to have been the likely end goal of the campaign.

Victims received an email with a Zip file attached. This Zip file contained a malicious Excel file. If victims opened the malicious Excel document, Qakbot was launched on their machines. Once Qakbot was executed, the attackers carried out some reconnaissance activity, including discovering shared resources on the device, as well as the name of the server and local groups on the device. Meanwhile, AdFind and various other suspicious files were also executed. A Cobalt Strike beacon loader was then also executed from a scheduled task. The attackers then attempted to execute another unknown file, which is likely to have been ransomware.

Vulnerabilities in Public-Facing Applications Leveraged by Ransomware Actors

Leveraging vulnerabilities in public-facing applications has become an increasingly popular attack vector for cyber criminals and advanced persistent threat (APT) groups over the last couple of years, and ransomware actors have been no exception.

The ProxyLogon vulnerabilities in Microsoft Exchange Server, which came to light in March 2021, were known to be leveraged by ransomware actors, among others. The AvosLocker (aka Sirex) ransomware, which is an RaaS offering that was first seen in July 2021, was spotted in late November and December 2021 leveraging vulnerabilities in Microsoft Exchange Server to gain initial access to victim networks. It would then drop web shells in non-standard folders on the server, likely to allow for remote code execution.

The actors also abused the legitimate SoftEther VPN, renaming a copy of it to "systemresetosupdate.exe" to hide its functionality. Mimikatz and SecretsDump were also dropped in these attacks for credential theft. Certutil was used to download additional payloads, while AnyDesk was installed for lateral movement.

Elsewhere, bugs in virtual private networks (VPNs) were also a popular target. A known bug (CVE-2018-13379) in Fortinet's VPN product is known to have been exploited by targeted ransomware actors. The Australian Cyber Security Centre (ACSC) published an advisory in mid-2021 warning that LockBit 2.0 ransomware attackers were using CVE-2018-13379 to gain initial access to victim networks. Elsewhere, Canthroid (aka Thieflock) is known to compromise victims by exploiting a 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 exploitation of this vulnerability allows an attacker to create their own credentials and join the target's network.

More recently, the vulnerabilities in Apache Log4j, which were discovered in December 2021, were reportedly being exploited by ransomware families, among others. The Dridex botnet, which is known to deliver ransomware, was reported as exploiting the vulnerabilities. Meanwhile, it was also reported that a ransomware family called Khonsari was attempting to leverage the vulnerabilities to access victim networks.

Case Study

Botnets: The Return of Emotet and the Importance of Access Brokers

The biggest development in the area of ransomware infection vectors over the last few months has been the apparent return of the Emotet botnet.

Emotet was one of the most notorious botnets on the cyber-crime landscape before it was taken down by law enforcement early in 2021. Emotet was known to act as a distributor and loader for a wide variety of threats, but prior to its disappearance it had been most strongly linked to collaborations with Trickbot and the Ryuk ransomware. It was considered a major victory for law enforcement when Emotet was successfully taken offline and computers that had been infected by it cleaned up, but in mid-November 2021 Emotet reappeared.

While in its prior incarnation Emotet was often seen delivering Trickbot, when it returned Trickbot appeared to be used to drop Emotet on victim machines in an effort to rebuild the botnet. Subsequently, a report from Advanced Intel claimed actors associated with Conti were involved with the return of Emotet, having reportedly managed to convince former Emotet operators to begin working again, setting up backend infrastructure and reviving their malware builder. The return was apparently driven by a demand for initial access type malware, with Conti reportedly believing that by bringing Emotet into their orbit they can corner the ransomware market as it will give them an edge over rival ransomware operators. Emotet has also been seen dropping Cobalt Strike since its reappearance, which is a common pre-ransomware tool.

Botnets are known to be one of the preferred distribution methods of ransomware actors, and Emotet was far from the only botnet used to distribute ransomware payloads. Other well-known botnets used for this purpose include the aforementioned Trickbot (associated with Miner), Dridex (associated with Hispid), and IcedID (seen used with Conti). However, Emotet was a particularly powerful botnet at its height and if it gets back to a similar level of penetration as it had prior to its takedown, its impact on the ransomware and cyber-crime landscape in general is likely to be significant.

Conclusion

Indications are that ransomware will remain the dominant threat on the cyber-crime landscape in 2022. The main names on the ransomware landscape are likely to continue to change and evolve as takedowns and sanctions have an impact on ransomware developers and their affiliates. However, as Hispid (aka Evil Corp) shows, sanctions alone are not necessarily enough to stop these ransomware gangs, rather actions like that can just force them to rebrand frequently. However, it became clear in 2021, particularly since the Colonial Pipeline attack, that authorities are increasingly willing to take action to disrupt and take down ransomware and other cyber-crime gangs.

A significant occurrence in the first weeks of 2022 was the arrest by Russian authorities in Russia of 14 members of the REvil ransomware gang, with Russian law enforcement saying they took this action after receiving information about alleged REvil members from U.S. authorities. This was a highly unusual move from police in Russia, which have generally largely turned a blind eye to the activities of the large number of ransomware gangs that are believed to operate in the country, provided Russian organizations or individuals are not targeted. This is why we so often see machines located in Russia and other CIS countries excluded from the lists of countries that ransomware will attempt to infect. However, if this recent operation indicates a greater willingness on the part of authorities in Russia to take action against ransomware gangs in the country it could have a significant impact on the ransomware landscape.

Despite the disruptions to the ransomware landscape caused by takedowns and arrests, ransomware operators continue to innovate. This was seen with the development of Noberus, the first professional ransomware strain coded in Rust that has been used in real-world attacks, and the development of new tools for use in ransomware attacks, such as the SquirrelWaffle loader and the Exmatter exfiltration tool. The return of the Emotet botnet, if it reaches anything like the influence it had prior to its shutdown, is also likely to have a significant impact on the ransomware landscape in 2022.

While it can be hard to predict what will happen on the cyber-crime landscape in any given year due to the fast-changing nature of cyber criminals' activity, it seems clear that targeted ransomware attacks will be a key threat that large enterprise organizations will continue to face this year, and likely beyond. This is why it is important for all organizations to have an effective cyber-security strategy in place in order to protect themselves and mitigate the dangers of targeted ransomware attacks.

Mitigation

Symantec recommends customers 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.

Protection

How Symantec Solutions Can Help

Symantec, a division of Broadcom Software, 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, 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 the Symantec 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

Symantec™
by Broadcom Software

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

Copyright © 2022 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom Inc. and/or its subsidiaries. Broadcom, the pulse logo, Connecting everything, and Symantec are among the trademarks of Broadcom.

SES_TTL_WP112 January 31, 2022