BROADCOM SOFTWARE

WHITE PAPER

The Ransomware Threat

By Symantec Threat Hunter Team

WHITE PAPER

The Ransomware Threat

BROADCOM SOFTWARE

TABLE OF CONTENTS

Introduction

Ransomware continues to be among the most critical risks facing organizations of all sizes. Attackers have perfected techniques and business models that will pose a challenge to even the best prepared organizations.

While the encryption of a high volume of computers on a network can potentially be mitigated by adequate backups, ransomware actors have discovered new avenues of extortion, such as threatening to release data stolen prior to encryption. While ransomware attacks are time consuming to perform, ransomware actors have managed to achieve scale through the introduction of "ransomware-as-a-service" operations, renting out their tools and infrastructure to other attackers in exchange for a cut of the profits.

The ransomware landscape experienced a period of upheaval during 2022, in part caused by the Russian invasion of Ukraine, which led to the breakdown of relationships between threat actors based in Russia and collaborators based in other countries, which in some cases involved the leaking of internal data on ransomware operations.

A number of major ransomware operations also closed during 2022, most notably Conti, which appeared to be prompted by a desire to maintain a lower profile. Former Conti associates have reportedly split into smaller groups and begun collaborating with other threat actors.

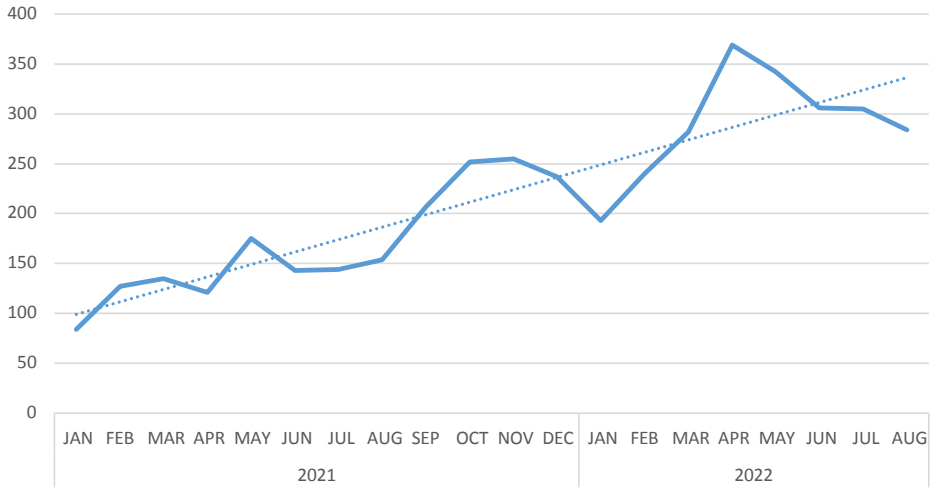
Unfortunately, the negative impact of disruption has been counteracted by the growth of newer ransomware operations. Ransomware attacks show no sign of abating and will probably continue to be a major focus for cyber-crime actors for as long as they yield tangible rewards.

Ransomware by Numbers

Despite severe disruption in the ransomware landscape over the past year, the overall threat posed by ransomware to organizations has not diminished and instead has increased.

NEW RANSOMWARE OPERATIONS TEND TO QUICKLY EMERGE AND REPLACE THREATS THAT HAVE EITHER BEEN RETIRED OR SHUTDOWN.

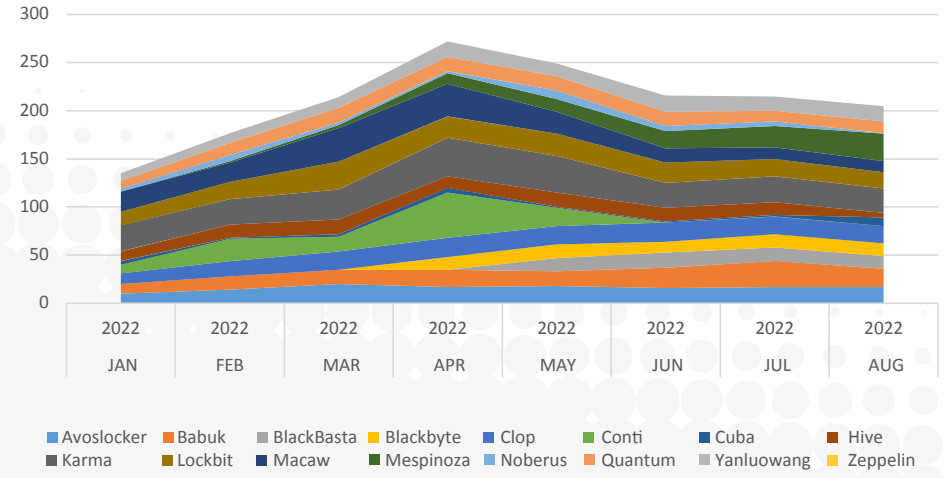
Figure 1. Number of organizations affected by targeted ransomware attacks, January 2021 to August 2022



While the number of attacks has periodically dipped, most notably in the summer months of 2021 and 2022, and in early 2022, the number of organizations attacked is trending upwards. Driving this increase are two factors. Firstly, new ransomware operations tend to quickly emerge and replace threats that have either been retired or shutdown. Secondly, the advent of ransomware-as-a-service has made it easier for attackers to remain active. If one ransomware-as-a-service operation shuts down, its affiliates will usually have a range of alternative options.

It should be noted that these figures are only a representative sample of all attempted targeted ransomware attacks. They consist of confirmed attacks from known targeted ransomware families. Most targeted ransomware attacks are blocked before the payload is deployed, meaning they may not be identified as a ransomware attack. In addition to this, even if a payload is deployed, it may be blocked by a generic or machine-learning-generated detection signature rather than a detection linked to that ransomware family and thus won't be logged as a confirmed targeted ransomware attack.

Figure 2. Number of organizations affected by major targeted ransomware operations, January 2022 to August 2022

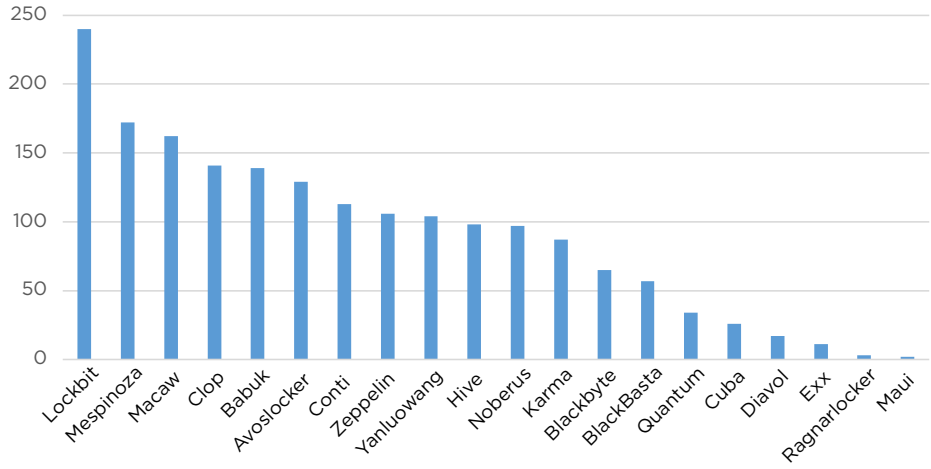


WHILE THERE ARE DOZENS OF TARGETED RANSOMWARE THREATS OPERATING AT ANY ONE POINT OF TIME, THE MAJORITY OF ATTACKS TEND TO INVOLVE A SMALL NUMBER OF PROMINENT RANSOMWARE OPERATIONS THAT TEND TO DOMINATE THE RANSOMWARE LANDSCAPE.

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.

While there are dozens of targeted ransomware threats operating at any one point of time, the majority of attacks tend to involve a small number of prominent ransomware operations that tend to dominate the ransomware landscape, usually by being able to win over affiliates with superior infrastructure and tooling. When big operations disappear, such as the Conti shutdown in May 2022, other groups tend to gain, with operations such as Noberus and Black Basta expanding in this case.

Figure 3. Top ransomware payloads by organizations attacked, January 2022 to August 2022



Ransomware Tools

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 tactics, techniques, and procedures (TTPs) are employed to infiltrate the victim's network, steal credentials, elevate privileges, move laterally across the network, potentially exfiltrate sensitive data, 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, 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 pre-ransomware tools, January – August 2022

PsExec	22%	SystemBC	7%
VssAdmin	22%	PDQ Deploy	7%
Cobalt Strike	15%	Rclone	7%
PowerShell	15%	AdFind	4%
WMI	11%	Netscan	4%
net.exe	11%	Atera	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.

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. A large proportion of the list was taken up by freely available, dual-use tools or operating system features, such as PsExec. The main exception was Cobalt Strike, commodity malware that is commercially sold as a penetration testing framework but is frequently used by ransomware actors.

- **PsExec:** Microsoft Sysinternals tool for executing processes on other systems. The tool is primarily used by attackers to move laterally on victim networks.
- **VssAdmin:** A Windows command-line tool that is used to manage Volume Shadow Copies. It can be used by attackers to delete shadow copies and/or resize the storage allocation. Resizing may limit the space allocated for Volume Shadow Copies, potentially preventing more from being created.
- **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.
- **PowerShell:** Microsoft scripting tool that can be used to run commands, download payloads, traverse compromised networks, and carry out reconnaissance.
- **WMI (Windows Management Instrumentation):** Microsoft command-line tool that can be used to execute commands on remote computers.
- **Net.exe:** Microsoft tool that can be used to stop and start the IPv6 protocol.
- **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.
- **PDQ Deploy:** A legitimate software tool that allows users to manage patching on multiple software packages in addition to deploying custom scripts.
- **Rclone:** An open-source tool 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.
- **AdFind:** A publicly available tool that is used to query Active Directory. It has legitimate uses but is widely used by attackers to help map a network.
- **NetScan:** SoftPerfect Network Scanner (netscan.exe), a publicly available tool used for discovery of host names and network services.
- **Atera:** Legitimate remote monitoring and access software. It and similar tools are often used by attackers to obtain remote access to computers on a network.

WITH MILLIONS OF INCIDENTS LOGGED EACH YEAR, IT IS POSSIBLE TO FORM A PICTURE OF WHAT THE MOST FREQUENTLY USED TECHNIQUES ARE.

Tactics, Techniques, and Procedures (TTPs)

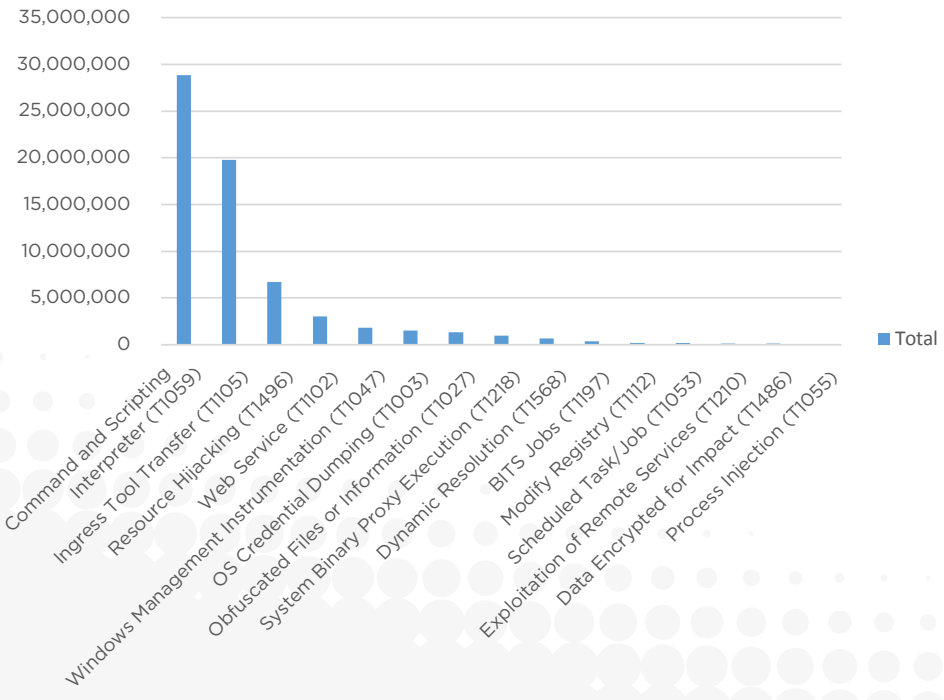
The MITRE ATT&CK matrix classifies attack techniques and tactics. It divides attack tactics into 14 main categories, which map to the typical attack chain between vector and payload execution.

- Reconnaissance
- Resource Development
- Initial Access
- Execution
- Persistence
- Privilege Escalation
- Defense Evasion
- Credential Access
- Discovery
- Lateral Movement
- Collection
- Command and Control
- Exfiltration
- Impact

Within these categories, there are 193 distinct attack techniques and 401 sub-techniques. Some may be employed at multiple stages of an attack chain, meaning they can apply to more than one of the above 14 categories.

Symantec's Cloud Analytics classifies all incidents with a MITRE technique name. With millions of incidents logged each year, it is possible to form a picture of what the most frequently used techniques are. Cloud Analytics draws on intelligence gathered from analyst investigations and leverages advanced machine learning to identify and block patterns of suspicious activity. Because it is designed to identify malicious activity, more so than malicious tools, the vast majority of incidents created relate to TTPs.

Figure 4. Top MITRE techniques associated with Cloud Analytics Incidents, January – October 2022



It is important to note that these incidents are associated with all attacks, not just ransomware. However, this overall data nevertheless has relevance to any organizations attempting to safeguard against ransomware.

Prevalent techniques point to potential pain points or areas of weakness in organizations' defenses. A high proportion of the most frequently used techniques are leveraged by ransomware actors.

These include:

- **Command and Scripting Interpreter (T1059):** This involves an attacker leveraging a command or scripting tool, usually built into the operating system, in order to execute commands or run scripts. In the vast majority of incidents created by Cloud Analytics the interpreter used is PowerShell, a component of Windows.
- **Ingress Tool Transfer (T1105):** Transferring tools or files from external sources onto a compromised network, either via download from a C&C server or through other methods such as FTP. Introducing new tools on to the targeted network is a key component of a ransomware attack. The ransomware payload itself, along with any other tools needed to deploy the ransomware across the network will need to be transferred.
- **Web Service (T1102):** Attackers may use an existing, legitimate web service as a means for relaying information and commands to and from a compromised computer. Well known websites and social media platforms can sometimes be used for C&C purposes since communication to them may not arise suspicion. Ransomware actors need external C&C servers to host tools and relay commands.
- **Windows Management Instrumentation (T1047):** Windows Management Instrumentation (WMI) is a Windows component that can be used to execute commands on remote computers. It is frequently used by ransomware attackers to deploy tools and payloads across the victim's network.
- **OS Credential Dumping (T1003):** This technique involves obtaining credentials, either hashed or in cleartext, usually through a dump of the computer's memory. A range of freely available tools such as Mimikatz or LaZagne can be used to perform this task. Credential dumping is a key step in most ransomware attacks. Stolen credentials can be used to elevate privileges and move laterally to other machines on the network.
- **Obfuscated Files or Information (T1027):** Attempting to make a malicious file difficult to discover by encoding it or otherwise obfuscating its contents. Obfuscation is frequently used by ransomware actors in order to disguise malicious tools.
- **System Binary Proxy Execution (T1218):** Attackers may use a trusted application to execute malicious content. For example, some ransomware attackers have used mshta.exe in order to perform proxy execution of malicious .hta files, JavaScript, or VBScript through a trusted Windows utility.
- **Dynamic Resolution (T1568):** Where attackers dynamically establish connections to C&C infrastructure to evade static detection methods. This is usually done by tools that share a common algorithm with the C&C infrastructure the attackers use. A number of ransomware actors have used this technique.

RECENT BLACK BASTA ATTACKS HAVE FEATURED THE QAKBOT MALWARE (W32. QAKBOT) AT AN EARLY STAGE IN THE ATTACK CHAIN, SUGGESTING THAT CARDINAL MAY CURRENTLY BE PURCHASING ACCESS TO TARGETED NETWORKS FROM QAKBOT'S OPERATORS.

- **BITS Jobs (T1197):** Windows Background Intelligent Transfer Service (BITS) is a low-bandwidth, asynchronous file transfer mechanism. Ransomware attackers frequently leverage BITSAdmin, a Microsoft Windows tool that can be used to create download or upload jobs and monitor their progress.
- **Modify Registry (T1112):** Ransomware actors are known to modify the registry to hide configuration information within registry keys, or deleting information in order to remove evidence of intrusions.
- **Scheduled Task/Job (T1053):** Ransomware actors have been known to leverage built-in task scheduling functionality to facilitate the execution of malicious code.
- **Exploitation of Remote Services (T1210):** Ransomware actors may attempt to exploit remote services to gain unauthorized access to internal systems once inside of a network. This is frequently achieved through exploitation of known vulnerable services such as SMB or RDP.
- **Data Encrypted for Impact (T1486):** Data encryption for malicious purposes is the main end goal of virtually all ransomware attacks.
- **Process Injection (T1055):** Ransomware actors may inject code into processes in order to evade process-based defenses as well as to possibly elevate privileges. This technique is leveraged by both ransomware and precursor malware such as Bumblebee and BazarLoader.

Ransomware Threat Actors

Cardinal

Ransomware families: Black Basta (Ransom.Basta)
Active since: 2022
Ransomware-as-service: No

Cardinal is the operator of the recently-developed Black Basta ransomware. The first evidence of its existence dates from April 2022, when a Russian-language post on underground forums said that it was interested in purchasing access to organizations based in the U.S., Canada, UK, Australia, and New Zealand. The group made an immediate impact with a high volume of attacks, which suggests that they are experienced operators but, as yet, there has been no evidence of any clear link to older ransomware operations. While there have been some reports that Black Basta is a ransomware-as-a-service operation, no confirming evidence has emerged. Cardinal has never advertised for affiliates.

Recent Black Basta attacks have featured the Qakbot malware (W32.Qakbot) at an early stage in the attack chain, suggesting that Cardinal may currently be purchasing access to targeted networks from Qakbot's operators.

Attacks involving Black Basta have been observed using living-off-the-land tools such as PowerShell, VssAdmin, WMI, PsExec, BITSAdmin; the commodity malware Backdoor.SystemBC (aka Coroxy), Mimikatz, Bloodhound, and Sharphound; and legitimate tools such as SoftPerfect Network Scanner (aka netscan) Rclone, Atera Agent, Splashtop, and GoToAssist.

According to SentinelOne, the group is known to use a custom defense-impairment tool called WindefCheck.exe. It will display a fake Windows Security GUI and tray icon even if Windows Defender is disabled. A custom packer used with this tool was also used to create a version of BIRDDOG

HECAMEDE HAS BEEN ACTIVE SINCE AT LEAST JULY 2021. THE GROUP SPRANG TO PUBLIC ATTENTION IN FEBRUARY 2022 WHEN THE U.S. FEDERAL BUREAU OF INVESTIGATION (FBI) AND THE U.S. SECRET SERVICE ISSUED A JOINT ALERT STATING THAT BLACKBYTE HAD BEEN USED TO ATTACK MULTIPLE ENTITIES IN THE U.S. INCLUDING ORGANIZATIONS IN AT LEAST THREE U.S. CRITICAL INFRASTRUCTURE SECTORS.

(aka SocksBot), a backdoor used by the Coreid group (aka FIN7). This suggests that at least one developer has worked for both groups. Whether this is the extent of the ties between the two groups remains unclear.

Black Basta has been observed changing the icons of encrypted files to the Basta icon, which is a geometric image of a cube. Files encrypted by Black Basta are appended with the .basta file extension. Cardinal also has a Linux variant of Black Basta that targets VMware ESXi virtual machines (VMs) running on enterprise Linux servers.

Hecamede

Ransomware families: BlackByte (Ransom.Blackbyte)
Active since: 2021
Ransomware-as-service: Yes

Exbyte: New Custom Exfiltration Tool

In October 2022, Symantec's Threat Hunter Team discovered that at least one Hecamede affiliate had begun using a custom data-exfiltration tool during their attacks. The malware (Infostealer.Exbyte) is designed to expedite the theft of data from the victim's network and upload it to an external server.

Exbyte is written in Go and designed to upload stolen files to the Mega.co.nz cloud storage service.

On execution, it performs a series of checks for indicators that it may be running in a sandboxed environment. To do this, it calls the IsDebuggerPresent and CheckRemoteDebuggerPresent APIs. It then checks for the running processes from the following applications:

- MegaDumper 1.0 by CodeCracker / SnD
- Import reconstructor
- x64dbg
- x32dbg
- OLLYDBG
- WinDbg
- The Interactive Disassembler
- Immunity Debugger - [CPU]

It then checks for the following antivirus or sandbox-related files:

- avghooka.dll
- avghookx.dll
- sxin.dll
- sf2.dll
- sbiedll.dll
- snxhk.dll
- cmdvrt32.dll
- cmdvrt64.dll
- wpespy.dll
- vmcheck.dll
- pstorec.dll
- dir_watch.dll
- api_log.dll
- dbghelp.dll

This routine of checks is quite similar to the routine employed by the BlackByte payload itself, as documented recently by Sophos.

Next, Exbyte enumerates all document files on the infected computer, such as .txt, .doc, and .pdf files, and saves the full path and file name to %APPDATA%\dummy. The files listed are then uploaded to a folder the malware creates on Mega.co.nz. Credentials for the Mega account used are hardcoded into Exbyte.

Exbyte is not the first custom-developed data-exfiltration tool to be linked to a ransomware operation. In November 2021, Symantec discovered Exmatter, an exfiltration tool that was used by the BlackMatter ransomware operation and has since been used in Noberus attacks. Other examples include the Ryuk Stealer tool and StealBit, which is linked to the LockBit ransomware.

Hecamede has been active since at least July 2021. The group sprang to public attention in February 2022 when the U.S. Federal Bureau of Investigation (FBI) and the U.S. Secret Service issued a joint alert stating that BlackByte had been used to attack multiple entities in the U.S. including organizations in at least three U.S. critical infrastructure sectors. In recent months, BlackByte has become one of the most frequently used payloads in ransomware attacks.

In recent BlackByte attacks investigated by Symantec, the attackers exploited the ProxyShell (CVE-2021-34473, CVE-2021-34523, and CVE-2021-31207) and ProxyLogon (CVE-2021-26855 and CVE-2021-27065) vulnerabilities in Microsoft Exchange Servers to gain initial access.

Symantec has observed attackers using AdFind, AnyDesk, NetScan, and PowerView prior to deploying the ransomware payload.

Cimbex

Ransomware families: Quantum (Ransom.Quantum), MountLocker (Retired)
Active since: 2020
Ransomware-as-service: No

Cimbex first appeared in September 2020 with the creation of the MountLocker ransomware, which was one of the more frequently used ransomware payloads for a number of months. MountLocker was frequently renamed by affiliates, e.g. XingLocker and AstroLocker.

The most recent version of the group's payload has been dubbed Quantum. While Quantum has occasionally been described as a ransomware-as-a-service operation, this appears to be unconfirmed.

The main infection vector appears to be email. In some cases, email campaigns have delivered the IcedID malware, which was then used to deliver Quantum. IcedID was seen in some instances being delivered as a DLL within an ISO file. Quantum has also used LNK files to execute payloads, as well as using scheduled tasks to achieve persistence on victim machines.

The Bumblebee loader has also been seen delivering the Quantum ransomware. This too was delivered to targets via a spear-phishing email with an attached ISO file. This ISO file contained a Bumblebee DLL file and an LNK file, which loaded the Bumblebee DLL file using rundll32.exe.

The ransomware has also been known to leverage commodity and living-off-the-land tools like Cobalt Strike, Rclone, the Ligolo tunneling tool, ProcDump and AdFind. Actors using Quantum have also used LSASS to extract credentials, WMI for discovery tasks, as well as leveraging PsExec and PowerShell.

In the most recent Quantum attacks observed by Symantec, the attackers used the NPPSpy tool to collect login data, including cleartext passwords, from compromised machines. NPPSpy is a network provider/credential manager DLL that monitors for and extracts credentials and stores them in cleartext in a log file. While NPPSpy has been available for some time, it has rarely been used in the wild. The attackers were observed using NPPSpy on compromised Microsoft Exchange servers for two months before executing a Cobalt Strike stager, which was then used to deploy the Quantum ransomware.

COREID IS ONE OF THE MOST LONG-ESTABLISHED CYBER-CRIME GROUPS, HAVING BEEN ACTIVE FOR AT LEAST A DECADE. IT ORIGINALLY MADE A NAME FOR ITSELF USING A VARIANT OF THE NOTORIOUS CARBANAK FINANCIAL TROJAN, WHICH WAS USED TO STEAL HUNDREDS OF MILLIONS OF DOLLARS.

Syrphid

Aliases: Bitwise Spider
Ransomware families: LockBit (Ransom.Lockbit)
Active since: 2019
Ransomware-as-service: Yes

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 ransomware-as-a-service 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. LockBit attackers are also known to buy access to already compromised servers on underground forums.

In some cases, the attackers will brute force 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 affiliates 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 from July 2021 onwards, when Syrphid appeared to be one of the main beneficiaries of the departure of the Sodinokibi ransomware operation. The latter ceased operations after the public attention drawn by the Kaseya ransomware supply chain attack and the subsequent indictment of one of its members. In 2022 LockBit was the most frequently used ransomware payload in attacks logged by Symantec.

In September 2022, the group appeared to undergo a period of internal discord when a builder for the LockBit 3.0 (aka LockBit Black) payload was leaked. A spokesperson for Syrphid claimed that a disgruntled developer was responsible for the leak.

Coreid

Aliases: FIN7, Carbon Spider
Ransomware families: Noberus, Darkside (retired), BlackMatter (retired)
Active since: 2012
Ransomware-as-service: Yes

Coreid is one of the most long-established cyber-crime groups, having been active for at least a decade. It originally made a name for itself using a variant of the notorious Carbanak financial Trojan, which was used to steal hundreds of millions of dollars from numerous financial institutions and their customers.

The group undertook a major shift in operations in 2020, when it moved to targeted ransomware attacks and launched its own ransomware-as-a-service operation called Darkside. This 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.

Darkside appeared to become inactive following the Colonial attack after some of its infrastructure was taken offline. Coreid re-emerged in late July 2021, when it launched a new ransomware-as-a-service operation called BlackMatter. Although BlackMatter's operators initially denied a link to Darkside, research by CrowdStrike linked Coreid to both the Darkside and BlackMatter ransomware strains.

NOBERUS ALSO ATTEMPTS TO PROPAGATE VIA NETWORK SHARES, LOOKING FOR AVAILABLE SHARES BY USING THE 'NET USE' COMMAND OR NETSHAREENUM FUNCTION. EMBEDDED ADMINISTRATIVE CREDENTIALS MAY THEN BE USED FOR PROPAGATION VIA NETWORK SHARE.

BlackMatter was active until early November 2021, when it announced it was shutting down, most likely due to the pressure the group was experiencing from law enforcement. The announcement also came just days before U.S. authorities announced they would be offering a $10 million reward for information that may lead to the arrest of any members of the gang who were behind the Darkside attack on Colonial Pipeline.

Coreid quickly reappeared with the launch of yet another new ransomware-as-a-service operation known as Noberus (aka ALPHV, BlackCat), which remains active to this day. While Noberus was initially positioned as a new venture, it is now widely believed to be a successor operation to BlackMatter.

Noberus, which is written in Rust, has a highly-customizable feature set allowing for attacks on a wide range of corporate environments. Coreid claims that Noberus is capable of encrypting files on Windows, EXSI, Debian, ReadyNAS, and Synology operating systems.

The malware is command-line driven and has the ability to use different encryption routines, spread between computers, kill virtual machines and ESXi virtual machines, and automatically wipe ESXi snapshots to prevent recovery. It can be configured with domain credentials that can be used to spread to and encrypt other devices on the compromised network. The malware also uses PsExec, which is embedded in a compressed form within Noberus, to copy itself to other devices on the network and execute itself.

Noberus also attempts to propagate via network shares, looking for available shares by using the 'net use' command or NetShareEnum function. Embedded administrative credentials may then be used for propagation via network share.

Once executed, it deletes any available shadow copies and collects system information via WMIC in order to collect Universally Unique Identifiers (UUIDs) from each machine. These are used to generate an 'access token' that makes up part of the unique Tor address victims are instructed to visit. The access token acts as a unique key, which is used to distinguish the victim when visiting Coreid's Tor site.

Noberus then proceeds to terminate a set of pre-defined processes and begin the encryption process. It can also exclude certain directories, file names, and file extensions from the encryption process.

In all the samples of Noberus seen by Symantec, the victim's administrative credentials were embedded as part of the configuration block, showing that the attacks were specifically targeted at the victim.

The ransomware offers two encryption algorithms (ChaCha20 and AES), as well as four encryption modes – Full, Fast, DotPattern, and SmartPattern – to affiliates. Full mode is the most secure but also the slowest. SmartPattern (aka intermittent encryption) offers encryption of "N" megabytes in percentage increments. By default, it encrypts with a strip of 10 megabytes every 10% of the file starting from the header, which would be an optimal mode for attackers in terms of speed and cryptographic strength.

Eamfo: Custom credential stealing tool used in Noberus attacks

At least one affiliate of the Noberus ransomware operation has begun using information-stealing malware that is designed to steal credentials stored by Veeam backup software. Veeam is capable of storing credentials for a wide range of systems, including domain controllers and cloud services. The credentials are stored to facilitate the backup of these systems. The malware (Infostealer.Eamfo) is designed to connect to the SQL database where Veeam stores credentials, and it steal credentials with the following SQL query:

- select [user_name],[password],[description] FROM [VeeamBackup].[dbo].[Credentials]

Eamfo will then decrypt and display the credentials.

Eamfo appears to have been in existence since at least August 2021, and there is evidence that it has previously been used by attackers using the Yanluowang and LockBit ransomware families. A recent report from BlackBerry also detailed Eamfo being used alongside a new ransomware strain it dubbed Monti, which appears to be based on the leaked source code of the Conti ransomware. The TTPs used in Monti attacks also closely resemble former Conti attack chains, suggesting those behind Monti may be former affiliates of that group.

Stealing credentials from Veeam is a known attack technique that can facilitate privilege escalation and lateral movement, providing the attackers with access to more data they can potentially exfiltrate and more machines to encrypt.

Noberus attacks involving Eamfo seen by Symantec also utilized GMER, a relatively old rootkit scanner that can be leveraged by ransomware actors to kill processes. GMER usage by ransomware attackers appears to have become more frequent in recent months, and it was also seen in the Monti attack detailed by BlackBerry.

Miner

Aliases: Wizard Spider
Ransomware families: Diavol (status unknown), Conti (retired), Ryuk (retired), GoGaLocker (retired), MegaCortex (retired)
Active since: 2014
Ransomware-as-service: Yes

Another veteran group, Miner is among the most powerful actors in the cyber-crime ecosystem. It has been 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 was introduced in September 2016. 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 was then repurposed for use as a credential stealer and as a distribution channel for other malware.

STEALING CREDENTIALS FROM VEEAM IS A KNOWN ATTACK TECHNIQUE THAT CAN FACILITATE PRIVILEGE ESCALATION AND LATERAL MOVEMENT, PROVIDING THE ATTACKERS WITH ACCESS TO MORE DATA THEY CAN POTENTIALLY EXFILTRATE AND MORE MACHINES TO ENCRYPT.

Miner also introduced new malware known as BazarLoader and BazarBackdoor in April 2020. Like Trickbot, BazarLoader was 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 pivoted into targeted ransomware, using the Ryuk ransomware. Ryuk was based on the older Hermes ransomware family, which it appears to have acquired from the original developer. During 2019, Miner began using two new ransomware families, GoGalocker (aka LockerGoga) and MegaCortex, but attacks involving GoGalocker and MegaCortex ceased in early 2020.

Miner was then linked to the Conti ransomware, which first appeared in December 2019 and developed into the one of the most long-lived and prolific ransomware-as-a-service operations. Conti unexpectedly and abruptly shut down in May 2022.

According to Advanced Intel, the operation was split into a number of smaller cells in order to reduce the chances of being disrupted by law enforcement. These cells were reportedly exploring partnerships with a number of smaller ransomware operations. Since its closure, there have been numerous reports of what appear to be former Conti affiliates working with a range of different ransomware groups, but to date no obvious successor operation has appeared.

The Conti closure came during a period of major retooling by the Miner group. Activity involving the Ryuk ransomware diminished in late 2022 and it appeared to be replaced by a new ransomware payload called Diavol. However, Diavol activity has diminished in recent months and it is unclear if this ransomware is still active.

In early 2022, one of the group's mainstay pieces of malware Trickbot was also retired. A new loader dubbed Bumblebee subsequently appeared, which is widely regarded as a successor tool for Trickbot and may also be intended as a replacement for BazarLoader. Bumblebee has been used as an infection vector for a number of ransomware families, suggesting Miner is selling access to other ransomware groups.

Bumblebee delivering Quantum ransomware

A mid-2022 attack involving the Quantum ransomware demonstrates how Bumblebee is now being leveraged by attackers to deliver ransomware.

The initial infection vector was a spear-phishing email with an attachment containing an ISO file. This ISO file contained a Bumblebee DLL file and an LNK file, which loaded the Bumblebee DLL file using rundll32.exe.

- rundll32.exe teas.dll,kXINkCKgFC

Bumblebee supports multiple commands like "Ins" for bot persistence, "Dij" for DLL injection, and "Dex" for downloading executables.

During the attack, Bumblebee contacted a C&C server (45.153.243.93) and created a copy in the %APPDATA% folder with a random name, and also created a VBS file at the same location to load the %APPDATA% DLL file.

A scheduled task was created using the Bumblebee "Ins" command to run a VBS file every 15 minutes.

A MID-2022 ATTACK INVOLVING THE QUANTUM RANSOMWARE DEMONSTRATES HOW BUMBLEBEE IS NOW BEING LEVERAGED BY ATTACKERS TO DELIVER RANSOMWARE.

- wscript.exe CSIDL_COMMON_APPDATA\[a-f0-9]{16}\[a-f0-9]{16}.vbs
- CSIDL_SYSTEM\rundll32.exe" CSIDL_COMMON_APPDATA\[a-f0-9]{16}\[a-f0-9]{16}.dll

After a couple of hours, Bumblebee used the "Dex" command to drop and run a Cobalt Strike payload named "wab.exe" in the %APPDATA% location. It also ran the "systeminfo" command.

- wmiprvse.exe --> wab.exe
- wmiprvse.exe --> wab.exe --> cmd.exe /C systeminfo

Using the "Dij" command, Bumblebee then injected the Metasploit DLL into the legitimate process "ImagingDevices.exe", which is a Windows Photo Viewer executable file.

In addition to this, using the "Dij" command Bumblebee injected the Cobalt Strike payload into the legitimate "wab.exe", which is a Windows Mail executable file.

Bumblebee then dropped the AdFind tool using the "Dij" command and tried to enumerate domain-related information like domain trust, domain users, domain groups, group permissions, etc.

At this point, Bumblebee dropped the Quantum ransomware using the "Dij" command. The attacker used both DLL and EXE payloads to encrypt files.

- rundll32.exe CSIDL_COMMON_APPDATA\[0-9]{10}.dll,start \shareall \nolog
- CSIDL_COMMON_APPDATA\[0-9]{10}.exe /shareall /NOLOG

Quantum collects system information and user information using WMI. It also checks for SQL-related services and stops them if found running. Quantum also checks for some processes related to malware analysis like procmon, wireshark, cmd, task manager, and notepad, and terminates them if found running.

Hispid

Aliases: EvilCorp, Indrik Spider
Ransomware families: Macaw, BitPaymer (retired), DoppelPaymer, WastedLocker (retired), Hades (retired), Phoenix Locker (retired), Grief (retired)
Active since: 2011
Ransomware-as-service: Not at present

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 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 was reported that DoppelPaymer was developed for use by affiliates.

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 that 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.

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.

The group began frequently 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 then Grief. The most recent name the group has been observed as using is Macaw.

In addition to regularly rebranding, the group has also resorted to using other groups' payloads to avoid being identified. In June 2022, Mandiant researchers said that Hispid had begun using LockBit in some of its attacks, effectively acting as a LockBit affiliate.

Hispid has also begun developing other new, non-ransomware tools. Research by IBM linked Hispid to new malware known as Raspberry Robin. Raspberry Robin can act as a loader for secondary payloads, although the ultimate payload remains unknown. In some cases, Raspberry Robin infections have been seen delivering the SocGholish malware, which has previously been used by Hispid as a precursor to ransomware.

Snakefly

Aliases: Graceful Spider
Ransomware families: Clop
Active since: 2019
Ransomware-as-service: Yes

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 a 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.

THE GROUP'S ATTACKS GENERALLY BEGIN WITH A MALICIOUS EMAIL THAT IS SENT FROM A PREVIOUSLY COMPROMISED ACCOUNT TO MAKE IT MORE CONVINCING.

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.

Birdwing

Aliases: Pysa
Ransomware families: Mespinoza
Active since: 2018
Ransomware-as-service: Unclear

Mespinoza has been one of the more prolific ransomware families during 2022. Developed by a cyber-crime group Symantec calls Birdwing, it is currently unclear whether the group sells Mespinoza to affiliates or whether it carries out all of its attacks itself.

In March 2021 the FBI issued an alert about Birdwing's activities, noting its frequent targeting of educational institutions.

Birdwing is known to gain unauthorized access to networks by compromising Remote Desktop Protocol (RDP) credentials. It has also used phishing emails.

An October 2021 investigation by Symantec noted that the attackers ran a malicious script named p.ps1, via PsExec. This script appears to be the same as one that was also described by Palo Alto. The attackers use the Microsoft .NET compiler (csc.exe) and cvtres.exe together to compile and execute an unknown malicious executable. Mespinoza was launched on machines approximately 24 hours after the p.ps1 file was seen. The Mespinoza payload is given the same name as a legitimate process – "svchost.exe".

Sirex

Ransomware families: AvosLocker
Active since: 2021
Ransomware-as-service: Yes

Sirex operates the AvosLocker ransomware-as-a-service. It first appeared in June 2021 and has been successful at winning affiliates, becoming one of the larger ransomware operators active during 2022.

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 were no weaknesses in its encryption, so it was 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 stolen from victims.

POWERSHELL EMPIRE IS A PUBLICLY AVAILABLE PENETRATION TESTING FRAMEWORK THAT IS OFTEN USED BY ATTACKERS BECAUSE OF ITS EASE OF USE AND THE FACT THAT THEY DON'T HAVE TO RUN POWERSHELL.EXE, POTENTIALLY BYPASSING ANY POWERSHELL-BASED SECURITY MEASURES.

Attackers using PDQ Deploy to deliver AvosLocker

PDQ Deploy is a legitimate software tool that allows users to manage patching on multiple machines in addition to deploying custom scripts.

At least one affiliate of AvosLocker has begun using it to execute malicious PowerShell commands on multiple computers on victims' networks using PowerShell Empire to deploy the AvosLocker payload.

PowerShell Empire is a publicly available penetration testing framework that is often used by attackers because of its ease of use and the fact that they don't have to run powershell.exe, potentially bypassing any PowerShell-based security measures.

The attackers appear to install PDQ Deploy themselves on the victim's network. There is also evidence that PowerShell Empire is also used to run a second script, which will execute the credential-dumping tool Mimikatz.

Recent AvosLocker TTPs

A number or recent AvosLocker attacks have used similar TTPs, suggesting they were carried out by the same threat actor.

Recent attacks used an anti-cheat system driver (mhyprot.sys) for the game Genshin Impact. The vulnerable driver elevates privileges, giving an attacker the ability to access any process/kernel memory; a capability the attacker used to terminate processes.

Other similar TTPs used in the attacks include the use of PsExec for lateral movement and/or remote code execution, and WMI for searching for and disabling Bitdefender services. An SFX file is also used to drop a bundle of tools for use in the attack.

Pinion

Ransomware families: Hive (Ransom.Hive)
Active since: 2021
Ransomware-as-service: Yes

Active since June 2021, Pinion runs the Hive ransomware-as-a-service operation, which has been quite active during 2022. While many ransomware operators profess to avoid attacking healthcare organizations, Pinion appears to be indiscriminate in its choice of targets and Hive has been used to attack several organizations in the healthcare sector, such as non-profit U.S. healthcare provider Memorial Health Systems (MHS) in August 2021.

Hive will attempt to stop processes related to backups, security, and file copying. It has been known to drop a hive.bat script into directories containing encrypted files, 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 batch file, shadow.bat, is dropped into the directory to delete shadow copies,

A TACTIC SEEN ACROSS THESE ATTACKS WAS THE USE OF NETLOGON SHARED FOLDERS TO DELIVER THE RANSOMWARE ACROSS THE NETWORK.

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 contains a Tor link for victims to contact the attackers via live chat. Some victims have also reported receiving phone calls from the attackers.

Hive: Energy sector focus

During 2022, at least one Hive affiliate attacked multiple oil and gas organizations with a regularity that suggested a deliberate focus on the energy sector.

A tactic seen across these attacks was the use of Netlogon shared folders to deliver the ransomware across the network. In several cases, shared folders were used to infect other organizations who had a business relationship with the original victim.

The SystemBC (aka Coroxy) backdoor, Cobalt Strike, and PowerSploit were leveraged in several attacks. VssAdmin, a legitimate Windows command-line tool was frequently used to delete shadow copies. In some cases, a dual-use tool called PCHunter was also deployed.

Dryxiphia

Aliases: Yanluowang
Ransomware families: Yanluowang
Active since: 2021
Ransomware-as-service: Yes

Dryxiphia was discovered by Symantec researchers in September 2021, attempting to carry out ransomware attacks using a new ransomware family called Yanluowang.

Symantec 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 the Thieflock ransomware, suggesting that they may have been a Thieflock affiliate who shifted allegiances to the new Yanluowang operation.

In November 2022, an anonymous individual leaked data that they said included code and internal chats from the Yanluowang ransomware operation. Yanluowang ceased operations after the leak but it is unclear yet whether this closure is permanent.

Batfly

Ransomware families: Karma, Nemty, JSWorm, Nefilim, Fusion, Milihpen, Gangbang
Active since: 2019
Ransomware-as-service: Yes

Active since 2019, Batfly's first ransomware was Nemty, which was available for purchase on underground forums.

In 2020, it rebranded its ransomware to Nefilim and announced it would be no longer for sale. Batfly said that it would instead only work with trusted affiliates.

Milihpen 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.

Its most recent payload Karma appeared in May 2021.

Pollen

Ransomware families: Zeppelin, Buran, VegaLocker
Active since: 2019
Ransomware-as-service: No

Active since 2019, Pollen initially used the VegaLocker ransomware, which somewhat unusually targeted Russian speakers and was spread via malvertising on an online Russian advertising network.

Pollen pivoted to targeted ransomware attacks later that year when it developed the Zeppelin ransomware and began targeting organizations in the U.S and Europe. In a reversal of its previous tactics, Zeppelin, like most ransomware, is designed not to run on computers in Russia or other Commonwealth of Independent States (CIS) countries.

Zeppelin is not run as a ransomware-as-a-service operation but is sold on underground forums. Unlike other ransomware developers, Pollen does not run a ransomware leaks site.

Because Zeppelin can be 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.

Vice Society: A new breed of ransomware group

For the past number of years, ransomware attackers could be split into two broad categories: ransomware developers who may carry out their own attacks and/or sell access to their malware and infrastructure using the ransomware-as-a-service business model; and affiliates who carry out attacks using a toolset provided by a ransomware-as-a-service.

The recently emerged Vice Society is a new type of threat actor because it does not appear to develop its own ransomware but does cultivate its own identity and branding.

According to a CISA Alert, it has deployed versions of Hello Kitty/Five Hands and Zeppelin. Recent investigations by Symantec indicate that it may also be using the Noberus payload. Unlike other ransomware affiliates, Vice Society operates its own data leak site. This degree of autonomy suggests that the group has more power or influence than the average affiliate. Another hallmark of the group is that it has a heavy focus on the U.S. education sector.

Recent Vice Society attacks investigated by Symantec used two masqueraded variants of PAExec for lateral movement. PAExec is a publicly available remote administration tool that has similar functionality to the Windows tool PsExec. In each case the file was renamed PuE.exe. The renaming was likely done to obfuscate its detection or functionality. In one case, the malware Neshta (W32.Neshuta) was used to deliver PAExec

ORGANIZATIONS WHO WISH TO GUARD AGAINST RANSOMWARE ATTACKS SHOULD ADOPT A DEFENSE-IN-DEPTH STRATEGY, USING MULTIPLE DETECTION, PROTECTION, AND HARDENING TECHNOLOGIES TO MITIGATE RISK AT EACH POINT OF A POTENTIAL ATTACK CHAIN.

Conclusion

Current patterns of activity suggest that ransomware will continue to be a major threat to organizations in 2023. Indeed, the current trends suggest that ransomware attacks may increase again next year. Worsening economic circumstances driven by energy prices, interest rates, and inflation may also contribute. Organizations under pressure to contain or reduce spending may not be able to invest as much into their security operations as planned.

The advent of double extortion, where attackers exfiltrate data and threaten to release it unless the ransom is paid is also driving activity. Attackers no longer have to encrypt the entire network to yield maximum results. In some cases, attackers have eschewed encryption completely and opted to solely extort victims with stolen data.

Organizations who wish to guard against ransomware attacks should adopt a defense-in-depth strategy, using multiple detection, protection, and hardening technologies to mitigate risk at each point of a potential attack chain.

In addition to this, organizations should prioritise deepening their knowledge of current infection vectors used, commonly employed TTPs, and the relationship between botnet operations and ransomware actors. This information will assist in prioritization and identifying potential areas of weakness in their defensive posture.

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.

SYMANTEC WEB ISOLATION ELIMINATES WEB THREATS AND SOLVES THE CHALLENGE OF PROVIDING ACCESS TO UNKNOWN, UNCATEGORIZED AND POTENTIALLY RISKY WEB SITES

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

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.

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.

- 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

BROADCOM SOFTWARE

About Broadcom Software

Broadcom Software is a world leader in business-critical software that modernizes, optimizes, and protects the world's most complex hybrid environments. With its engineering-centered culture, Broadcom Software has an extensive portfolio of industry-leading infrastructure and security software, including AIOps, Cybersecurity, Value Stream Management, DevOps, Mainframe, and Payment Security. Our software portfolio enables scalability, agility, and security for the largest global companies in the world.

For more information, visit our website at: software.broadcom.com

Ransomware Whitepaper December 15, 2022