March | 2026

Arete

2025 Annual Crimeware Report

Cyber Threat Trends and Highlights

www.areteir.com

Table of Contents

Overview

Arete helps organizations stay ahead of cyber threats with standardized, intelligence-led detection, response, resolution, and resilience capabilities. Leveraging data and intelligence collected during ransomware and extortion incident response engagements, this report highlights notable trends and shifts in the threat landscape throughout 2025.

The first half of 2025 largely followed a relatively predictable pattern, with the majority of activity coming from the same groups that Arete observed in the second half of 2024. However, after a noticeable lull in activity during Q2, the Akira ransomware group had an unprecedented surge in attacks starting in mid-July that continued throughout the second half of the year. In August alone, Akira was responsible for over half of all ransomware and extortion events Arete responded to, and although its activity started to trend down after August, Akira still maintained historically high attack volumes each month for the rest of 2025.

Akira's unusually high activity levels were largely driven by widespread exploitation of a SonicWall VPN access control vulnerability from 2024. Although Akira was not the only threat group to exploit this vulnerability, it was the most successful.

In addition to vulnerability exploits, social engineering techniques evolved throughout the year. In early 2025, multiple threat groups found success using email bombing and social engineering tactics involving Microsoft Teams to gain initial access. ClickFix, a tactic that leverages fake error dialog boxes to trick users into manually executing malicious PowerShell commands, emerged in 2025 and evolved throughout the year in multiple campaigns.

Trends in ransom demands and payments remained largely consistent with previous years, although there were a few deviations due to the high number of Akira attacks in the second half of the year.

As was the case in 2024, the majority of threat groups remained opportunistic in 2025, commonly leveraging software vulnerabilities, stolen credentials, and social engineering campaigns rather than targeting specific sectors.

Statistics and Trends from Arete's Incident Response Engagements

The threat landscape in 2025 was largely dominated by Akira and Qilin, with Akira's activity in particular reaching unprecedented levels during the year. Akira was already the most prolific threat group in 2024 by a sizeable margin, when the group was responsible for almost 15% of all ransomware and extortion incidents observed by Arete, while the second-most active group accounted for only about 6% of all activity. In 2025, Akira accounted for over 28% of Arete engagements, with a notable surge in the second half of the year.

81
Total Named Threat Actors

52
Total Unnamed Threat Actors

Qilin emerged as one of the top threats starting in Q2, following the sudden departure of the RansomHub threat group from the ransomware ecosystem in early April. The remainder of the 2025 threat landscape was a mix of established groups like Play and INC Ransom, as well as rebrands and subgroups like Lynx, Sinobi Group, and World Leaks.

Akira was the top threat group observed by Arete in 2025, accounting for over 28% of all ransomware and extortion activity throughout the year and over 41% during Q3.

Akira Dominates the Threat Landscape

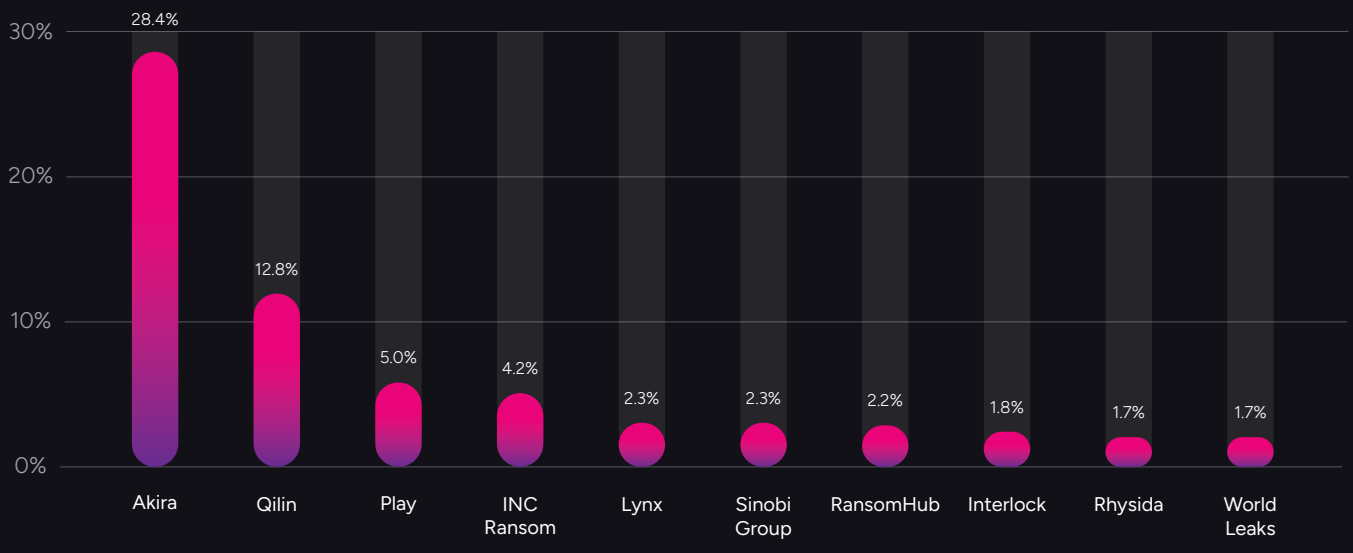
In Q1 of 2025, Akira's activity remained consistent with what Arete observed in 2024, with the group accounting for about 15% of engagements in the first quarter of 2025, followed by a lull in Q2 when it was only responsible for 8% of ransomware attacks. However, starting in July, Akira absolutely dominated the threat landscape. In August, the group was responsible for over half of all ransomware and extortion events, and it accounted for over 41% of activity during the third quarter.

Akira's spike was largely driven by its widespread exploitation of vulnerable SonicWall appliances, specifically through CVE-2024-40766. Although this critical SonicWall VPN access control vulnerability had been patched in 2024, administrators who failed to reset the passwords for all local user accounts on the SonicWall appliance left it vulnerable to exploitation, even though the patched version of the firmware was installed. Although this guidance was disclosed in the original upgrade instructions, it was a key step that many organizations missed, and SonicWall issued updated guidance in August 2025.

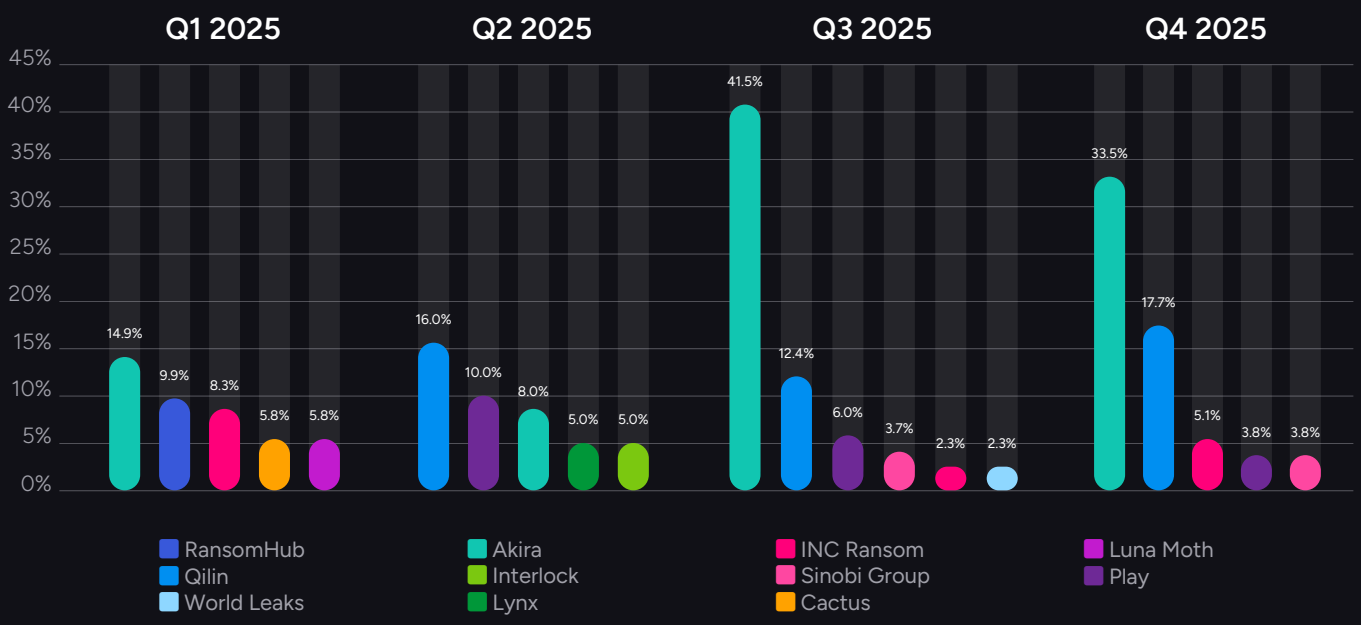
Akira's attack tempo slowed down somewhat in the final quarter of the year, but it still accounted for a historically high percentage of engagements, with one in three ransomware incidents attributed to Akira in Q4 2025. For comparison, in Q4 2024, Akira accounted for 18% of ransomware incidents, which at the time was the highest quarterly activity from a single threat group observed by Arete since at least 2022.

Akira's 2025 campaigns reflected a highly opportunistic yet technically capable operation, and it is difficult to assess how long Akira will be able to sustain such high attack volumes.

TOP THREAT GROUPS OBSERVED IN 2025



TOP THREAT GROUPS BY QUARTER



Other Top Threat Groups in 2025

Qilin

Qilin became noticeably more active in 2025, emerging as the most active threat group during Q2, and trailing only Akira since Q3. This uptick can be attributed to several factors, including the group's exploitation of several vulnerabilities, attracting ex-affiliates of now-defunct groups like RansomHub, and a willingness to work with existing threat groups like Scattered Spider. Given these factors and the activity levels observed in 2025, Qilin will likely remain an active threat in 2026.

Play

Play remains a persistent threat and was the third most active threat group in 2025, after Akira and Qilin. The group is particularly difficult to deal with during communications and is one of the most aggressive threat groups in terms of posting victims to its data leak site (DLS). Play also has higher initial demands than other threat groups. In 2025, Arete did not observe an initial demand from Play of less than $400,000, and about half were greater than $1 million, demonstrating the scale of potential financial losses associated with this threat actor.

Interlock

Although Interlock has only operated since September 2024, the sophistication of its operations is consistent with that of experienced ransomware operators. The group develops its own malware to facilitate attacks and does not appear to operate as a Ransomware-as-a-Service (RaaS), nor has it been observed advertising on dark web forums. Starting in July 2025, Interlock was observed deploying a new remote access trojan (RAT) through a variation of the ClickFix technique called "FileFix," which uses Windows File Explorer to trick users into executing malicious PowerShell scripts. Interlock's evolving tactics and strategic use of ClickFix social engineering techniques demonstrate a high level of operational maturity. The group was among the top ten most active threat groups observed by Arete in 2025 and will likely remain a persistent threat in 2026.

INC Ransom

This group has operated since 2023, but Arete observed a distinct increase in attacks from the group during 2025, with more than double the number of engagements attributed to the group in 2024. This was partly due to the group's exploitation of vulnerabilities in the SimpleHelp Remote Monitoring and Management (RMM) software in early 2025, as well as activity consistent with the TamperedChef infostealer campaign observed later in the year.

Lynx and Sinobi Group

The Lynx RaaS emerged in mid-2024 following law enforcement operations against ALPHV and LockBit. Based on substantial overlap in source code structure and encryption routines, discussed in greater detail below, Lynx appears to be a structured evolution of the INC Ransom codebase, although the groups appear to operate independently. The Sinobi Group, on the other hand, emerged in 2025 and also demonstrates strong similarities with Lynx, including overlapping code, infrastructure, and an almost identical Tor chat and DLS.

Ransomware Spotlight:
Code Comparison, Lineage, and Evolution Between INC Ransom, Lynx, and the Sinobi Group

INC Ransom emerged in mid-2023 as a RaaS operation employing double-extortion tactics. Public reporting later identified that the INC source code was offered for sale on underground forums in early 2024, enabling downstream reuse by other operators and setting the stage for codebase proliferation.

Shortly thereafter, Lynx ransomware emerged in mid-2024. Rather than representing a ground-up rewrite, Lynx appears to be a structured evolution of the INC codebase, reflecting a shift toward a more mature RaaS model with expanded affiliate operations and the potential for increased operational scale.

By mid-2025, the Sinobi Group surfaced and rapidly established operational momentum. Sinobi appears to be derived from or heavily influenced by Lynx, as evidenced by near-identical binaries, 99% code similarity with the Lynx ransomware family, shared infrastructure patterns, and similar operational playbooks. However, as Lynx continues to operate under its original name, it remains unclear whether Sinobi is a rebrand or a subgroup spawned from a sale or sharing of the Lynx encryptor or infrastructure. Notably, activity attributed to Lynx has noticeably decreased since the third quarter of 2025, while Sinobi has become more active. While this data suggests that this may be a gradual rebrand, the nearly identical ransomware and infrastructure are contrary to typical threat actor rebrands aimed at evading law enforcement scrutiny.

Meanwhile, INC Ransom continued to evolve, with a recent version of its ransomware developed in the Rust programming language, representing a notable shift from earlier C/C++ based implementations and indicating continued modernization of the INC codebase. Despite significant binary-level divergence, the Rust-compiled variant preserves core behaviors and execution logic.

Sinobi appears to be derived from or heavily influenced by Lynx, as evidenced by near-identical binaries, 99% code similarity with the Lynx ransomware family

	INC RANSOM (C++)	LYNX	SINOBI GROUP
Ransom Notes	Base64-encoded	Base64-encoded	Base64-encoded
Encryption Architecture	Hybrid	Hybrid	Hybrid
Symmetric Algorithm	AES-128	AES-128	AES-128
Asymmetric Algorithm	Curve25519 (ECC)	Curve25519 (ECC)	Curve25519 (ECC)
File Encryption Logic	Same	Same	Same
Encrypted File Meta Data	Same except for ransomware brand	Same except for ransomware brand	Same except for ransomware brand
Ransom Notes Names	INC-README.txt	ReadMe.txt	ReadMe.txt
Data Leak Site Starts With	http://inc	http://lynx	http://sinobi
Threat Actor Chat Site	Same	Same	Same
Command Line Arguments	Partially Same	Updated	Same as Lynx
Desktop Wallpaper Name	background-image.jpg	background-image.jpg	background-image.jpg
Desktop Wallpaper Location	%Temp%	%Temp%	%Temp%
Send Ransom Notes to OneNote	Yes	Yes	Yes

Figure 1 | Table showing similarities between the three ransomware families (Source: Arete)

Base64-Encoded Ransom Notes

The three ransomware samples were not packed, and most of the supporting strings are present in cleartext text format. However, the ransom notes are Base64-encoded within the ransomware binary, as shown below.

INC

```
.rdata:004215A0 aFn5FibjtkmgumF db 'fn5+fiBJTkMgUmFuc29tIH5+fn4NCg0KLS0tLS0+IFlvdXIgZGF0YSBpcyBzdG9sZ'
.rdata:004215A0                                         ; DATA XREF: sub_406830+19↑o
.rdata:004215A0                                         ; sub_406830+36↑o ...
.rdata:004215A0                 db 'W4gYWSkIGVuY3J5cHRlZC4NCklmIHlvdSBkb24ndCBwYXkgdGhlIHJhbnNvbSwgdG'
.rdata:004215A0                 db 'hlIGRhdGEgd2lsbCBiZSBwdWJsaXNoZWQgb24gb3VyIFRPUiBkYXJrbmV0IHNpdGV'
.rdata:004215A0                 db 'zLg0KVGhlIHNvb25lciB5b3UgcGF5IHRoZSByYW5zb20sIHRoZSBzb29uZXIgeW91'
.rdata:004215A0                 db 'ciBjb21wYW55IHdpbGwgYmUgc2FmZS4NCg0KVG9yIEJyb3dzZXIgTGluazoNCglod'
.rdata:004215A0                 db 'HRwOi8vaW5jYmxvZzZxdTR5NG1tNHp2dzVucm11ZTZxYnd0Z2pzeHB3NmI3aXh6c3'
.rdata:004215A0                 db 'N1MzZ0c2FqbGRvYWQub25pb24vDQoJaHR0cDovL2luY2Jsb2c3dm11cTdya3RpYzc'
.rdata:004215A0                 db 'zcjRoYTRqNzU3bTNwdHltMzd0eXZpZnpwMnJvZWR5eXp6eGlkLm9uaW9uLw0KDQpM'
.rdata:004215A0                 db 'aW5rIGZvciBub3JtYWwgYnJvd3NlcjoNCglodHRwOi8vaW5jYXB0LnN1Lw0KCQ0KL'
.rdata:004215A0                 db 'S0tLS0+IFdoYXQgZ3VhcmFudGVlcyBhcmUgdGhhdCB3ZSB3b24ndCBmb29sIHlvdT'
.rdata:004215A0                 db '8NCldlIGFyZSBub3QgYSBwb2xpdGljYWxseS8tb3RpdmF0ZWQgZ3JvdXAgYW5kIHd'
```

Lynx

```
.rdata:000000014002CDB0 aR29vzcbhznrlcm db 'R29vZCBhZnRlcm5vb24sIHdlIGFyZSBMeWS4IEdyb3VwLg0KDQpBcyB5b3UgY2FuI'
.rdata:000000014002CDB0                                         ; DATA XREF: main:loc_14000901D↑o
.rdata:000000014002CDB0                                         ; main+953↑o ...
.rdata:000000014002CDB0                 db 'HNlZSB5b3UgaGF2ZSBiZWVuIGF0dGFja2VkIGJ5IHVzISBXZS8vZmZlciB5b3UgdG'
.rdata:000000014002CDB0                 db '8gbWFrZSBhIGRlYWwgd2l0aCB1cy4gYWxsIHlvdSBuZWVkIHRvIGRvIGlzIGNvbnR'
.rdata:000000014002CDB0                 db 'hY3QgdXMgYnkgZm9sbG93aW5nIHRoZSBpbnN0cnVjdGlvbnMgYmVsb3cuIA0KV2Ug'
.rdata:000000014002CDB0                 db 'YXJlIG5vdCBwb2xpdGljYWxseSBtb3RpdmF0ZWQgZ3JvdXAsIHdlIGFyZSBpbnRlc'
.rdata:000000014002CDB0                 db 'mVzdGVkIG9ubHkgaW4gbW9uZXksIHdlIGFsd2F5cyBrZWVwIG91ciB3b3JkLiBZb3'
.rdata:000000014002CDB0                 db 'UgaGF2ZSBhIHBvc3NpYmlsaXR5IHRvIGRlY3J5cHQgeW91ciBmaWxlcyBhbmQgc2F'
.rdata:000000014002CDB0                 db '2ZSB5b3VyIHJlcHV0YXRpb24gaW4gY2FzZSB3ZSBmaW5kIGdvb2Qgc29sdXRpb24h'
.rdata:000000014002CDB0                 db 'IA0KWW91IGhhdmUgdG8ga25vdyB3ZSBkbyBub3QgbGlrZSBwcm9jcmFzdGluYXRpb'
.rdata:000000014002CDB0                 db '24uIFlvdSBoYXZlIDcgZGF5cyB0byBjb211IHRvIHRoZSBjaGF0IHJvb20gYWSkIH'
```

Sinobi

```
.rdata:000000014002CDB0 aR29vzcbhznrlcm db 'R29vZCBhZnRlcm5vb24sIHdlIGFyZSBTaW5vYmkgR3JvdXAuDQoNCkFzIHlvdSBjY'
.rdata:000000014002CDB0                                         ; DATA XREF: main:loc_14000901D↑o
.rdata:000000014002CDB0                                         ; main+953↑o ...
.rdata:000000014002CDB0                 db 'W4gc2VlIHlvdSBoYXZlIGJlZW4gYXR0YWNrZWQgYnkgdXMhIFdlIG9mZmVyIHlvdS'
.rdata:000000014002CDB0                 db 'B0byBtYWtlIGEgZGVhbCB3aXRoIHVzLiBhbGwgeW91IG5lZWQgdG8gZG8gaXMgY29'
.rdata:000000014002CDB0                 db 'udGFjdCB1cyBieSBmb2xsb3dpbmcgdGhlIGluc3RydWN0aW9ucyBiZWxvdy4gDQpX'
.rdata:000000014002CDB0                 db 'ZSBhcmUgbm90IHBvbGl0aWNhbGxSIG1vdGl2YXRlZCBncm91cCwgd2UgYXJlIGlud'
.rdata:000000014002CDB0                 db 'GVyZXN0ZWQgb25seSBpbiBtb25leSwgd2UgYWx3YXlzIGtlZXAgb3VyIHdvcmQuIF'
.rdata:000000014002CDB0                 db 'lvdSBoYXZlIGEgcG9zc2liaWxpdHkgdG8gZGVjcnlwdCB5b3VyIGZpbGVzIGFuZCB'
.rdata:000000014002CDB0                 db 'zYXZlIHlvdXIgcmVwdXRhdGlvbiBpbiBjYXNlIHdlIGZpbmQgZ29vZCBzb2x1dGlv'
.rdata:000000014002CDB0                 db 'biEgDQpZb3UgaGF2ZSB0byBrbm93IHdlIGRvIG5vdCBsaWtlIHByb2NyYXN0aW5hd'
.rdata:000000014002CDB0                 db 'Glvbi4gWW91IGhhdmUgNyBkYXlzIHRvIGNvbWUgdG8gdGhlIGNoYXQgcm9vbS8hbm'
```

Figure 2 | INC, Lynx, and Sinobi ransomware binaries (Source: Arete)

Threat Actor DLS and Chat Sites

Analysis of the threat actor DLS and chat sites associated with INC, Lynx, and Sinobi shows that all three are built using the same source code, including identical application structure, interface components, routing behavior, and operational logic.

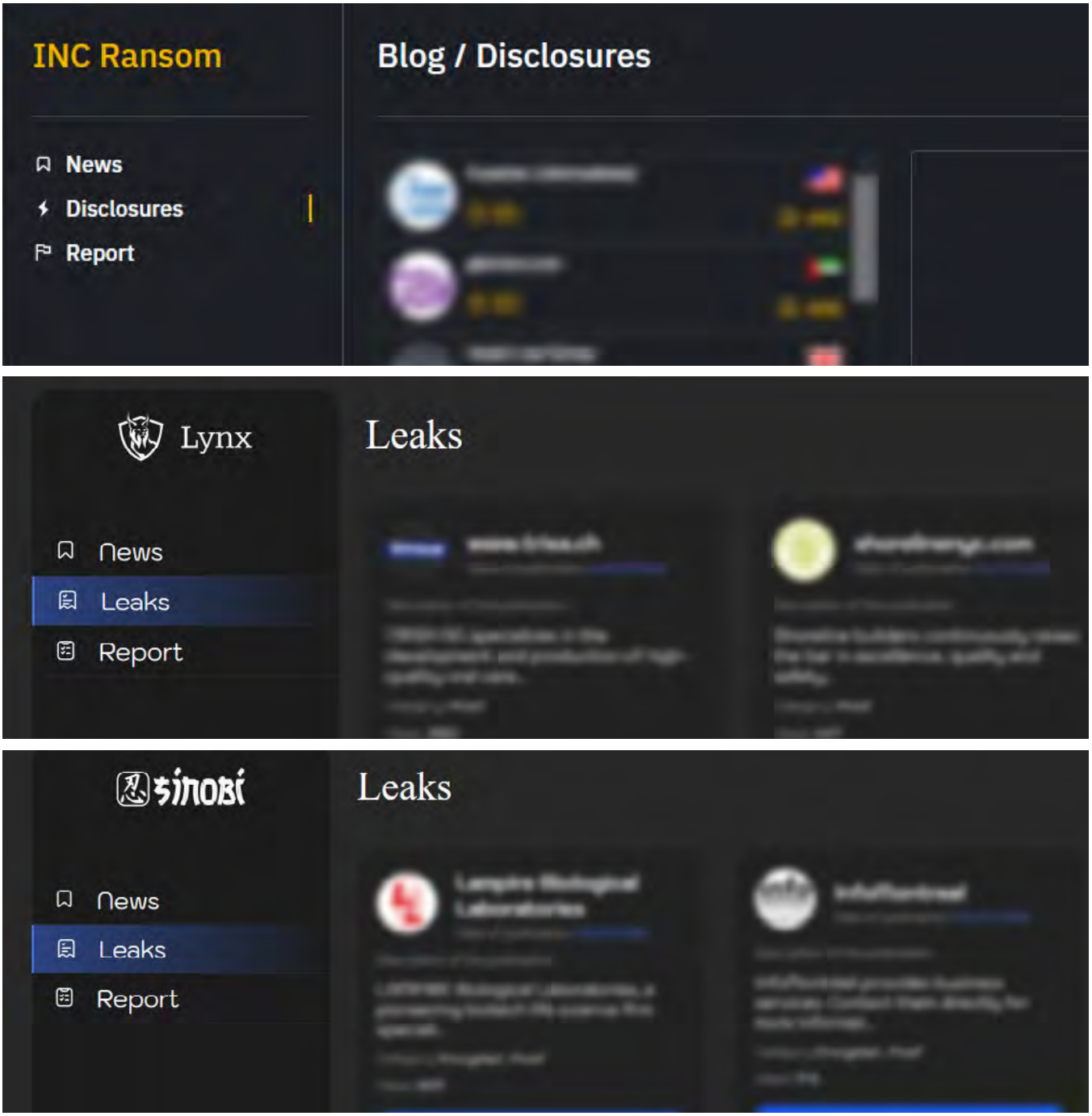


Figure 3 | INC, Lynx, and Sinobi data leak sites (Source: Arete)

Threat Actor Chat Site Source Code Pattern

All three sites use the same type of source code, including the same main JavaScript file and a similar file-name structure, demonstrating that they were created in the same way and operate using the same core program.

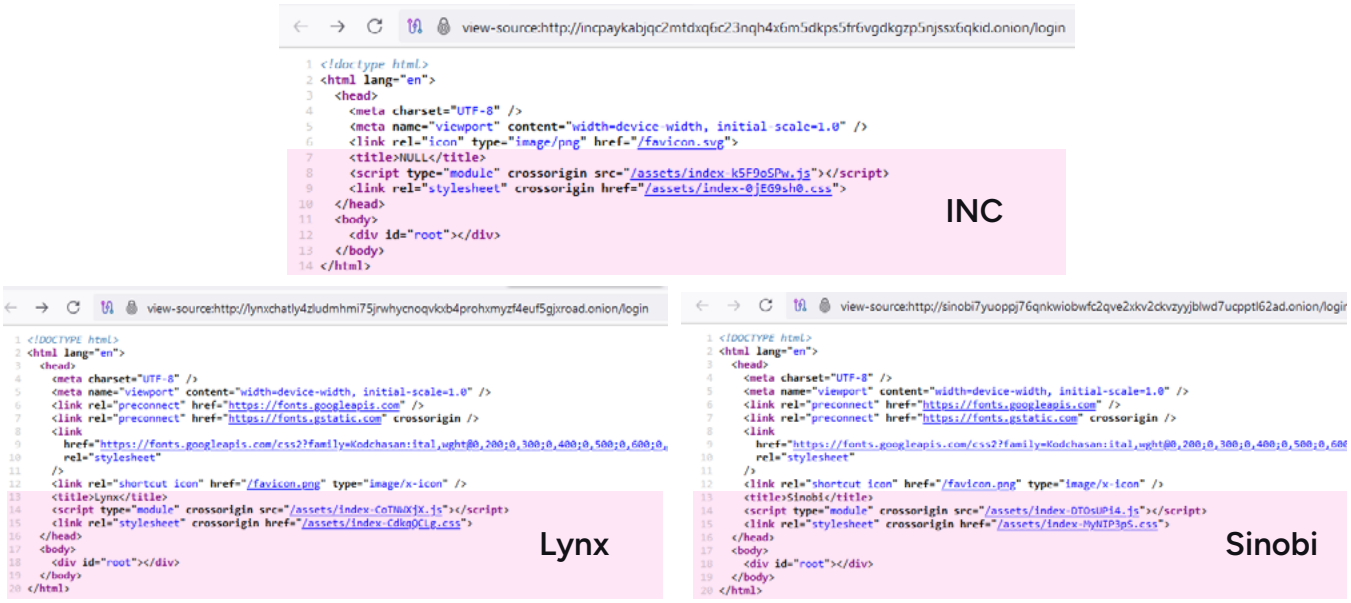


Figure 4 | INC, Lynx, and Sinobi chat site source code (Source: Arete)

File Encryption Logic

Analysis of the file-encryption routines used by INC, Lynx, and Sinobi shows that all three rely on the same underlying logic, following an identical sequence of operations and control flow.

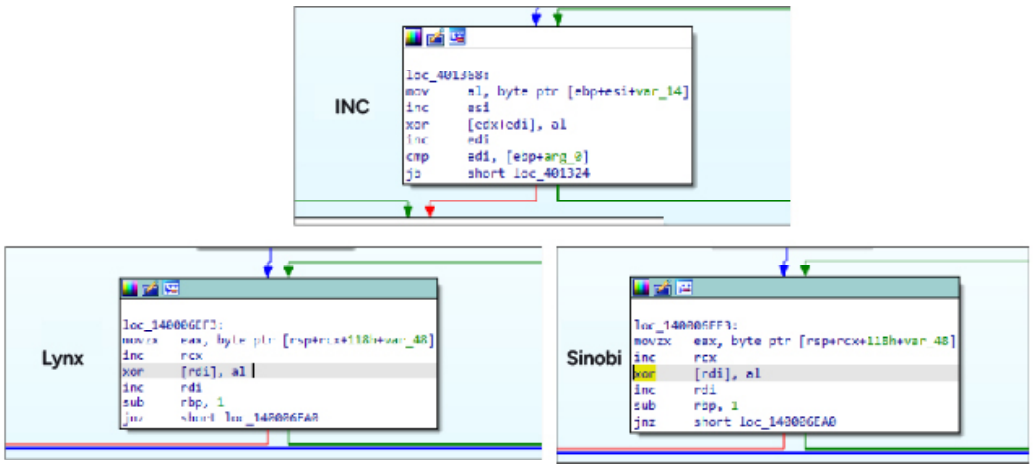


Figure 5 | INC, Lynx, and Sinobi file encryption routines (Source: Arete)

Encrypted File Metadata

Encrypted file metadata from INC, Lynx, and Sinobi ransomware samples demonstrates that all three use the same underlying metadata structure, with identical byte patterns and layout across variants.

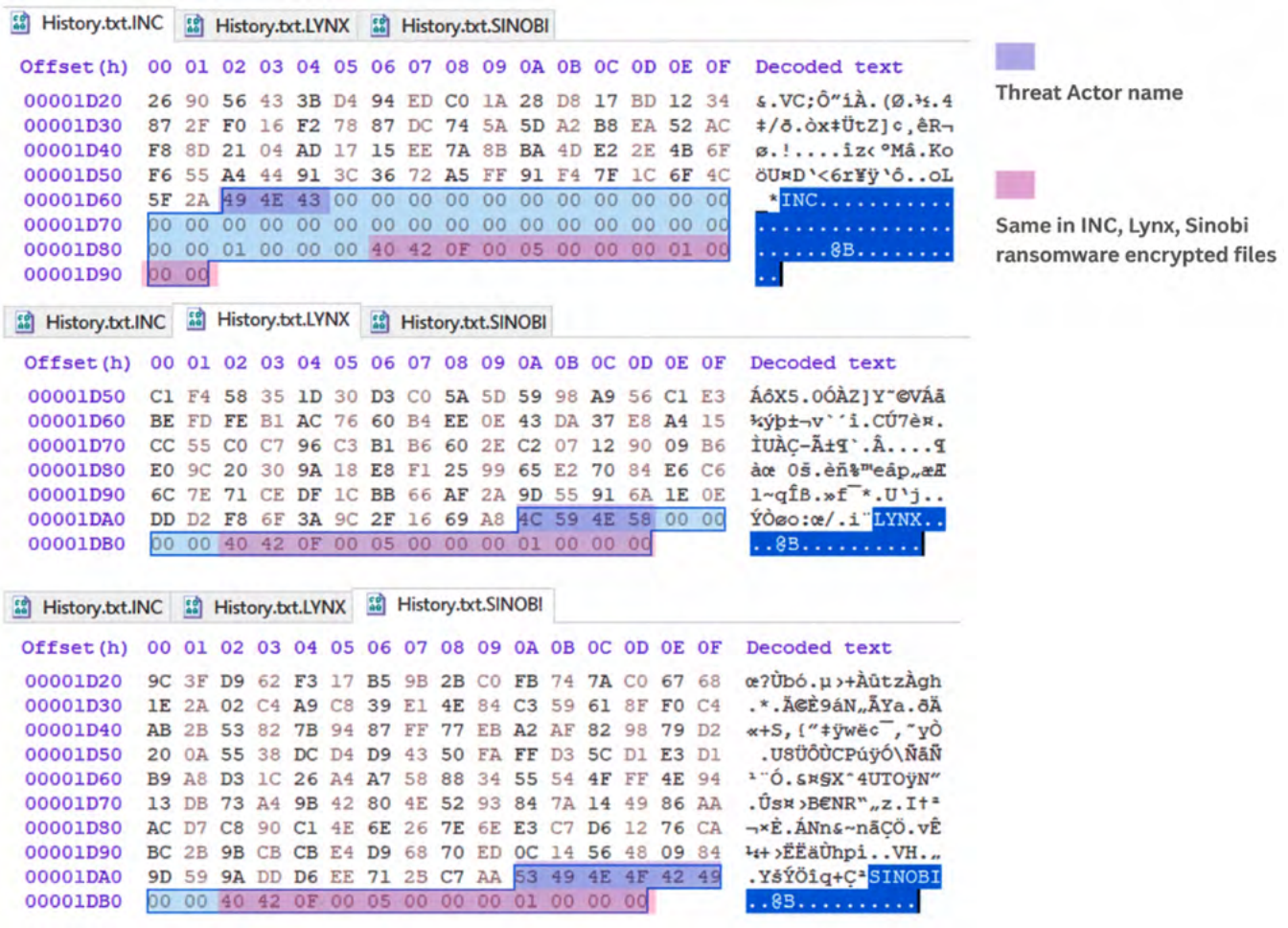


Figure 6 | INC, Lynx, and Sinobi encrypted file metadata (Source: Arete)

Command Line Arguments

The INC, Lynx, and Sinobi ransomware families support an almost identical set of operational arguments.

INC (C++)	LYNX	SINOBI
--file <FILE>	--file <filePath>	--file <filePath>
--dir <DIRECTORY>	--dir <dirPath>	--dir <dirPath>
--mode <MODE>	--mode <mode>	--mode <mode>
--ens	--encrypt-network	--encrypt-network
--lhd	--load-drives	--load-drives
--sup		
--hide	--hide-cmd	--hide-cmd
--kill	--kill	--kill
--debug		
--help	--help	--help
	--verbose	--verbose
	--silent	--silent
	--stop-processes	--stop-processes
	--no-background	--no-background
	--no-print	--no-print
	--safe-mode	--safe-mode

Figure 7 | INC, Lynx, and Sinobi command line arguments (Source: Arete)

In the first quarter of 2026, Arete continues to observe activity from Lynx, and Sinobi and INC are likely to remain persistent threats this year. The overlaps between these three groups illustrate the unique operational model in which threat actors can leverage shared code and infrastructure while maintaining separate ransomware brand identities.

INC

```
C:\Users\Akxy>C:\Users\Akxy\Desktop\INC.exe --help
USAGE:
        C:\Users\Akxy\Desktop\INC.exe [ARGUMENTS]

ARGUMENTS:
        --file <FILE>           Encrypt only selected file
        --dir <DIRECTORY>       Encrypt only selected directory
        --mode <MODE>           Choose mode for file encryption (fast, medium, slow)
        --ens                   Encrypt network shares
        --lhd                   Load hidden drives
        --sup                   Stop using process
        --hide                  Hide console window
        --kill                  Kill processes/services by mask
        --debug                 Enable debug mode
        --help                  Display this message
```

Lynx

```
C:\Users\Akxy>C:\Users\Akxy\Desktop\Lynx.exe --help
Usage: C:\Users\Akxy\Desktop\Lynx.exe <ARGUMENTS>
Arguments:
        --file <filePath>                               Encrypt only specified file(s)
               --file C:\temp.txt
               --file C:\temp.txt,D:\temp2.txt
        --dir <dirPath>                                 Encrypt only specified directory(ies)
               --dir C:\
               --dir C:\,D:\
        --mode <mode>                                   Encryption mode
               --mode fast                              Encrypt 5% from entire file
               --mode medium                            Encrypt 15% from entire file (default)
               --mode slow                              Encrypt 25% from entire file
               --mode entire                            Encrypt 100% from entire file
        --help                                          Print this message
        --verbose                                       Enable verbosity
        --silent                                        Enable silent encryption (no extension and notes will be added)
        --stop-processes                                Try to stop processes via RestartManager
        --encrypt-network                               Encrypt network shares
        --load-drives                                   Load hidden drives (will corrupt boot loader)
        --hide-cmd                                      Hide console window
        --no-background                                 Don't change background image
        --no-print                                      Don't print note on printers
        --kill                                          Kill processes/services
        --safe-mode                                     Enter safe-mode
```

Sinobi

```
C:\Users\Akxy>C:\Users\Akxy\Desktop\Sinobi.exe --help
Usage: C:\Users\Akxy\Desktop\Sinobi.exe <ARGUMENTS>
Arguments:
        --file <filePath>                               Encrypt only specified file(s)
               --file C:\temp.txt
               --file C:\temp.txt,D:\temp2.txt
        --dir <dirPath>                                 Encrypt only specified directory(ies)
               --dir C:\
               --dir C:\,D:\
        --mode <mode>                                   Encryption mode
               --mode fast                              Encrypt 5% from entire file
               --mode medium                            Encrypt 15% from entire file (default)
               --mode slow                              Encrypt 25% from entire file
               --mode entire                            Encrypt 100% from entire file
        --help                                          Print this message
        --verbose                                       Enable verbosity
        --silent                                        Enable silent encryption (no extension and notes will be added)
        --stop-processes                                Try to stop processes via RestartManager
        --encrypt-network                               Encrypt network shares
        --load-drives                                   Load hidden drives (will corrupt boot loader)
        --hide-cmd                                      Hide console window
        --no-background                                 Don't change background image
        --no-print                                      Don't print note on printers
        --kill                                          Kill processes/services
        --safe-mode                                     Enter safe-mode
```

Figure 8 | INC, Lynx, and Sinobi command line arguments (Source: Arete)

Extortion-Only Groups in 2025

Although established ransomware groups like Akira, Qilin, and Play largely dominated the threat landscape, a continued shift towards cyber extortion, rather than data encryption, became even more prevalent throughout 2025. Major incidents involving organizations like PowerSchool, Salesloft, and Snowflake showed that extortion-only attacks can threaten not only the organizations that host the data but also the original data owners, creating the potential for additional extortion attempts. Even with traditional ransomware groups, Arete has observed that demands for proof of data deletion are at times higher than the original decryption demands.

In parallel, extortion groups in 2025 took the place of more traditional "big game hunters" of previous years. Extortion-only threat groups have the unique ability to carefully and quietly exfiltrate large amounts of data prior to extorting the victim. These extortion scenarios can exceed 1 TB of data exfiltrated from large organizations and create unique concerns about the victim organizations' reputations.

Notable Extortion Groups in 2025

World Leaks

In late 2024, the Hunters International ransomware group publicly announced its intent to cease operations and rebrand as World Leaks, citing increased risk and pressure from international law enforcement. With this rebrand, affiliates were reportedly equipped with a custom-built exfiltration tool to automate data theft from victim networks. Arete first observed incidents from the new World Leaks extortion group in April 2025, and the group became the tenth-most active threat group observed by Arete throughout the year.

Everest

Everest could be considered a jack-of-all-trades, with the group deploying encryptors, brokering initial access, and, most recently, focusing on extortion-only operations. Since largely pivoting away from encryption-based attacks, the group has extorted several high-profile victims, including Under Armour in 2025, and in 2026, has already claimed to have exfiltrated 1.4 TB of data from the information management service company Iron Mountain.

Scattered Lapsus$ Hunters

Last but certainly not least is Scattered Lapsus$ Hunters, a collective formed in late 2025 from members of Scattered Spider, Lapsus$, and ShinyHunters. Although each threat group individually specialized in different aspects of cybercrime, together they combined their strengths to power this new operation:

Scattered Spider: English-speaking group with the ability to conduct sophisticated social engineering attacks for initial access.

LAPSUS$: Specializes in insider threat recruitment and source code theft.

ShinyHunters: Specialties related to large-scale data exfiltration and extortion.

Operating together, the groups successfully launched a campaign against Salesforce and its customers. The group targeted Salesloft and AI drift components to capture information, allowing them to create additional extortion opportunities throughout the rest of 2025, even launching an "extortionware" portal to threaten Salesforce and other organizations impacted by their extortion activities. While the success of their campaigns appears mixed, it highlights the downstream impacts of successful credential theft on critical systems.

This ongoing shift towards extortion highlights that threat actors are increasingly willing to play the long game, compromising SaaS platforms, identity systems, and supplier ecosystems to quietly accumulate data and credentials. This positions these groups to execute prolonged, multi-victim extortion campaigns that extend far beyond the initial breach and will likely become more common in the threat landscape moving forward.

Scattered Spider Remains in the Headlines

In 2025, Scattered Spider remained a highly adaptive, access-focused threat cluster that prioritizes social engineering over malware development or vulnerability exploitation. Scattered Spider is a global collective made up primarily of US- and UK-based individuals who are part of a subculture called "The Com," which consists of loose clusters tied together through communication. This native English fluency enables the group to excel at social engineering operations, and they are also adept at abusing legitimate functionality in cloud resources. Despite the arrests of several of its members in 2024 and 2025, the Scattered Spider collective remained an active threat in 2025 and was responsible for multiple high-profile cyberattacks during the year.

In the first half of 2025, the group gained media visibility by attacking well-known retail organizations in the UK, including Marks & Spencer, Co-op, and Harrods, as well as US insurance and aviation companies such as Aflac, Qantas, and Hawaiian Airlines. After forming the Scattered Lapsus$ Hunters in the second half of the year, the group claimed responsibility for attacks against Jaguar Land Rover and the massive campaign against Salesforce users.

Disappearing Act: Several Groups Depart the Threat Landscape in 2025

Although many established threat groups remained active in 2025, Arete also observed several previously prominent groups cease activities.

Black Basta

Black Basta made headlines in May 2024 for its attack on Ascension Healthcare, one of the largest private healthcare systems in the US. The group was relatively active in the last quarter of 2024 but ceased activity in 2025, and its DLS went down permanently in January 2025. In early February, a Telegram user leaked 200,000 chat logs from Black Basta, spanning from September 2023 to September 2024. These logs revealed extensive details about the inner workings of the organization, and the release likely led to the group going dark. Despite this departure, in the first quarter of 2025, the Cactus threat group was observed using malware and social engineering tactics similar to those used by Black Basta in late 2024, suggesting that some affiliates likely migrated to other groups.

Bian Lian

BianLian was one of the top threat groups observed in February 2025, before ceasing activity for the remainder of the year. The group posted its last victims to its DLS in late March, with the DLS eventually going completely dark. There has been no reporting to indicate why the group suddenly ceased operations.

RansomHub

RansomHub was one of the top threat groups in 2024 and had the second-highest activity of all ransomware and extortion groups in the first quarter of 2025, behind only Akira. However, in early April, RansomHub's infrastructure abruptly went offline, and the group did not reemerge in the threat landscape for the remainder of 2025. Reports indicated that some ex-affiliates may have migrated to the Qilin RaaS, which experienced an uptick in activity starting in Q2 and lasting throughout 2025.

Arete observed several previously prominent groups cease activities.

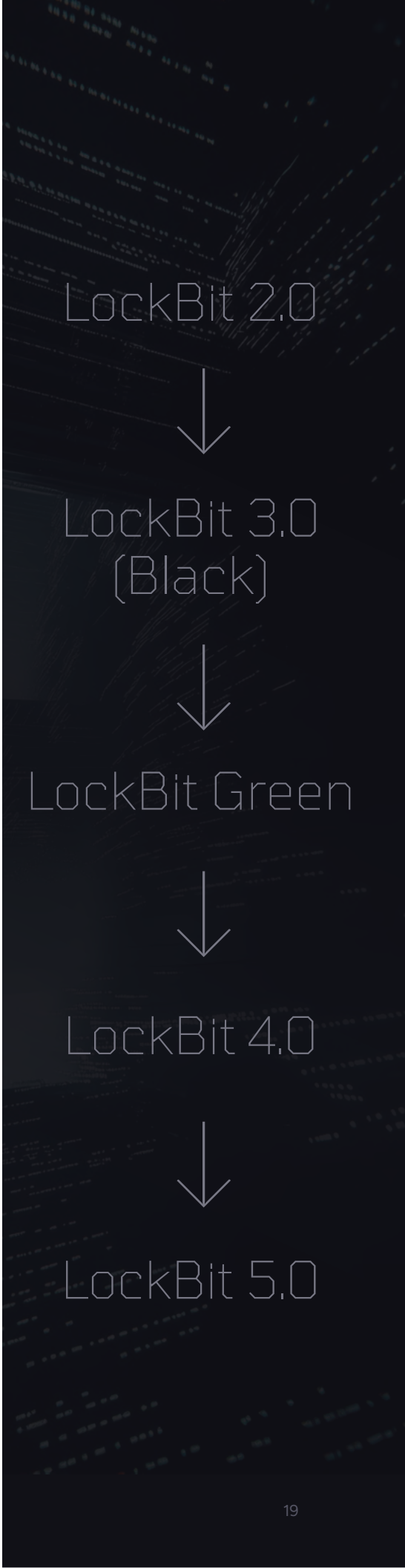
LockBit 5.0:
Back from the Dead?

In late 2025, the once-prolific LockBit group reemerged in what appears to be an effort to reestablish itself in the threat landscape. LockBit "5.0" was first announced on the RAMP dark web forum in early September 2025, and in early December, the group posted an announcement on its old DLS with a link to the new LockBit 5.0 DLS.

This isn't the first time LockBit has tried to resuscitate its RaaS since international law enforcement disrupted the group's infrastructure in early 2024. In December 2024, LockBit announced the release of LockBit 4.0, with the new version becoming available to affiliates in February 2025. However, 4.0 did not appear to gain much traction, and Arete did not observe any incidents involving LockBit in 2025.

The latest LockBit 5.0 variant has numerous code overlaps with LockBit 4.0, with notable improvements, including anti-analysis features and unique 16-character extensions added to each encrypted file. Ransom notes for the 5.0 version direct victims to Tor chat panels, similar to those the group used prior to law enforcement disruptions.

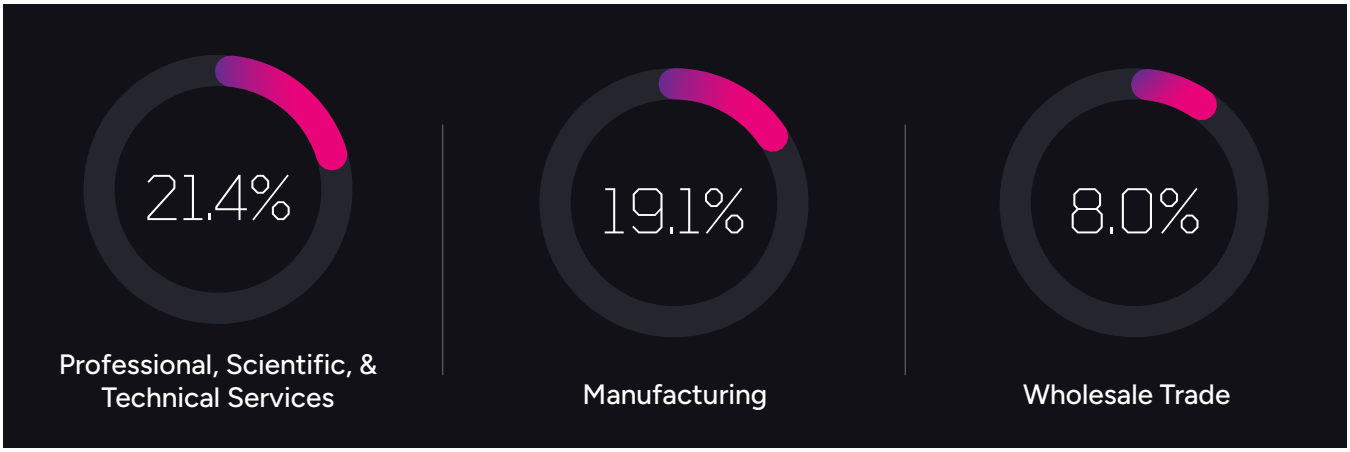
Although Arete has already observed several incidents in 2026 with the new LockBit 5.0 variant, it remains to be seen whether LockBit will return to consistent activity levels. With the group continuing to operate under the LockBit brand, the sanctions against Dmitry Khoroshev, the developer and administrator of the LockBit RaaS who went by the alias LockBitSupp, should inhibit victims contemplating payment for LockBit 5.0 decryption keys, creating a substantial barrier to the group reclaiming its place as one of the top RaaS organizations. If the group becomes an increasingly active threat in 2026, the OFAC sanctions implications make it exceedingly important for organizations to have adequate data protection and security practices in place to be able to recover from potential encryption and extortion attacks without payment.



Sector Impacts and Threat Actor Targeting

Trends in impacted sectors throughout 2025 were similar to what Arete observed in 2024. Professional, Scientific, and Technical Services and Manufacturing remained the top two most impacted sectors, with each accounting for about 20% of all engagements, similar to their respective percentages in 2024. The other top five most impacted industries also remained the same, with the exception of Wholesale Trade surpassing the Finance and Insurance sector. This shift was likely due to the abnormally high volume of Akira engagements in 2025, as opposed to threat groups actively targeting Wholesale Trade organizations.

MOST IMPACTED SECTORS



As was the case in 2024, threat actors in 2025 remained opportunistic, with very few groups targeting a specific industry. Akira, for example, whose activity far surpassed that of the other threat groups throughout the year, had victims in 18 of the 20 sectors impacted and largely targeted software vulnerabilities. The exception to this was the Luna Moth extortion group, which continued to target law firms in the Professional, Scientific, and Technical Services sector. Almost 90% of the group's attacks were against organizations in this industry. However, this had a negligible impact on the overall statistics for the year, as two-thirds of Luna Moth's activity was in the first quarter, and the group was relatively quiet for the remainder of 2025.

NAICS SECTOR NAME	PERCENTAGE OF ENGAGEMENTS
Professional, Scientific, & Technical Services	21.4%
Manufacturing	19.1%
Wholesale Trade	8.0%
Construction	7.7%
Healthcare & Social Assistance	7.5%
Administrative & Support & Waste Management & Remediation Services	5.6%
Finance & Insurance	4.9%
Information	4.0%
Retail Trade	3.7%
Transportation & Warehousing	3.7%
Public Administration	2.8%
Real Estate & Rental & Leasing	2.6%
Other Services (except Public Administration)	2.4%
Educational Services	2.3%
Accommodation & Food Services	1.0%
Management of Companies & Enterprises	1.0%
Agriculture, Forestry, Fishing & Hunting	0.7%
Arts, Entertainment, & Recreation	0.7%
Mining, Quarrying, & Oil & Gas Extraction	0.5%
Utilities	0.5%

Figure 9 | Most impacted NAICS sectors in 2025 (Source: Arete)

** The North American Industry Classification System (NAICS) is the standard used by Federal agencies to classify US business organizations. The Cybersecurity and Infrastructure Security Agency (CISA) has their own separate classifications of critical infrastructure sectors.*

Trends in Ransom Demands and Payments

Ransom demands and payments remained largely comparable to those observed by Arete in recent years. Although the median ransom demand increased by $100,000 in 2025 compared with the past two years, the median ransom payment only increased slightly. The percentage of time a victim is able to recover without paying a ransom also remained about the same over the past three years, with payments made in only a little over 31% of all ransomware and extortion incidents in 2025.

Again, Akira's uncharacteristically high attack volume influenced this data in 2025 more so than any other threat group. Although Akira received ransom payments less often than the rest of the threat groups combined, their median ransom demand was substantially higher at $750,000, and subsequently, the median payments for Akira were also higher at a little over $200,000, which could contribute to the higher overall median amounts compared to the previous two years.

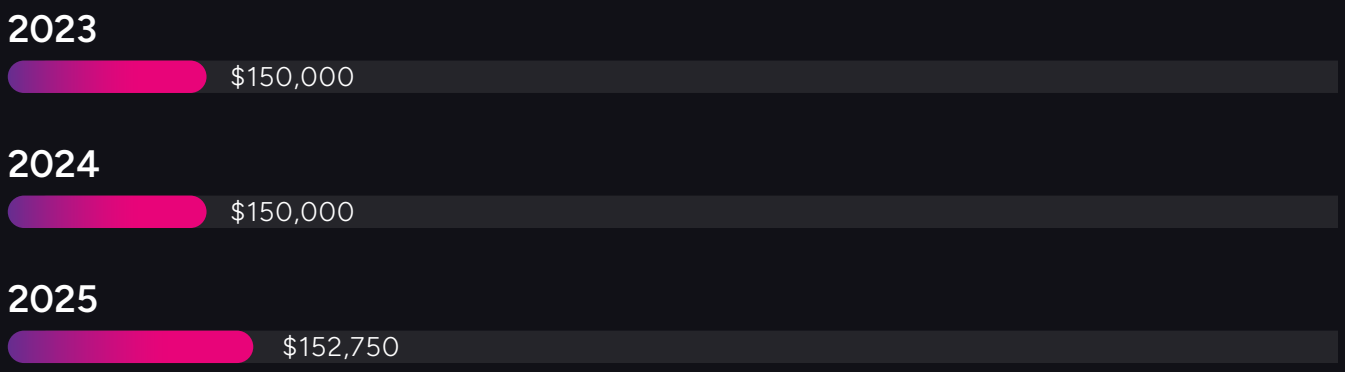
SECTORS	PERCENTAGE OF TIME A RANSOM IS PAID	MEDIAN DEMAND
Professional, Scientific, & Technical Services	37.4%	$542,200
Wholesale Trade	28.3%	$590,000
Construction	27.3%	$740,500
Manufacturing	25.5%	$696,500
Healthcare & Social Assistance	18.6%	$500,000

Figure 10 | Ransom demands and payment percentages for top 5 sectors in 2025 (Source: Arete)

Looking at ransom demands for the most impacted sectors, median demands remained within a consistent range of $500,000 to a little over $740,000 in 2025; again, slightly higher than the $400,000 to $742,000 range observed in 2024. Professional, Scientific, and Technical Services remained the sector most likely to make a ransom payment, a trend that has stayed consistent over the past year. This likely reflects a greater willingness to pay for the suppression of sensitive stolen data. Conversely, Healthcare and Social Assistance was the most resilient of the most impacted sectors in 2025, making ransom payments significantly less often than the other sectors.

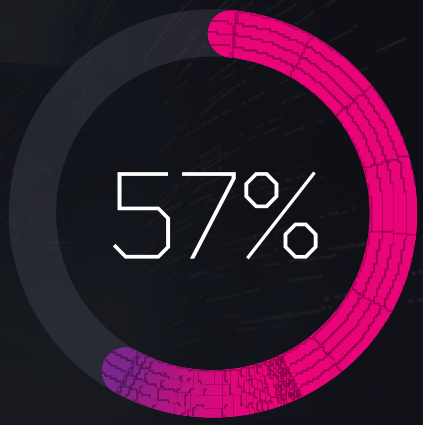
MEDIAN RANSOM DEMAND

MEDIAN RANSOM PAYMENT

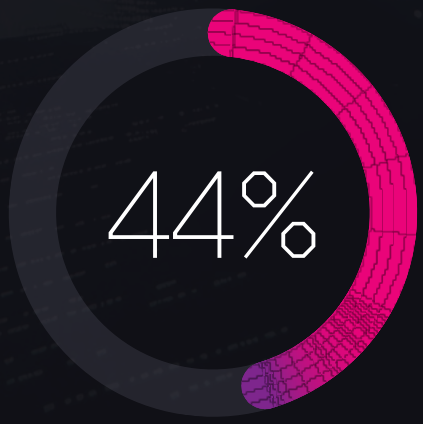


PERCENTAGE OF TIME A RANSOM IS PAID

Play



Qilin



Akira

DLS Stats:

How Often Victims Get Posted?

Almost all the top threat actors that Arete observed in 2025 operate a DLS that they use as an additional pressure tactic to get victims to pay ransoms. However, whether data is actually posted to these sites varies among threat actors, with some groups posting much more frequently than others.

Of the top three most active threat groups in 2025, Play was the most aggressive in posting victims to its DLS. Throughout the year, Play posted victims to its DLS in 90% of engagements with no ransom payment, oftentimes posting the victim while actively negotiating a ransom. Qilin, on the other hand, posted victims around 57% of the time in Arete engagements with no payment.

Most surprising was Akira. Akira's DLS has a "News" section, where the group initially posts victim names and descriptions, and a "Leaks" section, where they eventually leak data from victim organizations. However, among the Akira engagements with no ransom payment in 2025, only 44% of victims were actually posted to the DLS, and victim data was leaked just 16% of the time. One factor contributing to this lower percentage is that Akira doesn't exfiltrate data for every victim, and the percentage of victims posted to the "News" section is consistent with how often Arete observes data exfiltration in Akira engagements. Additionally, in the second half of the year, Arete observed a noticeable lag between the end of communications and the posting of a victim, coinciding with the surge in Akira incidents. This sudden spike in attacks likely overwhelmed Akira's infrastructure and capabilities, potentially contributing to the low percentage of actual data leaks.

Initial Access Trends and Vulnerabilities Exploited

Throughout 2025, vulnerability exploits, compromised credentials, and social engineering attacks were the top attack vectors observed by Arete. Vulnerabilities in perimeter devices enabled groups like Akira and Qilin to sustain high attack volumes across multiple industries throughout the year.

Top Vulnerabilities Exploited in 2025

SonicWall (SonicOS / SSL VPN)

In 2025, ransomware and extortion groups increasingly centered their operations around the exploitation of CVE-2024-40766, a critical SonicWall SSL VPN access control vulnerability that emerged as one of the most prominent initial access vectors observed during the year. Beyond CVE-2024-40766, threat actors also exploited a broader set of SonicWall vulnerabilities, including CVE-2024-53704, CVE-2025-32818, CVE-2025-40600, CVE-2025-40601, and related SonicOS flaws. Collectively, these vulnerabilities enabled attackers to bypass authentication, manipulate VPN access controls, or abuse memory handling weaknesses to establish unauthorized VPN sessions on internet-exposed SonicWall appliances, particularly in environments lacking multi-factor authentication (MFA) or timely patching.

Akira emerged as the most active and operationally successful ransomware group abusing SonicWall SSL VPN vulnerabilities, and this exploitation was a cornerstone of Akira's late-2024 and 2025 campaigns, with this activity continuing to be observed in 2026. The group systematically scanned for vulnerable SonicWall deployments and leveraged these flaws to gain unauthenticated or improperly authorized access. Intelligence also indicated extended dwell times, with Akira revisiting environments compromised months earlier through SonicWall exploitation and retroactively adding victims to its data leak site. This behavior underscores how initial access obtained via perimeter devices was often retained and monetized well after the initial intrusion.

Other ransomware groups, including Qilin, INC, and WhiteRabbit, adopted similar exploitation techniques throughout 2025, reinforcing SonicWall VPN vulnerabilities as a broadly weaponized entry point across the ransomware ecosystem. The repeated exploitation of these vulnerabilities by multiple groups highlights the scalability and reliability of SonicWall SSL VPNs as an initial access mechanism.

Fortinet (FortiGate, FortiManager, FortiWeb, SSL VPN)

Fortinet exploitation typically begins with SSL VPN or management interface abuse, especially on devices without MFA. Vulnerabilities such as CVE-2024-55591 (FortiManager) and CVE-2025-24472 (FortiOS / FortiProxy) enable authentication bypass or privilege escalation to super-admin through crafted requests, while CVE-2025-64446 (FortiWeb) allows unauthenticated attackers to create new administrative users via path confusion flaws. Qilin has been the most consistent and frequently observed ransomware group exploiting Fortinet vulnerabilities, using these flaws as a primary initial access vector across multiple campaigns. Qilin's operations commonly combine Fortinet SSL VPN access with exposed services such as File Transfer Protocol (FTP) to deploy web shells and establish persistence, a pattern later adopted by other groups, including Play, INC, and WhiteRabbit. Once administrative access is established, threat actors enable persistent VPN access, dump configuration files containing credentials, and move laterally into Windows environments before staging ransomware payloads, exfiltrating data, and disabling backups prior to encryption.

Oracle E-Business Suite

A critical Oracle E-Business Suite zero-day vulnerability (CVE-2025-61882) was actively exploited by the Cl0p ransomware group and affiliated actors to gain unauthenticated remote code execution within enterprise environments in October 2025. The vulnerability, located in the Oracle Concurrent Processing component, enabled attackers to breach systems without valid credentials and conduct large-scale data theft operations prior to extortion, consistent with Cl0p's established non-encryption extortion model. The exploitation of CVE-2025-61882 aligns with Cl0p's long-standing operational pattern of targeting high-value enterprise platforms through zero-day vulnerabilities, following similar campaigns such as the Accellion file transfer application in 2020, SolarWinds in 2021, GoAnywhere managed file transfer in 2023, and MOVEit Transfer also in 2023.

In parallel, a separate Oracle E-Business Suite Server-Side Request Forgery (SSRF) vulnerability (CVE-2025-61884) was publicly disclosed by the Scattered Lapsus$ Hunters via a Telegram channel, further highlighting systemic exposure within Oracle E-Business Suite deployments.

SimpleHelp

Ransomware groups exploited SimpleHelp remote management vulnerabilities in the first half of 2025, most notably CVE-2024-57727 and CVE-2024-57728, which affect SimpleHelp versions 5.5.7 and earlier. These vulnerabilities allowed attackers to abuse exposed SimpleHelp services to gain interactive remote access, often without triggering traditional malware-based detections. The use of a legitimate remote management platform provided ransomware operators with a low-noise mechanism for establishing persistence and maintaining control over compromised environments.

The INC ransomware group was observed exploiting CVE-2024-57727 to establish persistent remote sessions, upload tooling, and move laterally within victim networks. Similarly, the Medusa ransomware group targeted both CVE-2024-57727 and CVE-2024-57728, enabling the dumping of credential hashes and modification of configuration files to deepen access. Once embedded, attackers leveraged SimpleHelp's legitimate administrative capabilities to deploy ransomware payloads and disable security controls, reinforcing the trend of ransomware groups abusing remote management software in their attack chains.

The Evolution of Social Engineering

In 2025, ransomware operations increasingly converged around initial access driven by social engineering, with multiple threat groups demonstrating that human manipulation and deceptive software delivery were often more reliable and scalable than exploiting technical vulnerabilities. Rather than relying on zero-days or complex exploits, ransomware operators prioritized impersonation, vishing, phishing, artificial intelligence (AI)-enhanced impersonation techniques, trusted third-party abuse, and deceptive distribution channels to compromise identities, bypass security controls, and enable ransomware and extortion activity. These approaches were particularly prevalent in supply-chain and software trust abuse campaigns, including operations such as TamperedChef, which distributed trojanized freeware that later provided initial access leveraged by ransomware affiliates for follow-on intrusion and extortion.

The Interlock ransomware group exemplified this shift by adopting FileFix, an evolution of the ClickFix technique. Rather than delivering malware directly, Interlock tricked victims into executing malicious commands themselves. Users visiting compromised websites were instructed to paste attacker-provided commands into Windows File Explorer, triggering PowerShell execution that deployed an Interlock RAT. Threat actors subsequently leveraged this access for credential harvesting, data exfiltration, lateral movement, and ransomware encryption, reinforcing a user-assisted execution model designed to evade traditional defenses.

As mentioned previously in this report, Scattered Spider continued to rely heavily on help desk impersonation, MFA fatigue attacks, SIM swapping, and executive pretexting, including the reported use of AI-enhanced voice impersonation techniques. These methods enabled attackers to obtain valid credentials and reset accounts without exploiting software flaws.

In 2025, ransomware relied on social engineering, using AI-driven impersonation, phishing, and vishing to bypass security.

Additionally, an ongoing TamperedChef campaign highlighted the growing risk posed by deceptive software distribution channels. Malware associated with TamperedChef is frequently delivered through search engine optimization (SEO) poisoning or malicious Google Ads purchased by threat actors. This particular campaign distributes ManualFinder, a trojan-like application bundled with seemingly legitimate freeware such as PDF editors and the OneStart browser. Once installed, ManualFinder establishes persistence by running scheduled tasks that execute hidden JavaScript payloads, enabling long-term access. Activity linked to TamperedChef was most commonly observed in intrusions associated with ransomware groups such as Akira, followed by Qilin, INC Ransom, and Play ransomware operations, demonstrating how trojanized freeware increasingly serves as a precursor to ransomware deployment and extortion.

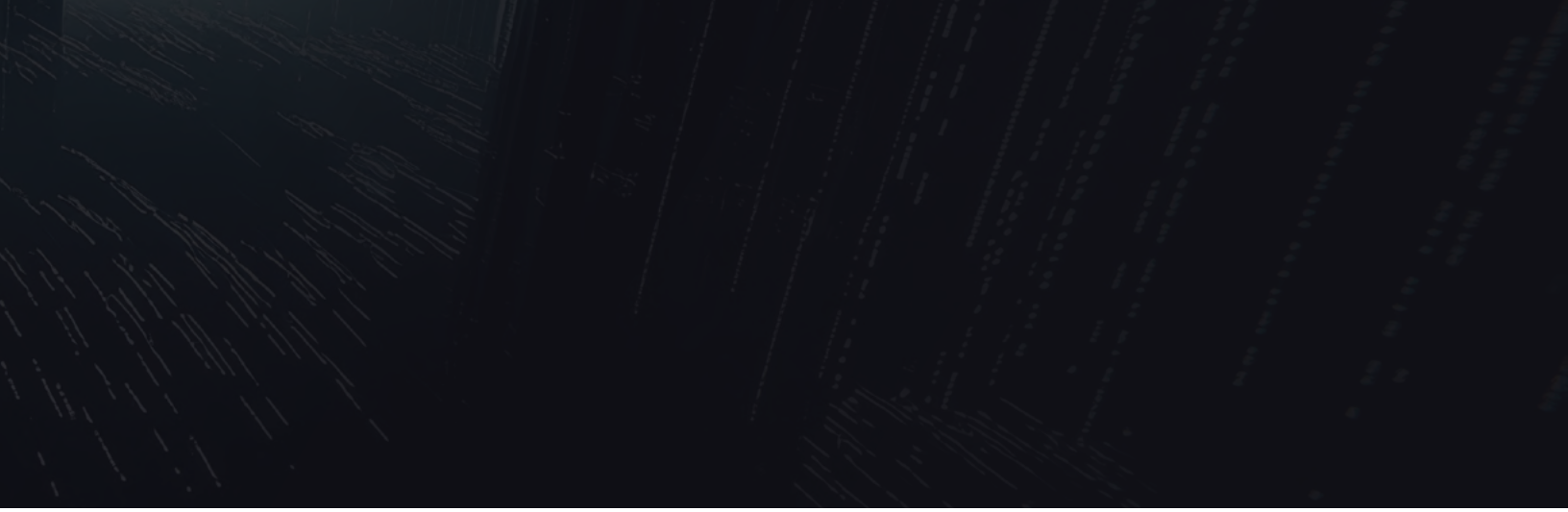
ClickFix Evolution

ClickFix initially emerged in early 2024 as a social-engineering-driven initial access technique rather than a distinct malware family. The earliest variants relied on deceptive web content that instructed victims to manually execute commands copied to their clipboard, typically via PowerShell or system terminals. From a technical perspective, this marked a shift away from exploit-based infection chains toward human-assisted execution, allowing threat actors to bypass traditional endpoint defenses, sandboxing, and exploit mitigations. In its early stages, ClickFix was primarily used to deploy commodity malware such as downloaders, stealers, and remote access trojans, establishing a foothold for subsequent activity rather than immediate monetization.

As the technique matured in 2025, ClickFix became increasingly modular and infrastructure-agnostic, enabling adoption by a wider range of threat actors. Campaigns began leveraging compromised websites, malvertising, and phishing emails to deliver highly contextual lures, including fake CAPTCHA challenges and software update failures. Technically, execution chains evolved to abuse living-off-the-land binaries (LOLBins) such as PowerShell, MSBuild, and command interpreters, with payloads often delivered in memory or dynamically compiled at runtime. This reduced forensic artifacts and made ClickFix particularly attractive to access brokers operating in the ransomware ecosystem.

By mid-2025, ClickFix was increasingly observed as part of ransomware-related intrusion chains, rather than standalone malware delivery. Initial ClickFix execution often led to the deployment of loaders or lightweight RATs, followed by credential harvesting, domain reconnaissance, and lateral movement using legitimate administrative tools. These behaviors aligned closely with pre-ransomware tradecraft, suggesting that ClickFix had become a viable replacement for traditional phishing attachments or exploit kits as an initial access vector. In several investigations, ClickFix-derived access was later monetized through ransomware deployment, either by the original operators or via resale to ransomware affiliates.

During this period, multiple ransomware groups and affiliates were linked to ClickFix-enabled intrusions, either directly or indirectly. Operators associated with the Akira, Qilin, Play, and INC ransomware groups were observed leveraging access obtained through social-engineering-based execution rather than malware-laden documents. This reflects a broader trend in the cyber threat



ecosystem of an increasing reliance on trusted user execution and legitimate tooling to reduce detection during early stages of compromise. ClickFix's low technical barrier and high success rate made it well-suited for this operational model, particularly in environments with strong email and attachment filtering.

In late 2025, ClickFix reached a new level of operational sophistication with the introduction of fake system-level interfaces, including full-screen Windows Update simulations and fake Blue Screen of Death (BSOD) pages. These variants did not exploit operating system vulnerabilities; instead, they used browser controls, JavaScript overlays, and visual fidelity to convincingly simulate critical system failures.

ClickFix has evolved from a simple clipboard-based trick into a strategic initial access technique embedded within the ransomware economy. Its success lies in its ability to externalize risk to the victim, leveraging human trust rather than software flaws, while seamlessly integrating with established ransomware playbooks. As ransomware groups continue to prioritize stealth, speed, and reliability in initial access, ClickFix is likely to remain a persistent and adaptive component of modern ransomware intrusion chains.

In late 2025, ClickFix reached a new level of operational sophistication with the introduction of fake system-level interfaces, including full-screen Windows Update simulations and fake Blue Screen of Death (BSOD) pages.

Most Observed Tools & Malware in Ransomware Operations

Ransomware intrusions in 2025 demonstrated a high degree of tooling convergence, with threat actors relying heavily on legitimate, dual-use, and commodity tools across all phases of the attack lifecycle. Rather than bespoke malware, affiliates prioritized tools that blend into enterprise environments, complicate detection, and enable flexible operations.

- RMM and remote access tools continued to dominate threat actor toolkits in 2025, reinforcing their role as one of the most effective mechanisms for maintaining persistent, hands-on-keyboard access to victim environments. Because these tools are widely used by IT teams and managed service providers, ransomware actors frequently abuse tools already present in the environment or deploy their own versions with minimal detection. Throughout 2025, AnyDesk remained the most commonly observed remote access tool across ransomware incidents, followed by ScreenConnect, Splashtop, TeamViewer, LogMeIn, GoToAssist, and RustDesk. These tools were observed across a wide range of ransomware operations, including Akira, Qilin, INC, Interlock, Black Basta, Cactus, and RansomHub, underscoring their ubiquity and low attribution value.

- For credential access, Mimikatz remained one of the most consistently used tools in 2025. Despite its age, the tool remains effective at extracting credentials, NTLM hashes, and Kerberos tickets from compromised systems. Mimikatz was observed in intrusions associated with Akira, Qilin, INC, LockBit, Black Basta, Medusa, and RansomHub, often appearing shortly after successful privilege escalation or defense evasion and enabling rapid lateral movement and domain-level access. Additionally, LaZagne was observed in several ransomware engagements and was used to recover credentials stored in browsers, memory, and local applications, further supporting credential harvesting efforts during early to mid-stage post-compromise activity.

- Network discovery and internal reconnaissance tools were heavily used throughout 2025 as ransomware actors sought to rapidly map victim environments and identify high-value targets. Advanced IP Scanner remained the most frequently observed network discovery utility, followed by NetScan and other lightweight scanning tools. These tools were commonly used by most prominent ransomware groups, including Akira, Qilin, INC, Interlock, Lynx, INC, and Cactus, often in conjunction with native Windows discovery commands and Active Directory enumeration tools such as AdFind. In many intrusions, PsExec was used in a reconnaissance-adjacent role to validate administrative access across discovered hosts prior to broader lateral movement.

Rather than bespoke malware, affiliates prioritized tools that blend into enterprise environments, complicate detection, and enable flexible operations.

- Data exfiltration tooling in 2025 demonstrated both continuity and gradual evolution. Traditional file transfer utilities such as WinSCP and SSH File Transfer Protocol (SFTP) over OpenSSH remained widely abused, while cloud-native tools became increasingly prominent. MegaSync was frequently observed in Qilin intrusions for high-volume data exfiltration, while the Interlock ransomware group commonly leveraged AzCopy to transfer data directly to attacker-controlled cloud storage. Native utilities such as Xcopy continued to be used for local data staging prior to exfiltration. As double extortion remains a central pressure tactic, these tools are expected to persist in 2026.

- In 2025, threat actors placed increased emphasis on defense evasion through the use of EDR and AV disabling tools, including Terminator EDR Killer, EDRKillShifter, Hotta Killer, FortiEDR removal utilities, and AVKiller malware, which were observed across ransomware intrusions attributed to Akira, Qilin, Interlock, and Medusa. Additionally, Bring-Your-Own-Vulnerable-Driver (BYOVD) techniques became increasingly standardized, with drivers such as rwdrv.sys, K7RKScan.sys, DBUtil_2_3.sys, and SysMon.sys abused in campaigns linked to the Akira, INC, Qilin, Safepay, and Monti ransomware groups. These techniques enabled attackers to disable kernel-level protections and operate with reduced endpoint visibility.

- Command-and-control and tunneling techniques also continued to evolve in 2025. Cloudflared and OpenSSH were widely used to establish encrypted outbound tunnels in ransomware intrusions, while more advanced operations deployed frameworks such as Cobalt Strike and Velociraptor for post-exploitation coordination. In select cases, SOCKS proxy–based C2 communication was observed, particularly in activity associated with Nitrogen ransomware, and enabled traffic obfuscation and flexible routing for attacker communications.

In addition to the widespread abuse of legitimate and dual-use tools, ransomware intrusions in 2025 continued to feature a range of commodity, modular, and custom malware used to facilitate initial access, persistence, command-and-control, and credential theft.

SocGholish remained one of the most prominent initial access malware frameworks observed throughout the year. SocGholish is a malvertising-based malware framework that deceives users into installing fake software updates, typically delivered through compromised legitimate websites. Using drive-by techniques and social engineering prompts, SocGholish executes a malicious JavaScript payload that grants attackers initial system access. In recent campaigns, the framework has been used to distribute ransomware, remote access trojans, and backdoors, leading to multiple high-profile enterprise compromises. The use of SocGholish has previously been linked to ransomware groups, including Akira, Qilin, Interlock, Play, Luna Moth, Cactus, Fog, and Termite, highlighting its role as a shared initial access mechanism rather than a group-specific tool.

SystemBC remained a widely used malware component across multiple ransomware ecosystems, including Qilin, Play, Lynx, and INC. SystemBC functions as both a proxy and a remote access trojan, supporting encrypted command-and-control communications and SOCKS5 proxying. This capability allows attackers to route traffic through infected hosts, maintain persistent access, execute remote commands, and deliver additional payloads. As of 2025, SystemBC has expanded beyond Windows environments, with observed Linux variants leveraging encrypted channels and proxy features to move laterally and evade detection.

Neshta virus activity was also identified in several ransomware-impacted environments, including those later associated with the Qilin, INC, and RansomHub ransomware groups. Although Neshta is a legacy file-infecting virus rather than ransomware-specific malware, its presence indicates prior compromise, infected executables, or secondary malware delivery, which can facilitate persistence and payload execution prior to ransomware deployment.

Lumma Stealer was also commonly observed in ransomware-related intrusions throughout 2025, particularly during the early stages of compromise. Lumma functions as a credential and information-stealing malware capable of harvesting browser-stored credentials, session cookies, cryptocurrency wallet data, and detailed system metadata. In multiple campaigns, Lumma was used to collect authentication material that later enabled lateral movement, privilege escalation, or direct ransomware deployment. Its modular architecture and frequent delivery via phishing campaigns, malicious downloads, and traffic-redirection techniques make it an effective precursor malware across diverse ransomware ecosystems.

The use of custom information-stealing malware such as **Grixba** was identified in intrusions associated with the Play ransomware group. Grixba is designed to harvest credentials and sensitive system information to support internal reconnaissance, lateral movement, and eventual ransomware execution. Although observed less frequently than commodity stealers, the targeted deployment of Grixba suggests its use in higher-value or more controlled intrusions, where custom tooling provides greater operational security and precision.

Many of the tools and malware observed in 2025 remained consistent with what cybercriminals used in previous years. Defending against threat actors abusing legitimate and dual-use tools requires clear governance over approved applications and strict control of authorized use. Effective endpoint detection and response capabilities, combined with user behavior monitoring and application allowlisting, are essential for identifying and disrupting both malware and legitimate tools used by threat actors within enterprise environments.

Outlook for 2026

Akira will likely remain a top ransomware threat throughout the year

Compromised credentials and social engineering will likely remain primary attack vectors in 2026

Arete will continue to leverage real-time threat intelligence to serve those impacted by cyberattacks

At the beginning of 2026, Akira's activity continued to slow from the levels observed in the second half of 2025. Even with this decline, Akira remained the most active threat group in January, and—barring law enforcement disruptions like those seen with ALPHV and LockBit in 2024, or an abrupt departure like RansomHub in 2025—the group will likely remain a top ransomware threat throughout the year. Qilin continues to recruit affiliates on dark web forums as of early 2026, suggesting that the group will also remain a prominent threat in the near term.

Akira's attack surge in 2025 exposed just how damaging software vulnerabilities in popular VPN and firewall products can be to multiple organizations. In addition to vulnerability exploits in perimeter devices and third-party software, compromised credentials and social engineering will likely remain primary attack vectors in 2026. Social engineering, in particular, will likely continue to evolve in 2026, with threat actors increasingly leveraging emerging technologies to find new and creative ways to trick victims. ClickFix-style phishing continues to mature, moving beyond simple prompts into immersive, user-driven workflows, which pose a complex threat to organizations. Generative AI could also enable hyper-personalized phishing, dramatically increasing user interaction rates and initial access success.

On that front, AI will continue to play an expanding role in the cyber threat landscape in 2026, with both cybercriminals and defenders leveraging the technology. AI-powered cyberattacks will likely become more prevalent this year as threat actors increasingly integrate AI into their operations, enabling the rapid analysis of massive volumes of stolen data to identify high-value victims and increase pressure to pay ransoms. Conversely, AI is redefining enterprise cybersecurity and forensics by accelerating threat detection, automating evidence analysis, and empowering security teams to stay ahead of increasingly sophisticated adversaries.

Regardless of how the threat landscape evolves in the coming year, Arete will continue to leverage real-time threat intelligence from the frontlines of incident response to serve those impacted by cyberattacks, helping organizations effectively prevent, detect, and respond to cyber threats.

Footnote / Appendix

Data Collection and Analysis Methodology

Arete provides comprehensive incident response services, and the insights shared in this report are derived from incident response, digital forensics, restoration, managed detection and response, endpoint protection, threat hunting, threat intelligence, threat actor communications, dark web monitoring, and advisory and consulting services. While not every client opts to use all the cyber solutions Arete offers, Arete gathers data points from thousands of unique ransomware engagements going back to 2018. By collecting and validating data from diverse sources, Arete builds a comprehensive threat intelligence repository, analyzes raw data, identifies patterns, and provides context to enable informed decision-making.

All data pertaining to threat actors is collected and analyzed to ensure victims are anonymized and there is no chance of threat actors or readers identifying any victim. Only data from incidents where victims were extorted by the threat actor, with or without encryption, are included in this report. While we share some insights from pre-ransomware attacks in which threat actors were disrupted prior to encrypting and/or stealing data, those incidents are not included in any statistics. Finally, any information that Arete assesses could be used by threat actors to improve their operations (e.g., negotiated discounts per threat actor) is excluded from public reports but available to trusted partners upon request.

Bias Acknowledgement

There are thousands of ransomware attacks claimed by threat actors worldwide each year, while many more likely go unreported or remain unknown to the victims. Arete conducts analysis based on the data collected during our incident response engagements. These incident response engagements primarily represent organizations that have cyber insurance. As our data represents just a sample of the overall number of global ransomware attacks, it creates a sampling bias. The analysis contained in this report reflects the trends Arete observes first-hand during our engagements with cybercriminals and may differ from trends observed by the greater cyber community.

Sources

Abrams, L. (2025, October 14). **Oracle silently fixes zero-day exploit leaked by ShinyHunters.** BleepingComputer. https://www.bleepingcomputer.com/news/security/oracle-silently-fixes-zero-day-exploit-leaked-by-shinyhunters/

Albuquerque, P., Zohdy, M., & Alfano, V. (2025, April 30). **Ransomware debris: An analysis of the RansomHub operation.** Group-IB. https://www.group-ib.com/blog/ransomware-debris/

Burgess, M. (2025, September 22). **A cyberattack on Jaguar Land Rover is causing a supply chain disaster.** WIRED. https://www.wired.com/story/jlr-jaguar-land-rover-cyberattack-supply-chain-disaster/

CVE-2025-24472: Fortinet FortiProxy auth bypass vulnerability. (2026, January 22). SentinelOne. https://www.sentinelone.com/vulnerability-database/cve-2025-24472/

Deep Instinct Threat Lab, & Kahlon, O. (2025, March 25). **RaaS Evolved: LockBit 3.0 vs LockBit 4.0.** Deep Instinct. https://www.deepinstinct.com/blog/raas-evolved-lockbit-3-0-vs-lockbit-4-0

Gatlan, S. (2025a, June 6). **Critical Fortinet flaws now exploited in Qilin ransomware attacks.** BleepingComputer. https://www.bleepingcomputer.com/news/security/critical-fortinet-flaws-now-exploited-in-qilin-ransomware-attacks/

Gatlan, S. (2025b, August 5). **SonicWall urges admins to disable SSLVPN amid rising attacks.** BleepingComputer. https://www.bleepingcomputer.com/news/security/sonicwall-urges-admins-to-disable-sslvpn-amid-rising-attacks/

Gen 7 and newer SonicWall firewalls – SSLVPN recent threat activity. (2025, August 4). SonicWall. https://www.sonicwall.com/support/notices/gen-7-and-newer-sonicwall-firewalls-sslvpn-recent-threat-activity/kA1VN0000000RDG0A2

Green, D. (2025, June 30). **3 key takeaways from the Scattered Spider attacks on aviation & insurance firms.** Push Security. https://pushsecurity.com/blog/key-takeaways-from-the-scattered-spider-attacks-on-insurance-firms

Hackers claim 1.4 TB theft from Iron Mountain, major data management company. (2026, February 6). CyberNews. https://cybernews.com/security/iron-mountain-data-breach-claims/

Inside Akira's SonicWall campaign: Darktrace's detection and response. (2025, October 9). Darktrace. https://www.darktrace.com/blog/inside-akiras-sonicwall-campaign-darktraces-detection-and-response

LLM01:2025 prompt injection. (n.d.). **GenAI | OWASP.** https://genai.owasp.org/llmrisk/llm01-prompt-injection/

LockBit ransomware group unveils version 5.0 on its sixth anniversary. (2025, September 4). Daily Dark Web. https://dailydarkweb.net/lockbit-ransomware-group-unveils-version-5-0-on-its-sixth-anniversary/

Oracle security alert advisory - CVE-2025-61882. (n.d.). Oracle. https://www.oracle.com/security-alerts/alert-cve-2025-61882.html

Oracle security alert advisory - CVE-2025-61884. (n.d.). Oracle. https://www.oracle.com/security-alerts/alert-cve-2025-61884.html

Paganini, P. (2025, June 6). **Attackers exploit Fortinet flaws to deploy Qilin ransomware.** Security Affairs. https://securityaffairs.com/178736/hacking/attackers-exploit-fortinet-flaws-to-deploy-qilin-ransomware.html

Pearl Camiling, S., & Santos, J. (2025, September 25). **New LockBit 5.0 targets Windows, Linux, ESXi.** Trend Micro. https://www.trendmicro.com/en_us/research/25/i/lockbit-5-targets-windows-linux-esxi.html

Picus Labs. (2025, October 20). **Scattered LAPSUS$ hunters: 2025's most dangerous cybercrime supergroup.** Picus Security. https://www.picussecurity.com/resource/blog/scattered-lapsus-hunters-2025s-most-dangerous-cybercrime-supergroup

Product notice: SonicOS SSLVPN NULL pointer dereference denial-of-service (DoS) vulnerability. (2025, April 24). SonicWall. https://www.sonicwall.com/support/notices/product-notice-sonicos-sslvpn-null-pointer-dereference-denial-of-service-dos-vulnerability/kA1VN0000000RBe0AM

Qilin ransomware: All you need to know. (2025, April 25). Red Piranha. https://redpiranha.net/news/qilin-ransomware-all-you-need-know

Ramos, A. (2025a, February 13). **Arctic Wolf observes authentication bypass exploitation attempts targeting SonicWall firewalls** (CVE-2024-53704). Arctic Wolf. https://arcticwolf.com/resources/blog/cve-2024-53704/

Ramos, A. (2025b, January 24). **Arctic Wolf observes campaign exploiting SimpleHelp RMM software for initial access.** Arctic Wolf. https://arcticwolf.com/resources/blog/arctic-wolf-observes-campaign-exploiting-simplehelp-rmm-software-for-initial-access/

Ransomlook.io. (2026). RansomLook. https://www.ransomlook.io/

Riegler, M., & Gautam, S. (2026, January 31). **Risk assessment report Moltbook platform & Moltbot ecosystem**. Zenodo. https://zenodo.org/records/18444900

Slaney, R. (2025, January 16). **Grixba's disguise: Play ransomware impersonates SentinelOne for stealth recon.** Field Effect. https://fieldeffect.com/blog/grixba-play-ransomware-impersonates-sentinelone

Smith, B. (2025, November 11). **The chronicles of ClickFix: 2025's biggest hit keeps evolving.** GridinSoft. https://gridinsoft.com/blogs/clickfix-evolution-2025/

SonicOS SSLVPN pre-auth stack-based buffer overflow vulnerability 7.5. (2025, November 19). SonicWall. https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2025-0016

SonicOS use of externally-controlled format string vulnerability 5.9. (2025, July 29). SonicWall. https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2025-0013

Team Huntress. (2025, August 4). **Huntress threat advisory: Active exploitation of SonicWall VPNs.** Huntress. https://www.huntress.com/blog/exploitation-of-sonicwall-vpn

The beginning of the end: The story of Hunters International. (2025, April 2). Group-IB. https://www.group-ib.com/blog/hunters-international-ransomware-group/

Threat actor: Everest. (n.d.). Halcyon. https://www.halcyon.ai/threat-group/everest

Ukhanov, P., Stark, G., Work, Z., Pearson, A., Murchie, J., & Larsen, A. (2025, October 9). **Oracle E-Business Suite zero-day exploited in widespread extortion campaign.** Google Cloud Blog. https://cloud.google.com/blog/topics/threat-intelligence/oracle-ebusiness-suite-zero-day-exploitation

USA & Canada
New Engagements arete911@areteir.com
Phone 646-907-9767
Cyber Emergency Helpline 866-210-0955

India
New Engagements arete112@areteir.com
Cyber Emergency Helpline 1800-890-7383

UK
New Engagements arete999@areteir.com
Cyber Emergency Helpline +44-800-208-8084

General Inquiries marketing@areteir.com

www.areteir.com