Bridewell

Cyber Security. Where it Matters.

Bridewell Threat Intelligence

# 2025 Cyber Threat Intelligence Report

# Contents

# Foreword

**“Our CTI Annual Report for 2025 shares insights from our malicious infrastructure tracking program, and intelligence gathered by our Security Operations Centre (SOC) and Managed Detection & Response (MDR) services. This report also spotlights the information stealer ecosystem, and presents significant and emerging threats in our research section.**

Overall, 2025 has continued to mirror some of the trends seen in 2024. Based on activity we have observed as part of our malicious infrastructure tracking and through wider industry reporting, we have moderate confidence that threat actors will continue to innovate and improve capabilities to evade defences. A brief summary of these trends can be found in the executive summary, with more detailed information available later on in the report.

Our goal with this report is to share security insights and defensive recommendations that you can leverage to improve your defence and make your organisation(s) more resilient against cyber attacks. While monitoring persistent threat actors to stay ahead of the emerging threat landscape is challenging, being able to mitigate the threat posed by adversarial infrastructure should play a key part in your defensive security strategy.”

**Gavin Knapp**
Cyber Threat Intelligence Principal Lead

> “Threat actors will continue to innovate and improve capabilities to evade defences.”

By Joshua Penny, Senior Cyber Threat Intelligence Analyst; Tom Igoe, Senior Cyber Threat Intelligence Analyst
Gavin Knapp, Cyber Threat Intelligence Principal Lead; Craig Smith, Senior CTI Analyst

# Executive Summary

**In 2024, our CTI team made significant improvements to our malicious infrastructure tracking capability. This included tracking 10% more threat groups than in the previous year.**

## Malicious Infrastructure

The 2024 analysis of our malicious infrastructure tracking capability revealed notable new activity, themes and trends, including:

- 40% of all tracked malicious infrastructure is hosted within the United States (US) or China, a drop of 8% from 2023.
- A notable increase in Sliver and Brute Ratel command-and-control (C2) infrastructure, compared to a decrease in Cobalt Strike during 2024.
- Malware and tools closely linked to Chinese-nexus groups, such as ShadowPad, PlugX, Supershell, and even Cobalt Strike dominate the top 10 tracked threats.
- Lumma Stealer, Redline Stealer, StealC and Meduza Stealer are the preferred information stealers of 2024, with Lumma Stealer leading the way.
- Information stealers remain a primary initial access mechanism for emerging and trending ransomware groups such as Akira, RansomHub and Hellcat.
- Chang Way hosting is responsible for a quarter of all Redline Stealer servers, following law enforcement action in October 2024.
- AsyncRAT and QuasarRAT are amongst the most popular Remote Access Trojans (RATs) used used in 2024 after Gh0stRAT.

## Information Stealers

In the information stealer landscape, major insights included:

- Law enforcement operations contributed to a drop in the volume of global compromises. The volume of compromises still managed to peak in holiday seasons, however, especially in August and December 2024.
- Lumma Stealer, Redline Stealer and StealC are the primary information stealers impacting the UK.
- In UK CNI, Racoon Stealer and StealC were the dominant force in ransomware intrusions that utilised information stealers.

## Research

From a research perspective, our thematic topics include:

**Phishing Kits**

- Phishing Kits, and evolving threats such as ClickFix, are techniques shaping a new way of deploying malicious code via social engineering tactics.
  - Multiple diverse variants of ClickFix were seen over 2024 with clever innovations being used and copied by other groups.
  - Exclusive to cyber crime between Q1 - Q3 2024, ClickFix exploitation expanded in Q4 when nation-state groups began incorporating the technique into their attack chains.
  - ClickFix experienced a large spike in campaigns at the end of 2024 and moving into 2025, a trend that demonstrates a developing threat.

**EDRKillers**

- Endpoint Detection and Response Killers (EDRKillers) surged across ransomware groups, with EDRKillShifter fuelling Ransomhub's rise as a market leader.
  - This year, we have seen wider adoption of dedicated sophisticated EDRKillers such as AVNeutralizer (AuKill), EDRKillShifter, EDRSandBlast, EDRSilencer, MS4Killer, and Disabler.
  - Bring-Your-Own-Vulnerable-Driver (BYOVD) is becoming a trending technique used by EDRKillers in global ransomware operations.

**Fog Ransomware**

- The emergence of Fog ransomware is notable for its significant overlap in Tactics, Techniques, and Procedures (TTPs) with Akira ransomware, a prominent threat that consistently ranked among the top 5 ransomware intrusions throughout 2024. Geographically, 50% of Fog Ransomware attacks targeted the US, with Germany being the second-most frequent target at ~10%.

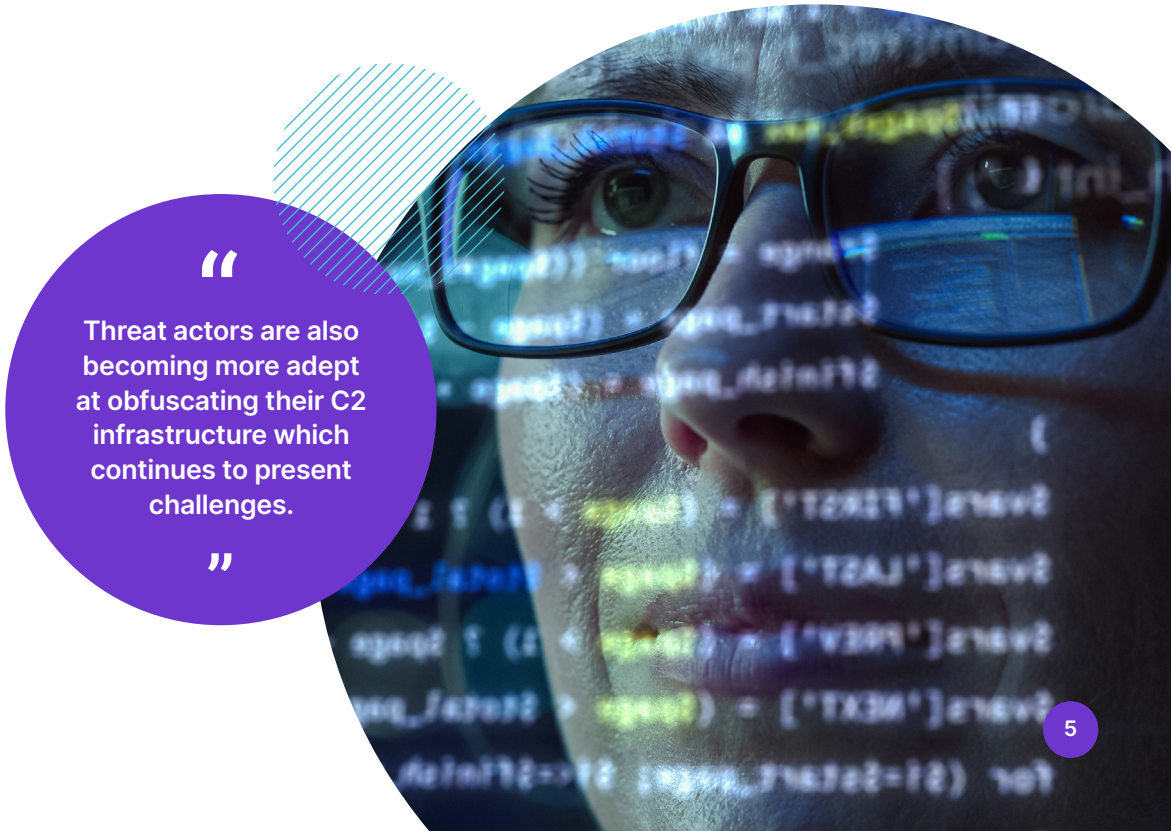
Finally, in Outlooks and Closing Remarks, we discuss emerging trends. These include: edge devices and vulnerability exploitation; operational relay box (ORB) networks; the cyber crime and ransomware ecosystems; cryptocurrency theft; generative artificial intelligence (genAI); geopolitical events; the Democratic People's Republic of Korea's (DPRK) exploitation of deceptive employment tactics; cloud native attacks; and remote management (RMM) tools.

# Executive Summary

## The Scope of Our Research

**It is important to understand that we leverage a specific set of open source and commercial tools which do not give us full coverage of host and network telemetry globally. Threat actors are also becoming more adept at obfuscating their C2 infrastructure which continues to present challenges in detecting malicious infrastructure with strong operational security.**

In addition to this, our security operations are primarily focused on the UK, US, and EU. As a result, the public and private intrusion data we have access to is not representative of all regions globally. There is also a heavy slant towards UK critical national infrastructure which is our primary area of focus.



# Adversary Infrastructure Tracking

Our adversary infrastructure program tracks threat groups in the PRE-ATT&CK stage leveraging various sources of telemetry to identify traffic from: Command-and-Control (C2) servers, botnets, RATs, initial access brokers (IABs), APTs, phishing, ransomware groups, open directories, TDS and ORB networks.

Gathering proactive indicators of attack (IOAs) allows us to hunt for those indicators on our clients' networks and alert our SOC/ MDR service.

## Overview of Dedicated Malicious Infrastructure

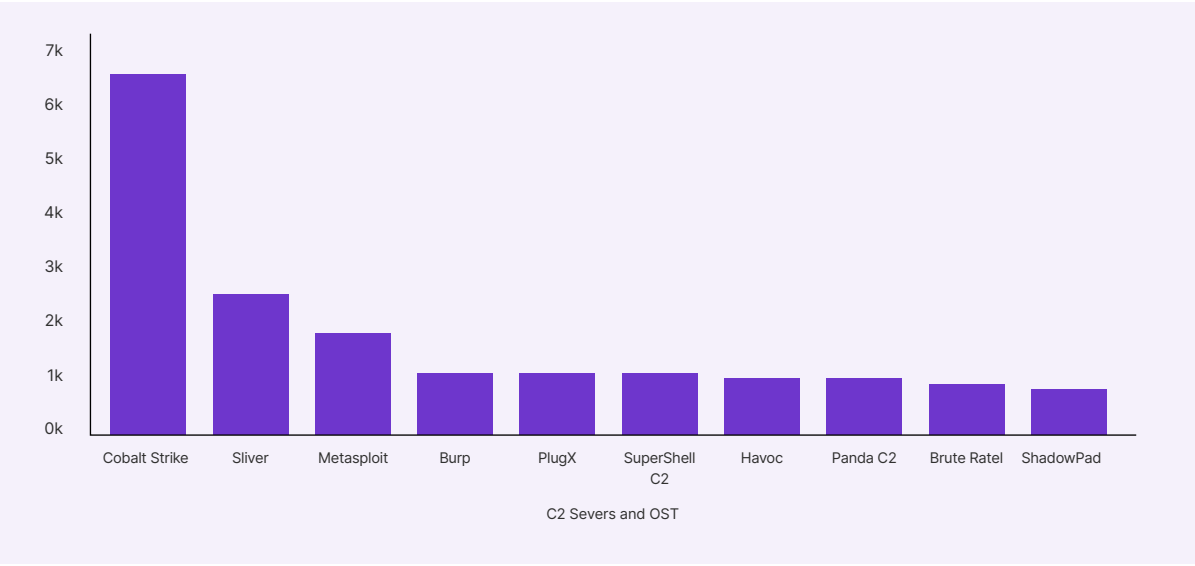
In 2024, Bridewell CTI tracked over 28,000 servers used by financially motivated threat actors and nation-state groups associated with malware C2 servers, phishing, payload hosting, threat actor controlled infrastructure and Offensive Security Tooling (OSTs).

This section will cover a summary of our adversary infrastructure tracking capability by infrastructure geolocation, infrastructure hosting providers, top 10 tracked threats, OSTs, information stealers, and RATs.

## Top 10 Tracked Threats

The top 10 tracked threats list for 2024 saw the removal of two major malware families: Qakbot and Raccoon Stealer. This was the direct result of law enforcement action and only small numbers of servers now remain active. New to the top 10 are Panda C2 and Brute Ratel as post-exploitation frameworks, and PlugX and ShadowPad, two well-known malware families linked to Chinese-nexus groups.

**Unique IPs Returned by Family**



# Adversary Infrastructure Tracking

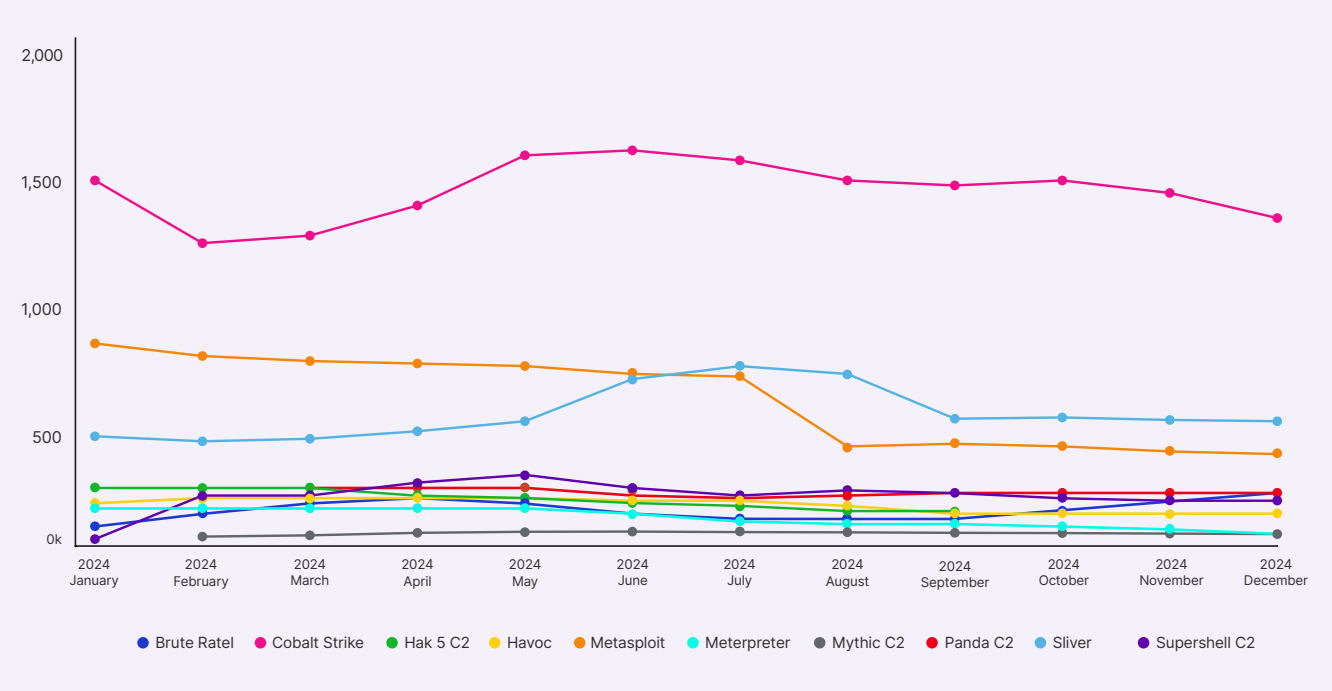
The top 10 threats in 2024 primarily consisted of C2 frameworks, post-exploitation tools, penetration testing utilities, and RATs that have been co-opted by cyber criminals for malicious purposes. Cobalt Strike, Sliver, Brute Ratel, and Panda C2 are widely used C2 frameworks that facilitate remote control, lateral movement, and persistence in compromised networks. Metasploit and Burp Suite, originally designed for security testing, are being exploited to help attackers gain unauthorised access. PlugX and Supershell are RATs typically linked to espionage campaigns, offering covert access and data exfiltration capabilities.

There are some other notable observations in 2024's top 10. Whilst Cobalt Strike servers topped 6000 in 2024, this still marks a drop from approximately 8000 servers from last year's report. Coupled with this decrease in numbers is the marked increase in C2 servers associated with Sliver and Brute Ratel infrastructure, suggesting a move away from Cobalt Strike amongst some threat actors.

However, the increase in Brute Ratel was most pronounced in the mid-latter quarter. Supershell servers continued to increase in numbers, peaking in May 2024 and remaining relatively high compared to 2023. Metasploit and Burp Suite are likely to remain in the top 10 in upcoming years due to their extensive use amongst pentest teams and criminals alike. This is due to their flexibility and extensibility which enables multiple use cases against targets.

When observing geographical hosting, malware and tools closely linked to Chinese-nexus groups, such as ShadowPad, PlugX, Supershell, and Cobalt Strike dominated the top 10 tracked threats. This highlights the scale and volume of possible infrastructure linked to Chinese-affiliated threat actors.

**Unique IPs by Query Name by Month**



# Adversary Infrastructure Tracking

## Global Hosting Distribution

In 2024, nearly 24% of all infrastructure we tracked was hosted in the United States. China hosted nearly 18%. The remaining countries were the same as in 2023, with Hong Kong, the Netherlands, and Germany rounding out our top five. The percentage shares for total infrastructure remained fairly consistent throughout the year with little deviation. This was to be expected given the role of hosting giants such as Amazon and Ali Baba.

Compared to 2023, we observed almost identical numbers of malicious infrastructure hosted within the US, on the same top ASNs, along with identical ASNs in China and Hong Kong. China saw a 6% reduction in malicious infrastructure hosting compared to 2023, which subsequently led to an increase in malicious infrastructure hosted in countries like the Netherlands and Germany.

When we analyse the Autonomous System Numbers (ASNs) per region, we can see that big hosting providers shared the majority of infrastructure within each of the top 3 regions. However, China presented over 80% of the malicious infrastructure hosting on its top 3 providers. We saw the smallest number of ASNs being used in China overall.

### United States

The top 3 hosting providers were Amazon (AS14618, AS16509), Digital Ocean (AS14061) and COLOCROSSING (AS36352), which equated to 39% of 379 ASNs in the US, 9% of the total malicious infrastructure distribution during 2024.

### China

The top 3 hosting providers were TENCENT (AS45090), ALIBABA (AS37963) and HWCSNET Huawei Cloud Service (AS55990), equating to 84% of 101 ASNs tracked in China, 14.74% of the total malicious infrastructure distribution during 2024.

### Hong Kong

The top 3 hosting providers were ALIBABA (AS45102), HWACENT-AS-AP (AS139471) and MYCLOUD-AS-AP LUOGELANG FRANCE LIMITED (AS135097), equating to 29% of 143 ASNs tracked in Hong Kong, 8.88% of the total malicious infrastructure distribution during 2024.

| Year | 2024 | | | | | | | | | | | | | Total |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Country | Jan | Feb | March | April | May | Jun | Jul | Aug | Sep | Oct | Nov | Dec | Total | |
| United States | 23.89% | 23.09% | 23.04% | 23.26% | 21.68% | 20.57% | 21.72% | 23.15% | 22.68% | 23.21% | 22.52% | 23.65% | 23.63% | 23.63% |
| China | 13.09% | 12.75% | 14.75% | 16.62% | 17.75% | 17.74% | 18.21% | 18.24% | 18.13% | 18.46% | 19.16% | 19.74% | 17.57% | 17.57% |
| Hong Kong | 9.06% | 9.59% | 9.98% | 11.32% | 12.97% | 13.31% | 11.00% | 7.46% | 7.78% | 7.69% | 7.68% | 7.22% | 8.88% | 8.88% |
| Netherlands | 7.28% | 7.65% | 7.05% | 6.53% | 6.17% | 6.49% | 7.27% | 8.81% | 8.69% | 8.47% | 8.54% | 8.88% | 8.40% | 8.40% |
| Germany | 8.80% | 8.51% | 7.91% | 7.20% | 6.91% | 7.06% | 7.15% | 8.29% | 8.77% | 8.80% | 8.51% | 7.75% | 7.52% | 7.52% |
| Russian Federation | 6.20% | 6.06% | 5.59% | 4.69% | 4.37% | 4.37% | 3.85% | 3.69% | 3.23% | 3.41% | 2.98% | 2.94% | 4.51% | 4.51% |
| Singapore | 3.29% | 3.76% | 3.77% | 3.78% | 3.76% | 4.08% | 4.06% | 3.95% | 3.71% | 3.64% | 3.77% | 3.86% | 3.54% | 3.54% |
| United Kingdom | 3.18% | 3.10% | 2.83% | 2.64% | 2.81% | 3.01% | 3.31% | 3.45% | 3.35% | 3.41% | 3.10% | 2.73% | 2.73% | 2.73% |
| France | 3.65% | 3.70% | 3.27% | 3.09% | 3.00% | 2.71% | 2.76% | 2.89% | 2.95% | 2.50% | 2.51% | 2.44% | 2.40% | 2.40% |
| Japan | 2.04% | 1.90% | 2.08% | 2.23% | 2.05% | 2.14% | 2.05% | 2.03% | 1.94% | 1.79% | 2.31% | 2.25% | 2.10% | 2.10% |

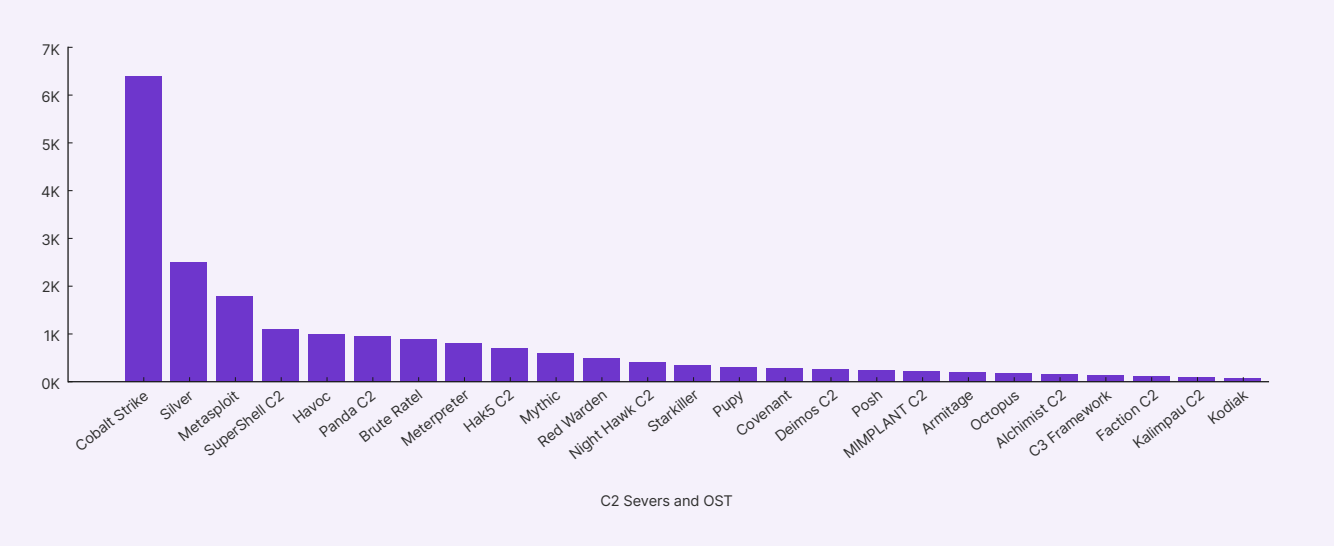
# Adversary Infrastructure Tracking

## Offensive Security Tooling (OSTs)

Post-exploitation frameworks are essential components in the arsenal of both red teams conducting security assessments and malicious actors orchestrating cyber attacks. These frameworks provide a suite of tools and capabilities that enable attackers to maintain persistence, move laterally within a compromised network, escalate privileges, and ultimately achieve their objectives, such as data exfiltration, system disruption, or ransomware deployment.

Our C2 tracking capability detected over 15,000 unique IP addresses associated with C2 frameworks in 2024. Half of all servers were hosted in either China or the United States (28% and 22% respectively). Sliver has seen a notable increase in utilisation by threat actors (12% to 17%), including Brute Ratel in the last three months of the year (up from 1% to 7%). Additionally, we continue to see increases in the usage of Supershell, usually deployed on similar IP addresses to other threat actor tools.

**Offensive Security Tools (OST)**




> "Our C2 tracking capability detected over 15,000 unique IP addresses associated with C2 frameworks in 2024."

# Adversary Infrastructure Tracking

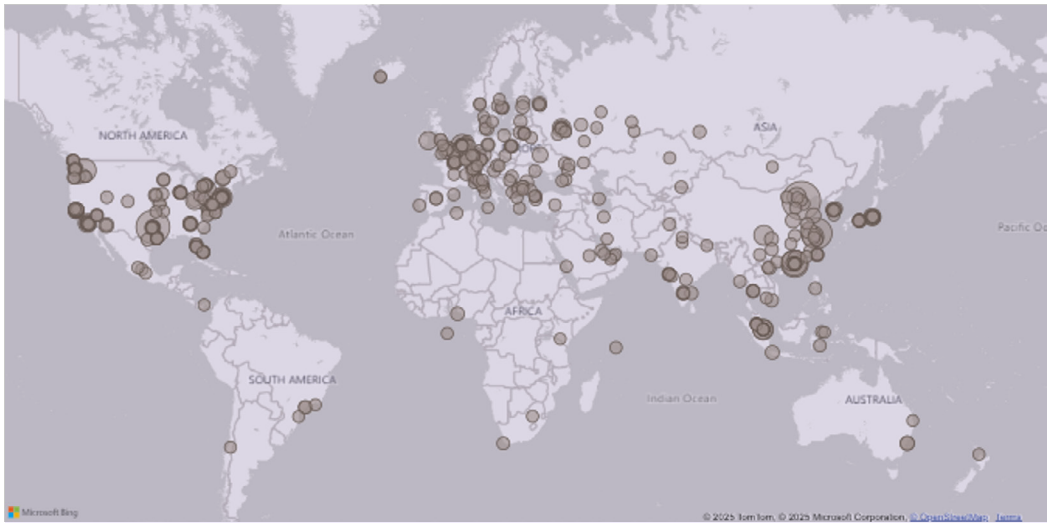
## Cobalt Strike

Cobalt Strike, a commercial framework initially designed for adversary simulation and penetration testing, has become one of the most widely utilised tools by threat actors. Its comprehensive features, including C2 functionalities, lateral movement techniques and payload deployment mechanisms, have made it a favourite among both legitimate security professionals and threat actors.

However, the dual-use nature of Cobalt Strike has led to widespread abuse, with pirated and unlicensed versions readily available on cyber criminal marketplaces, facilitating its use in numerous offensive campaigns.

The popular post-exploitation framework accounted for 42% of all servers tracked by tools under the OST category. Of the Cobalt Strike servers tracked that aren't redirectors, nearly 45% are hosted in China. These hosting providers, TENCENT (AS45090), ALIBABA (AS37963) and HWCSNET Huawei Cloud Service (AS55990), appear to be attractive infrastructure hosting providers as the shelf-life of C2 servers within China is considerable. The shelf-life of these services is typically up to a year, suggesting an absence of any outside interference from the hosting providers or law enforcement. TENCENT and ALIBABA in particular account for 80% of all Cobalt Strike servers hosted in China.

**Cobalt Strike C2 Global Distribution**




In comparison, 17% of Cobalt Strike servers were hosted on servers in the United States. Additionally, this was broken down in a much larger portion of hosting providers, with 37% of servers found on Digital Ocean (AS14061), Amazon (AS14618, AS16509), and COLOCROSSING (AS36352). 11% of Cobalt Strike servers were hosted in Hong Kong, with ALIBABA-CN-NET (AS45102), LUCIDACLOUD LIMITED (AS139659) and High Family Technology Co. (AS142032) accounting for 34% of servers in this region.

In response to the prevalent misuse of Cobalt Strike, particularly by ransomware gangs and nation-state actors, cyber security firms, law enforcement agencies, and industry organisations have made significant efforts to disrupt its illicit use. These efforts have included collaborative initiatives to identify and dismantle malicious infrastructure associated with Cobalt Strike.

However, we assess that whilst a decrease in the number of Cobalt Strike servers between 2023 and 2024 could attest to this disruptive action, numbers remain high overall and continue to do so in other geographical areas. Additionally, we have observed an increase in frameworks such as Sliver and Brute Ratel which suggests a move away from Cobalt Strike. Whilst we expected to see this more notably in countries such as the United States, the majority of new Brute Ratel servers are within China.

# Adversary Infrastructure Tracking

## Increased Adoption of Sliver and Brute Ratel

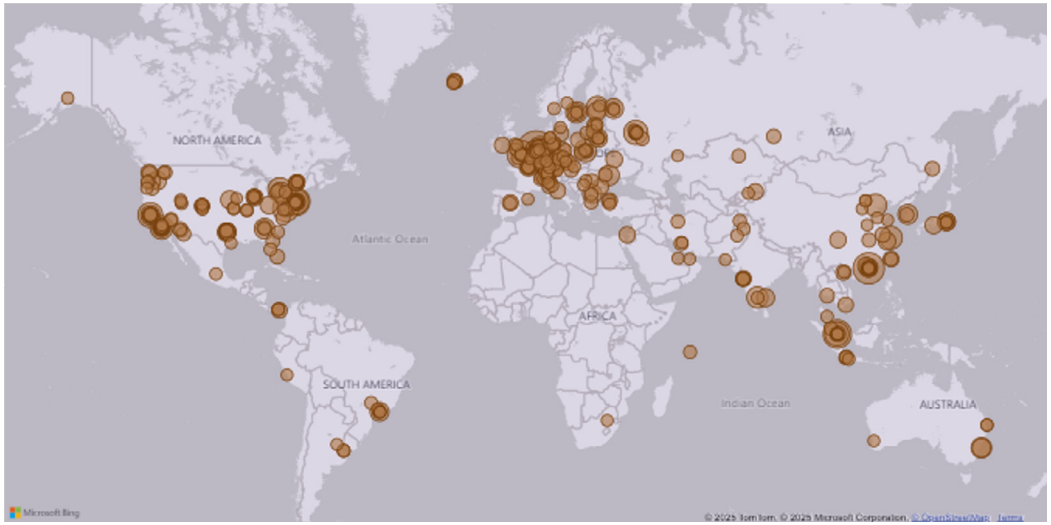
Sliver was developed as an open-source red team/ adversary emulation tool primarily used for security testing purposes. It is a common tool used by a wide range of threat actors to establish C2 within their target's environment and network.

Our C2 infrastructure tracking capability proactively monitors for Sliver network indicators. The figure to the right is a visual representing our current detection for Sliver. In 2024, we tracked over 2000 servers linked to Sliver.

The cyber security landscape in 2024 showed clear indicators of a growing trend towards the adoption of alternative post-exploitation frameworks, to Cobalt Strike, particularly Sliver and Brute Ratel, suggesting a shift in preferences among threat actors. This report highlights an increase in the detection of Sliver servers throughout the year.

While Cobalt Strike remained the dominant framework in terms of the number of C2 servers observed, Sliver experienced a notable rise in detections, positioning it as a prominent alternative alongside Metasploit. The Sliver offensive security framework has emerged as a significant tool in the cyber threat landscape, initially noted for its adoption by ransomware groups. However, its versatility and effectiveness have also attracted the attention of other malicious actors, including Advanced Persistent Threat (APT) groups and access brokers.

**Sliver Global Distribution**




Nearly 15% of OST C2 servers were attributed to the Sliver framework in 2024. Unlike Cobalt Strike geographical deployments, Sliver servers are vastly different. Whilst China hosted the highest number of C2 servers (almost 45%), the highest concentration of Sliver deployments in a single country was just 25% in the US. Second was the Netherlands at 13% and Germany at 11%. China drops to 5th highest with 6% of Sliver servers.

The top 3 hosting providers associated with each country are:

- The United States: Digital Ocean (AS14061), COLOCROSSING (AS36352) and UPCLOUDUSA (AS25697) accounted for 38% of Sliver servers in the US.
- The Netherlands: Stark Industries (AS44477), Digital Ocean (AS14061) and UPCLOUD (AS202053) accounted for 33% of Sliver server in the Netherlands.
- Germany: Digital Ocean (AS14061), Hetzner (AS24940) and Contabo (AS51167) accounted for 42% of Sliver servers in Germany.

# Adversary Infrastructure Tracking

Several documented instances in 2024 provide concrete evidence of threat actors actively deploying Sliver:

- The North Korean Andariel group's collaboration with Play ransomware involved the use of Sliver for initial access, demonstrating its adoption by a nation-state actor. Additionally, a campaign targeting German entities was observed utilising a Sliver implant, highlighting its use in targeted attacks.

- Furthermore, Sliver was reported to be delivered via exploits targeting vulnerable SimpleHelp Remote Monitoring and Management (RMM) instances, indicating its use by actors exploiting software vulnerabilities for access. The reasons for Sliver's popularity among diverse threat actors remain consistent; its open-source nature, evasion capabilities, and the growing perception of it as a viable alternative to Cobalt Strike.

- Investigations into RansomHub ransomware attacks between September and October 2024 revealed the involvement of ShadowSyndicate. This threat actor has been associated with multiple ransomware groups and utilises various tools, including Sliver, Cobalt Strike, IcedID, and Matanbuchus. ShadowSyndicate's role in facilitating RansomHub attacks suggests they may operate as an access broker, providing initial access to victim networks that ransomware affiliates then exploit.

- A September 2024 report highlighted the use of a "Sliver beacon" by a threat actor associated with BlackCat/ ALPHV ransomware. This is likely the group referred to as DragonForce or operating under the name Nitrogen. This group utilised a malicious application ("NitrogenInstaller") to deploy Cobalt Strike, followed by the Sliver beacon.

- In our recent report on Hellcat group, we published a thorough analysis of the emerging threat group and their utilisation of Sliver as a post-exploitation framework during their well-publicised attacks on companies such as Schneider Electric, Pinger, and Capgemini.

Brute Ratel, also known as BRC4, is a commercial framework intended for red-teaming and simulating adversarial attacks. It stands out in the current C2 market due to its ability to emulate different stages of an attacker's kill chain and provide a structured timeline for each executed attack. Brute Ratel's implants, known as badgers, can take various forms, including executables, service binaries, DLLs, and PowerShell scripts.

Only 4% of the OST frameworks tracked in 2024 belonged to Brute Ratel. However, Bridewell observed a 400% increase in tracked servers linked to the framework between January and December 2024.

At the beginning of 2024, 35% of BRC4 servers were hosted in China, with 15% and 19% being hosted in the United States and Japan respectively. However, there was a considerable shift in distribution through the year. We observed a gradual increase in servers hosted within the US but a drastic scaling of BRC4 infrastructure within China. In December, 76% of BRC4 servers were hosted in China, 10% in the United States and 2% in Japan. For the year in total, 64% of BRC4 servers were tracked as hosted in China.

# Adversary Infrastructure Tracking

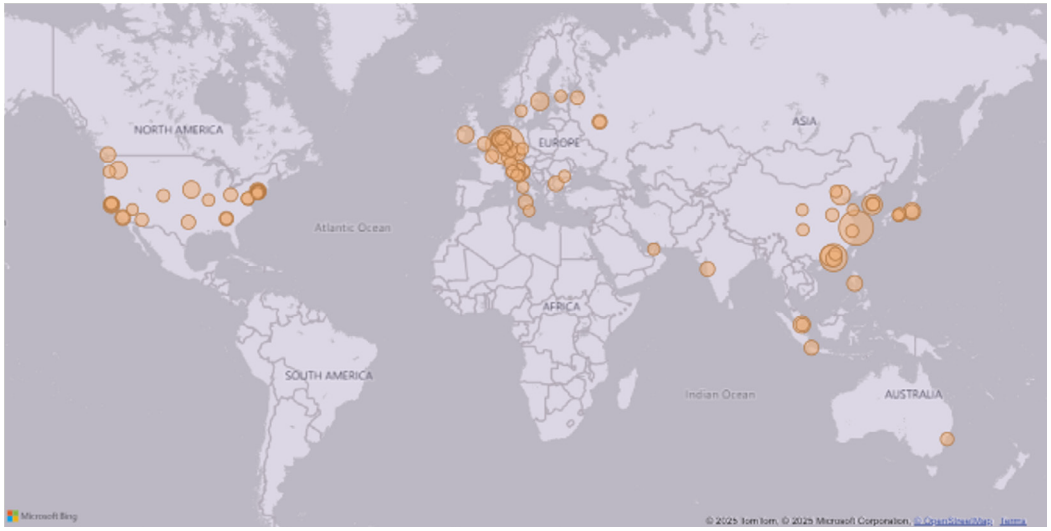
The top 3 hosting providers associated with each country are:

- China: TENCENT (AS45090), VOLCANO-ENGINE (AS137718) and China Telecom Group (AS4811) accounted for 93% of BRC4 servers in China.
- United States: DIGITALOCEAN (AS14061), AMAZON (AS16509) and IS-AS-1 (AS19318) accounted for 57% of BRC4 servers in the United States.
- Japan: AMAZON (AS16509), VULTR (AS20473) and Microsoft (AS8075) accounted for 98% of BRC4 servers in Japan.

The first documented instance of Brute Ratel being used for malicious purposes was attributed to the Russian state-sponsored threat actor APT29, also known as Nobellium or Cozy Bear, using BRC4 in campaigns between May and June 2022.

Regarding utilisation by ransomware groups, Black Basta has emerged as a prominent user of the Brute Ratel framework, often deploying it as a second-stage payload following initial access. In October 2024, LUNAR SPIDER was seen employing their Latrodectus downloader to deliver a Brute Ratel C4 payload in campaigns targeting the financial sector, potentially providing initial access that ALPHV could then leverage for ransomware deployment.

**Brute Ratel C2 Global Distribution**




Conti, a now defunct but influential ransomware operation, had former members who were discovered attempting to acquire licenses for Brute Ratel using fake company profiles. Additionally, the BlackSuit ransomware group has been observed utilising Brute Ratel for data exfiltration from compromised networks.

The Brute Ratel post-exploitation framework represents a significant and evolving threat to organisations across various sectors. Its sophisticated design, focused on evading modern security defences, has made it a tool of choice for both financially motivated cyber criminal organisations, particularly ransomware groups, and nation-state actors engaged in espionage and intelligence gathering.

The availability of a cracked version has further amplified its reach, lowering the barrier to entry for a wider range of malicious actors. As we move further into 2025, we expect to observe a similar trajectory for Brute Ratel.

# Adversary Infrastructure Tracking

## Supershell

Supershell C2 utilises web services for its operations and offers features like remote shell access, file management, and memory injection, and even supports team collaboration.

Its ease of use lowers the barrier to entry for cyber attacks, and its web interface makes it easily discoverable. Supershell C2 has been observed in active cyber attacks, often in conjunction with other malicious tools, and has been linked to threat actor groups believed to have connections to the China, emphasising its role in facilitating sophisticated remote control for nefarious purposes.

Supershell has been observed in campaigns such as those reported by Elastic Search in January 2024. In this campaign, threat actors targeted financial institutions in South-East Asia using tunnelling tools and Supershell. Understandably, threat actors in this region continue to operate on local hosting providers and with Supershell we saw no exception. 62% of servers were hosted in China, 17% in Hong Kong, and 12% in the United States by the end of 2024.

**Supershell C2 Global Distribution**

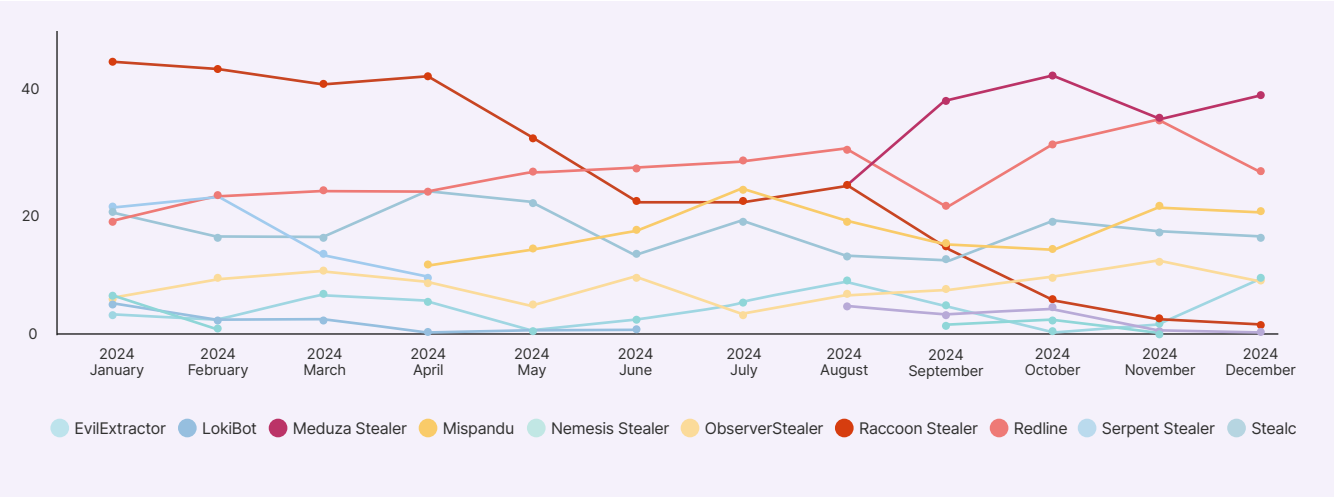
# Adversary Infrastructure Tracking

## Information Stealers

Information stealers (infostealers) remain an ever-present threat to organisations, acting as the initial precursive cut into a network. We have observed an increasing number of ransomware victims succumbing to attacks as a result of information stealer infections and this threat only grows as ransomware groups continue to exploit compromised credentials.

Prominent groups such as LockBit, RansomHub, Akira, and Hellcat were commonly associated with infections initiated by information stealers. Akira was among the ransomware groups that have rapidly deployed payloads within hours of gaining access, often through information stealers. The Hellcat group breached Telefonica and Schneider Electric, where JIRA credentials obtained via information stealers were allegedly used to facilitate the ransomware attacks and subsequent data leaks.

Unlike the distribution of OST infrastructure in geographies such as China, the information stealer landscape paints a different picture altogether. China doesn't crack close to the top 10 countries involved in the stealer ecosystem. We continue to see threat actors choose major hosting providers in the United States and Europe, as well as relying on Bullet Proof Hosting and Russian servers.




Throughout 2024, 30% of Information Stealer C2 servers were located within the United States with Amazon (AS14618) at 6%, Kakharov Orinbassar Maratuly (AS211849) at 5% and CNServers at 2% of the total distribution.

20% of Information stealers C2 infrastructure was hosted on ASNs with presence in the Netherlands. Anton-Levin (AS50053), Hostinger (AS47583) and the now inactive Limenet (AS394711) were responsible for this share of total servers.

We also observed 16% of information stealer C2s in Russia, a noticeable increase from OSTs. Top contributors to this were Media land LLC (AS206728), the now inactive Chromis Ltd (AS216319) previously linked to significant amount of Amadey and Redline Stealer-based malware traffic on its IP ranges, and JSC Mediasoft.

# Adversary Infrastructure Tracking

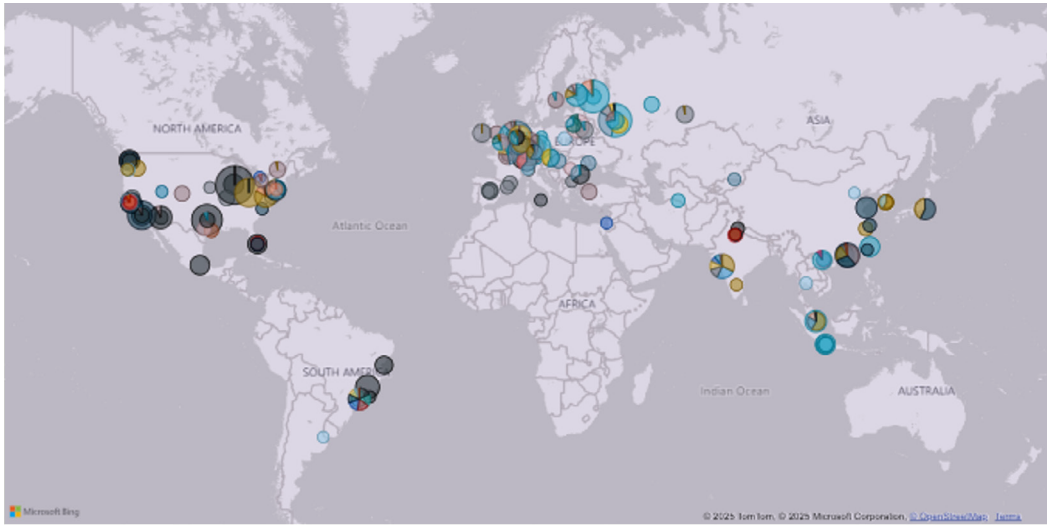
## Lumma Stealer

Throughout 2024, we observed Lumma Stealer rising in prevalence as the most dominant stealer on the market today, eclipsing stealers such as Raccoon Stealer, Redline Stealer, Meduza Stealer, Mispadu and StealC. This dominance has largely been observed within our datasets, occurring around similar time windows to increased Redline Stealer and Meduza Stealer C2 infrastructure towards the latter part of 2024.

Lumma Stealer campaigns in 2024 employed a diverse range of delivery methods and infection techniques, showcasing the adaptability of threat actors in their attempts to compromise systems. A particularly prominent method involved the use of malvertising, where malicious ads redirect users to fake CAPTCHA pages or other malicious landing pages. These deceptive pages often employ social engineering tactics to trick users into performing actions that lead to malware execution, such as copying and pasting malicious commands into the Windows Run dialog.

This technique allows attackers to bypass traditional browser-based security controls by having the user initiate the infection process outside the browser context. Another common delivery method involved bundling Lumma Stealer with cracked software. Threat actors would embed the malware within pirated versions of popular applications like ChatGPT, Vegas Pro, and Adobe Premiere, preying on users seeking to obtain these tools for free.

**Information Stealer C2 Global Distribution**



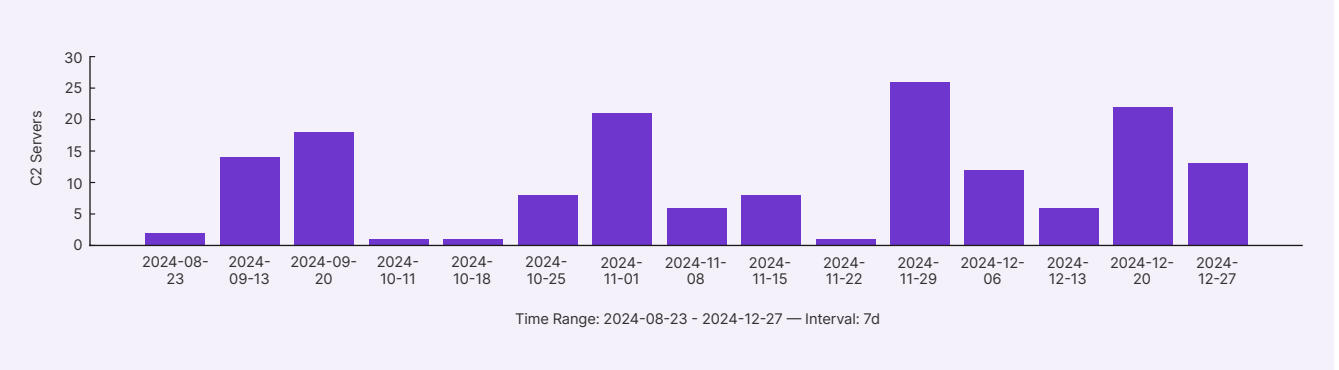

Traditional methods such as phishing emails and Discord messages containing malicious attachments or links also remained prevalent. Attackers also leveraged compromised websites to distribute Lumma Stealer, either by injecting malicious code into legitimate sites or by hosting malicious files directly.

# Adversary Infrastructure Tracking

In some instances, Lumma Stealer was delivered through compromised videos on online marketplaces and adult content websites using the Win/Rozena.ADZ injector, and it was also found embedded in Key Management Services (KMS) activators used for pirating Windows copies. A notable trend in 2024 was the abuse of legitimate platforms like GitHub repositories to host and distribute Lumma Stealer, often disguised as automation tools or legitimate software.

This included exploiting GitHub's release infrastructure to deliver the malware. Other delivery methods observed included Discord content delivery network (CDN) abuse, the use of fake hacker tools, drive-by compromise via Web Distributed Authoring & Versioning (WebDAV) servers, and exploiting the infrastructure of compromised educational institutions. Additionally, threat actors spread Lumma Stealer through compromised YouTube links, social media posts advertising cracked software, and even GitHub comments containing malicious links.

A majority of C2 domains for Lumma Stealer reside behind Cloudflare. However, we have identified a number of servers hosted on Bullet Proof Hosting and other providers widely linked to cyber crime. For example, we have identified Hetzner (AS24940), AS-REG (AS197695), Informacines sistemos ir technologijos (AS61272), Green Floid LLC (AS59729, AS204957), AEZA Group (AS204603) and STARK INDUSTRIES (AS44477) as also linked to Lumma Stealer C2 infrastructure.

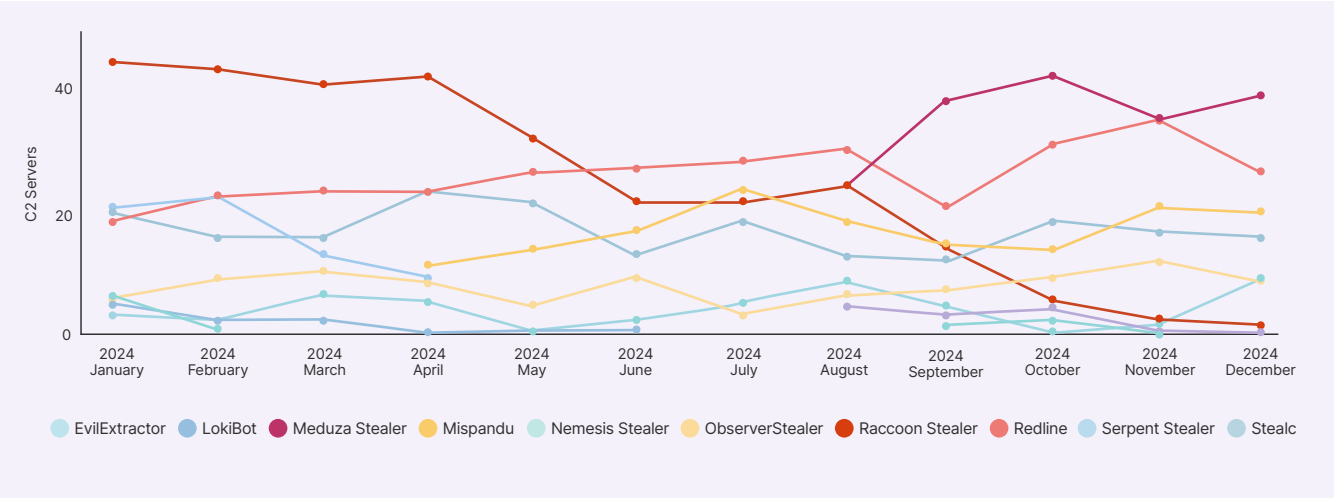



This rapid adoption by a wide range of threat actors placed Lumma Stealer as the top information stealer threat we tracked. The above graph demonstrates the rapid adoption and deployment of infrastructure linked to the stealer in the second half of 2024. As we cover in the Information Stealer specific section of the report, Lumma Stealer dominates the market in relation to ransomware groups purchasing credentials linked to the stealer to enable their operations - the C2 infrastructure we tracked confirms this trend.

# Adversary Infrastructure Tracking

## Rise of Meduza Stealer

We observed a substantial decline in Raccoon Stealer C2 infrastructure with a concurrent upwards trend with Redline Stealer and Meduza Stealer servers. Raccoon Stealer was dominant in the first half of 2024, and despite the sharp decline throughout the year, we tracked most of the C2 servers linked to the information stealer.




The Meduza Stealer first appeared on dark web forums in June 2023, quickly establishing itself as a notable competitor among established information stealers. This emergence aligns with the broader trend of increasing prevalence of Malware-as-a-Service (MaaS) information stealers in 2024, with Lumma Stealer leading this trend.

Meduza Stealer has undergone substantial technical improvements, focusing on expanding its functionality and enhancing its stealth capabilities including support for Chromium-based web browsers, enabling the extraction of local storage data, support for new browser-based cryptocurrency wallets and Google Account tokens called “Google Token Recovery.” The crypting stub used by the stealer has been improved to enhance its ability to evade detection and enhanced obfuscation techniques are offered as an optional service for an additional fee. These combined updates demonstrate a clear trend of continuous development focused on expanding the malware’s functionality.

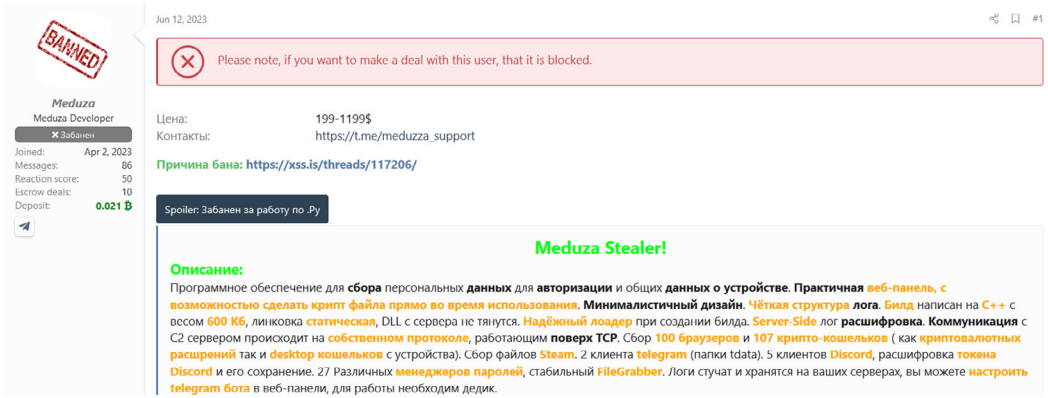
The most notable connection between Meduza Stealer and ransomware arises through its association with the threat actor group known as Scattered Spider. Scattered Spider, also tracked under various aliases such as Octo Tempest, Roasted 0ktapus, and UNC3944, is a financially motivated cyber criminal group active since at least 2022. This group is known for engaging in data extortion and has a history of deploying multiple ransomware variants, including ALPHV/BlackCat, RansomHub, and Qilin.

In June 2024, Meduza Stealer was banned from underground marketplaces and forums. It was identified that the stealer had no mechanisms in place to mitigate the users of the stealer within Commonwealth of Independent States (CIS) countries being infected. This lack of adherence to ethics amongst the underground community led to the developer being banned on the popular XSS forum. Meduza Stealer is glaringly omitted from credential stealer marketplaces for this reason and is likely why it is difficult to link credentials harvested by this stealer to ransomware groups. Despite all this, we continue to see the stealer increasingly adopted by threat actors.

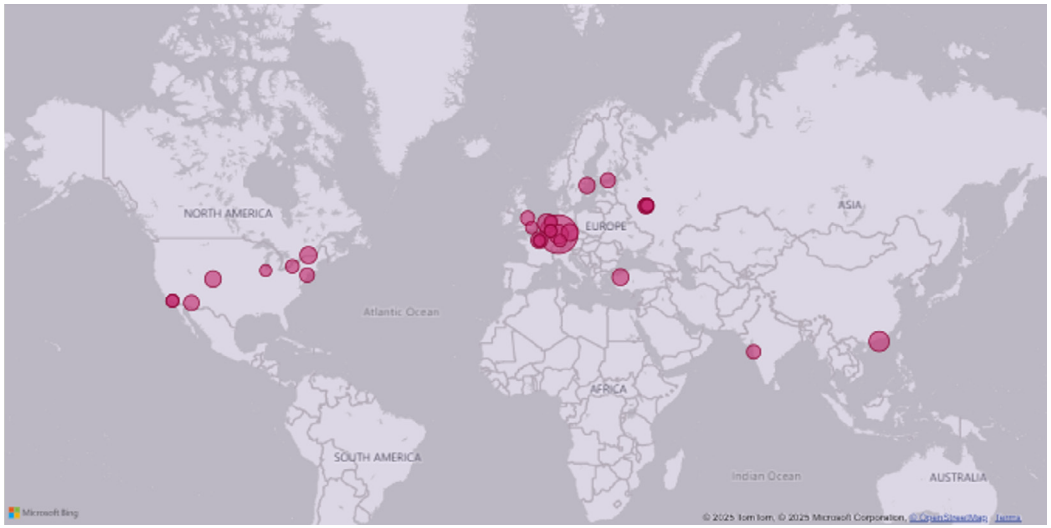
# Adversary Infrastructure Tracking

Recent enhancements are also reflected in the progressive increase in associated C2 infrastructure linked to Meduza Stealer and its growing adoption amongst threat actors. The AEZA ASN (AS14618) was the most utilised provider for Meduza Stealer C2 infrastructure across the top three countries, operating in Germany, the United States, and Sweden. 70% of Meduza Stealer servers were hosted in Germany, with 57% of those linked to AEZA, representing a significant portion of the overall distribution. This distribution differs from the general information stealer trend surround geographical distribution; Meduza Stealer has very little Russian presence in 2024 compared to its competitors.

The last quarter of 2024 saw a large spike in Meduza Stealer servers. Only Lumma Stealer had a higher volume of servers, suggesting ongoing updates and developments to make it a leading player in the ecosystem and that it is a rich source of data for ransomware and criminal groups. However, we are yet to observe any public data, internal intrusions, or evidence to link the stealer to ransomware activity outside of historical Scattered Spider intrusions.




**Meduza Stealer C2 Global Distribution**



# Adversary Infrastructure Tracking

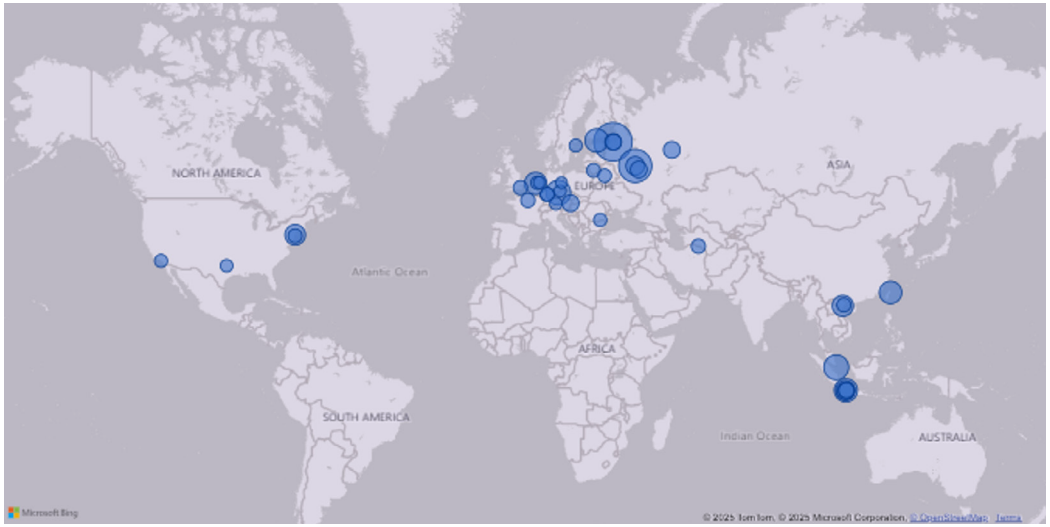
## Redline Stealer Resists Law Enforcement

Redline Stealer, much like all information stealers, relied heavily on social engineering tactics, including phishing emails, malvertising, and bundling with pirated software. Analysis of Redline Stealer's infrastructure highlights that the majority of the backend infrastructure linked to the stealer is hosted in Russia (55%), Germany (10%) and Finland (9%).

The hosting within Russia can be attributed to the following providers: Medialand (AS206728) with 17%, Chang Way Technologies (AS207566) at 7% and Redbyte LLC at 6%. The introduction of a new ASN linked to Chang Way, which also operates AS57523 is interesting. The new ASN, AS207566, appeared within our Redline Stealer dataset in October 2024, the same time as Operation Magnus, a coordinated international law enforcement action which disrupted the infrastructure of Redline Stealer and its clone, META Stealer.

Additionally, 63% of all Redline Stealer C2 servers were hosted in Russia, sparking a notable increase in post law enforcement action, which saw a decrease in countries such as the Netherlands, United States and Finland. Whilst reports suggest activity linked to the stealer has decreased, our dataset suggests the threat actors just moved to another location to resume operations.

**Redline Stealer C2 Global Distribution**



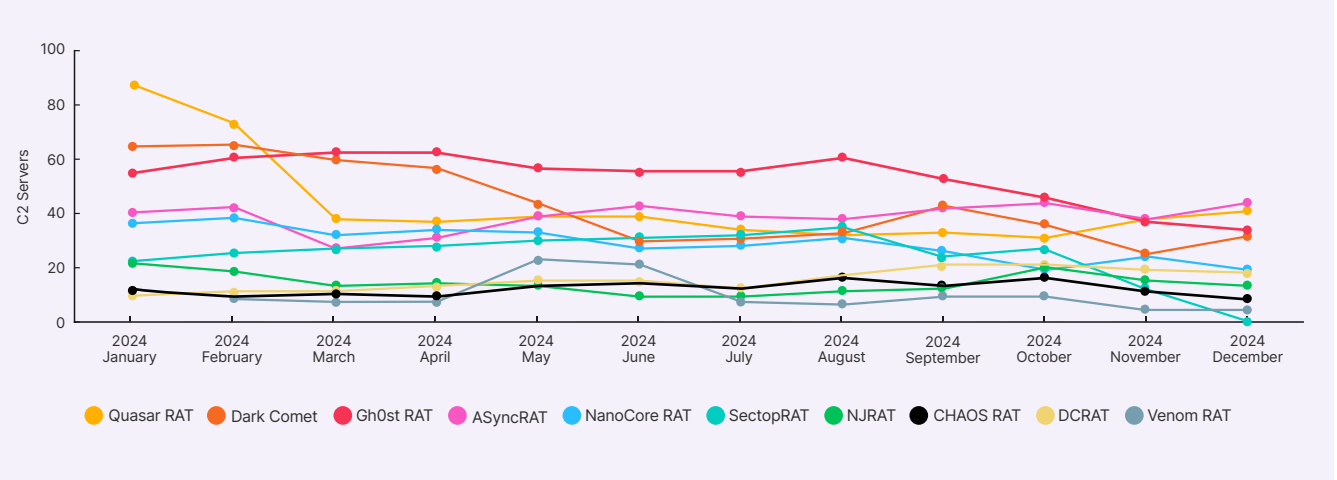

> **Analysis of Redline Stealer's infrastructure highlights that the majority of the backend infrastructure linked to the stealer is hosted in Russia.**

# Adversary Infrastructure Tracking

## RATs

The cyber threat landscape in 2024 continued to be significantly shaped by the proliferation and evolution of RATs. RATs are malicious software programs that grant attackers remote control over an infected computer.

Functioning similarly to legitimate remote administration tools, RATs allow cyber criminals to perform a wide range of actions, including stealing sensitive data, monitoring user activity through keylogging and webcam access, and even using the compromised system to launch further attacks. Throughout 2024, we observed persistent RAT utilisation by threats actors across multiple geographies and campaigns. Amongst our dataset, we saw Gh0stRAT topping the graph for most C2 servers, followed by QuasarRAT, Dark Comet, AsyncRAT, Nanocore, NJRAT, DCRAT and SectopRAT. By the end of 2024, we saw AsyncRAT and QuasarRAT as the most popular RATs.



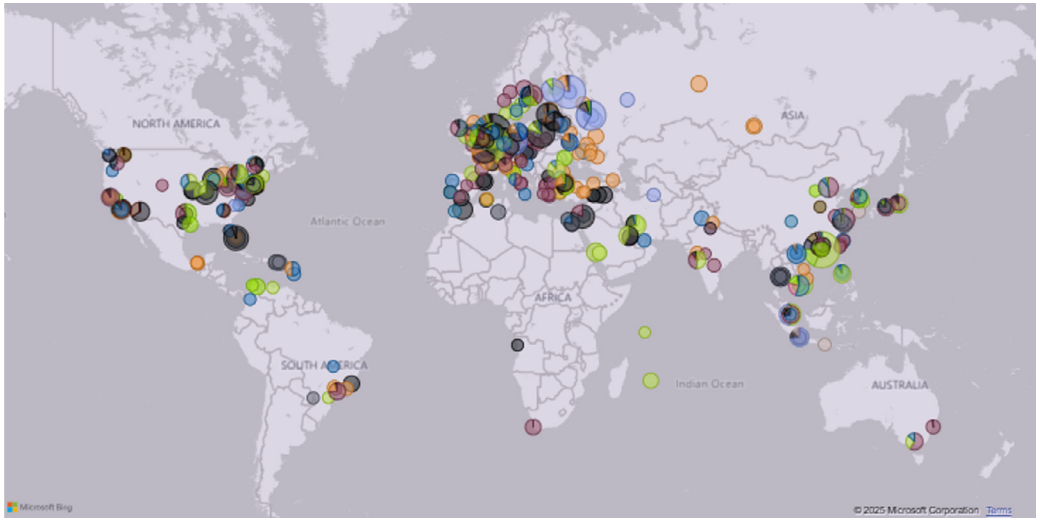

# Adversary Infrastructure Tracking

The general distribution of RAT C2 infrastructure, however, is far less top-heavy when compared to OSTs and Information stealers, with a more noticeable global distribution. This suggests that RATs, specifically open-source ones, are available to a range of skilled threat actors and used in campaigns affecting all continents.

Much like Information stealers, the geographical distribution remains fairly similar in the top 3; the United States accounted for 17% of RAT servers globally, with Amazon (AS16509, AS14618) and Reliablesite (AS23470) in the top 3. Russia and the Netherlands each accounted for 8% of RAT servers.

We observed heavy utilisation of LimeNet by a plethora of RATs up to September 2024, such as VenomRAT, ASyncRAT, Nanocore, Dark Comet, DCRAT, QuasarRAT, BlackNetRAT, BlackShadesRAT and NJRAT, when the hosting provider then ceased to operate under this ASN. Limenet is a well-known Bullet Proof Hosting provider, and we have routinely observed this level of activity associated with the ASN. At the end of September, Limenet announced a cleaning of their IP ranges, in response to actions taken to blocklist their IP ranges.

**RAT C2 Server Global Distribution**




> **The United States accounted for 17% of RAT servers globally, with Amazon (AS16509, AS14618) and Reliablesite (AS23470) in the top 3.**

# Adversary Infrastructure Tracking

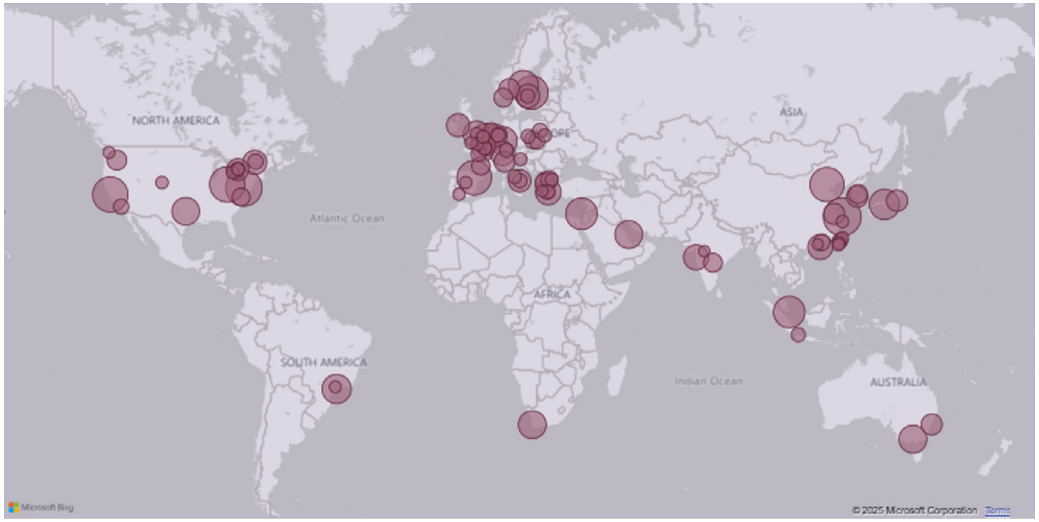
## Gh0stRAT

Gh0stRAT, a well-established malicious tool first identified in 2008, continues to pose a significant threat. A RAT which had its source code publicly released lead to the development of numerous variants and subsequent widespread adoption by various threat actors.

Intelligence suggests that geographical distribution of Gh0stRAT in 2024 was diverse, with a notable concentration in East Asia and specific instances of targeted attacks in other parts of the world. This is reflected within our dataset, where we observed a broad distribution of C2 servers distributed across all major continents reflecting the RATs global utilisation and targeting.

During 2024, the top 5 countries hosting Gh0stRAT C2 servers were the United States, Germany, Greece, China, and Japan. This broad utilisation of infrastructure can be linked to campaigns targeting well-reported regions such as Asia and the United States with Gh0stRAT variants. In 2024, regional Gh0stRAT activity was characterised by diverse deployment methods and targeted campaigns.

**Ghost RAT C2 Global Distribution**




Phishing emails and drive-by downloads, including a fake Google Chrome site targeting Chinese speakers, remain primary infection vectors. The emergence of new loaders like UULoader has enabled the delivery of Gh0stRAT and Mimikatz to Korean and Chinese speakers. We also observed the exploitation of software vulnerabilities, such as a vulnerable Windows driver delivering HiddenGh0st. Targets range from individual users to specific organisations, notably US entities involved in Artificial Intelligence (AI), targeted by the SugarGh0st variant.

# Adversary Infrastructure Tracking

## Quasar & Async RAT

By the end of 2024, QuasarRAT and AsyncRAT infrastructure ranked highest amongst RATs tracked by Bridewell. The first half of 2024 witnessed a substantial deployment of QuasarRAT, evidenced by its ranking as the ninth most frequently encountered malware family globally during the first two quarters.

Throughout the year, specific threat actors were identified utilising QuasarRAT in their operations. In January 2024, the threat group known as UAC-0050 once again focused its attacks on Ukraine, incorporating QuasarRAT into its arsenal alongside other tools like RemcosRAT and Remote Utilities.

Blind Eagle APT group directed its attention towards the Colombian insurance sector starting in June 2024, utilising a customised version of QuasarRAT dubbed BlotchyQuasar. Towards the end of 2024, a notable shift in attack vectors was observed with the exploitation of a severe PHP vulnerability, identified as CVE-2024-4577, to deploy QuasarRAT.

**Quasar RAT Global Distribution**


Much like Gh0stRAT infrastructure, QuasarRAT and AsyncRAT servers were broadly distributed however, there was notably very little presence within regions such as China for either RAT. We observed the majority of Quasar C2 servers in the United States, France and the United Kingdom at the beginning of 2024. However, by the end of 2024, the majority share of servers were hosted in Saudi Arabia, Hong Kong, Germany, and Mauritius demonstrating the fluctuating distribution of this malware.

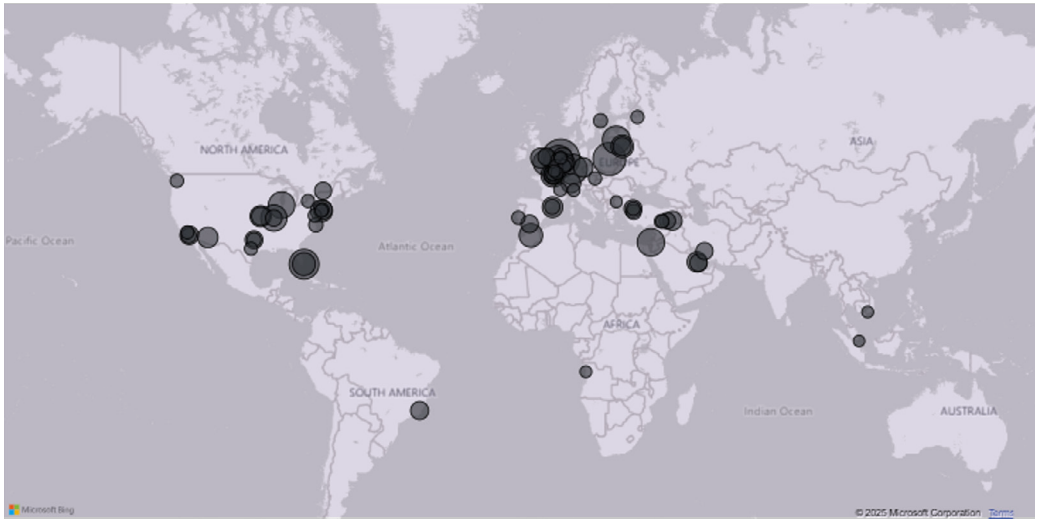
# Adversary Infrastructure Tracking

Similar to QuasarRAT, AsyncRAT maintained its position as a leading RAT throughout 2024. Its presence was noted in cyber incidents targeting a diverse array of sectors, including industrials, technology, financials, and healthcare. This broad targeting scope underscores its versatility and appeal to various threat actors with differing objectives.

AsyncRAT was commonly observed being delivered in conjunction with other RATs and information stealers, including XWormRAT, VenomRAT, and Vjw0rm. Due to its open-source nature and ease of use, AsyncRAT was observed being employed by a wide spectrum of threat actors, ranging from sophisticated Advanced Persistent Threat (APT) groups to less experienced cyber criminals.

The geographical picture looked similar for AsyncRAT, whereby the top three countries appeared in our data. However, by the end of 2024, we observed servers mostly located in Poland and Türkiye alongside the United States. The most identifiable difference between these two RATs was that we didn't observe a single C2 server belonging to AsyncRAT hosted in China, which demonstrates a clear preference for threat actors in that region.

**ASync RAT Global Distribution**




> "Similar to QuasarRAT, AsyncRAT maintained its position as a leading RAT throughout 2024."

# Adversary Infrastructure Tracking

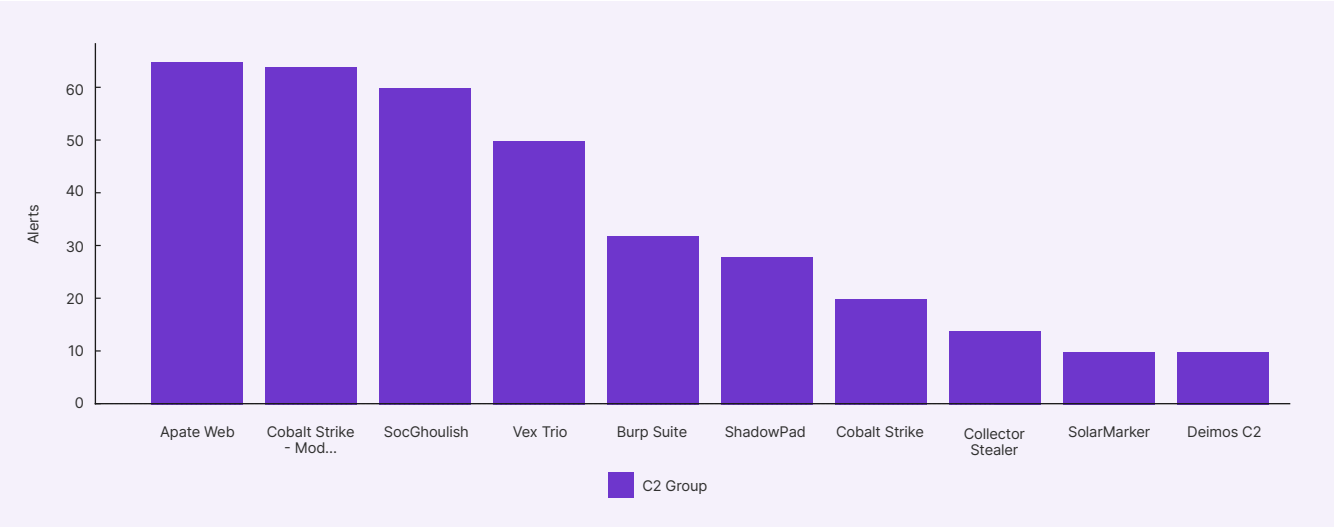
## CNI SOC/ MDR Service Detection Analysis

We use our malicious infrastructure tracking dataset to enable our managed detection and response (MDR) customers to prevent and detect threats. The following sections provide insights into the C2 detection alerts we observed within our customers' environments. The chart displays the top 10 C2 threat alerts we observed in client environments in 2024.

### Top Five Alerts

The most prominent C2 alert we observed in clients was for ApateWeb - a network made up of thousands of domains containing embedded JavaScript redirectors that are used to deliver the victims to pages containing scams, scareware, and potentially unwanted programs (PUPs).

A close second was Cobalt Strike Mod-Rewrite C2 alerts that detect cobalt strike servers that have deployed a layer of obfuscation using traffic redirection that will only send valid traffic to the C2 server, redirecting invalid traffic to a predefined destination (e.g. example.com). This improves the operational security (OPSEC) of the threat actor's infastructure, thereby reducing the likelihood of detection.



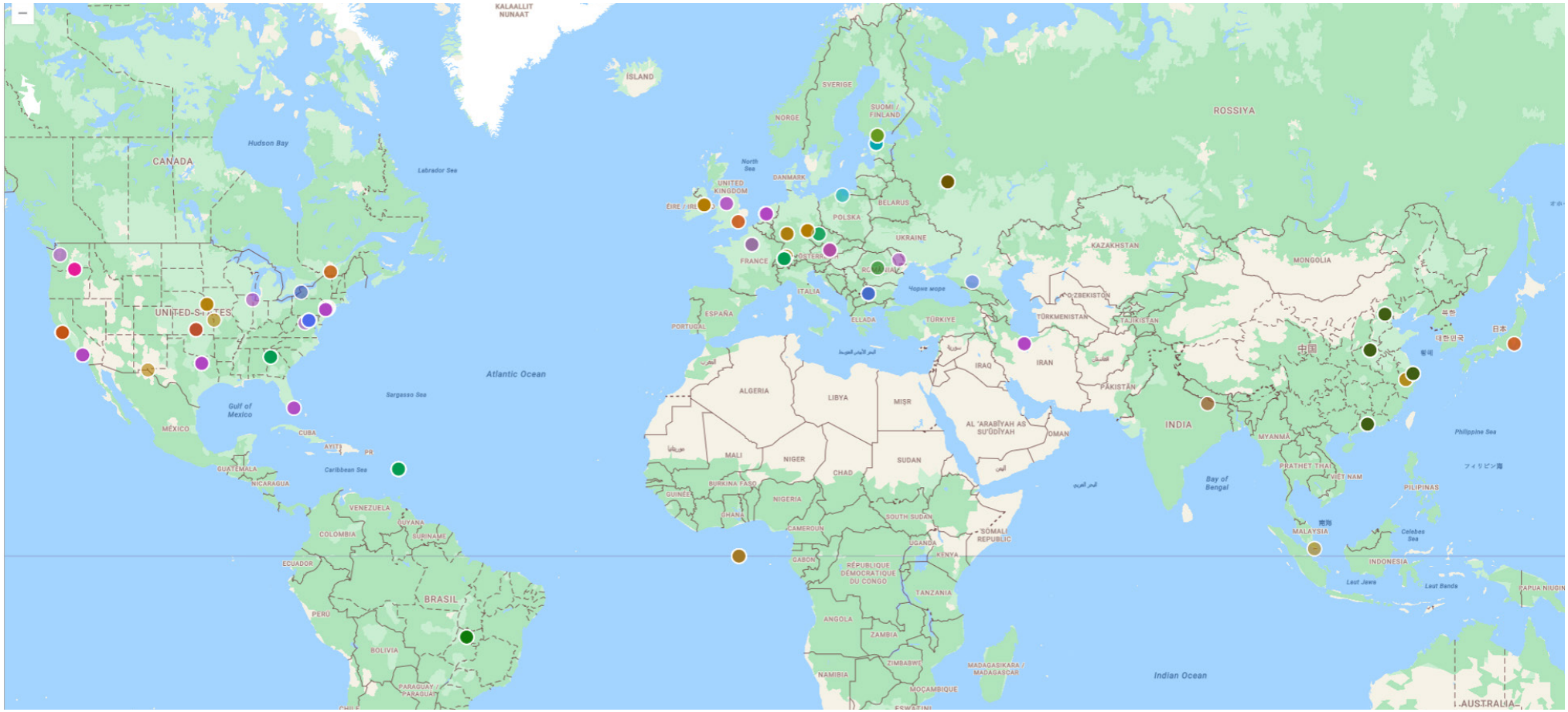

Third in the list was SocGholish/SocGhoulish infrastructure that masquerades as legitimate software in fake updates campaigns. This malware has been linked to TA505 (EvilCorp, Indrik Spider).

Fourth was VexTrio, a criminal enterprise providing traffic distribution system (TDS) services. A TDS is a complex network of servers that profile victim browsers and then redirect them to malware, scams, or illegal content. VexTrio also leverage lookalike domains, and registered domain generation algorithms (RDGAs) as part of their services.

To finish our top five observed alerts, we identified Burp Collaborator C2 servers. Burp Collaborator provides custom implementations of various network services on a single server. The server listens for requests that are induced by Collaborator payloads.

# Adversary Infrastructure Tracking

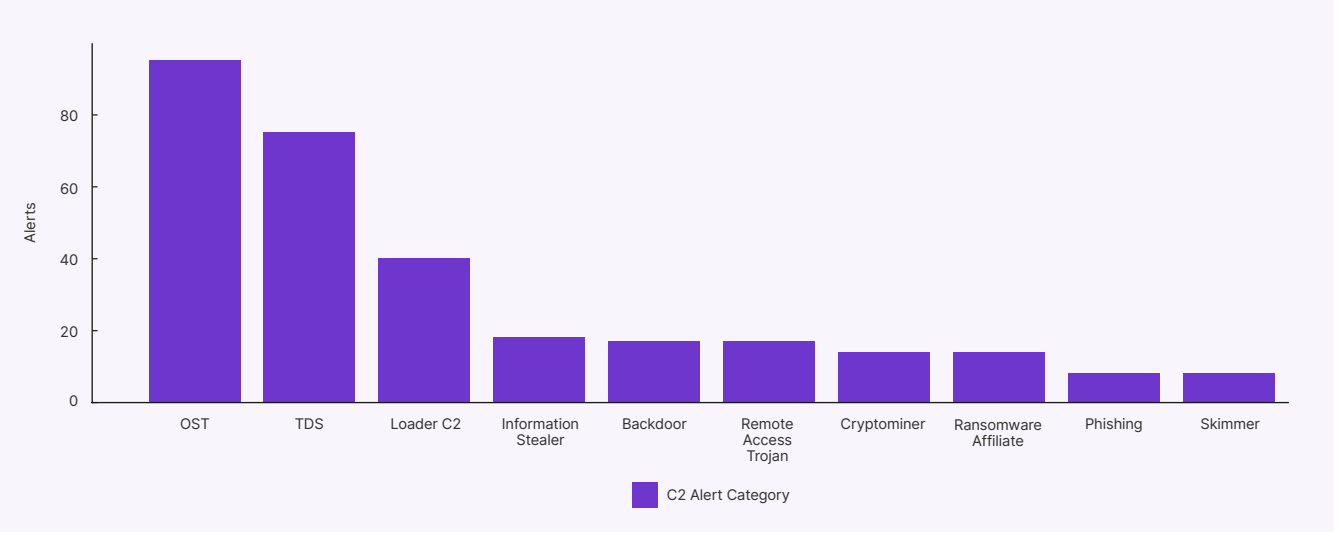
## C2 Alert Geolocations



# Adversary Infrastructure Tracking

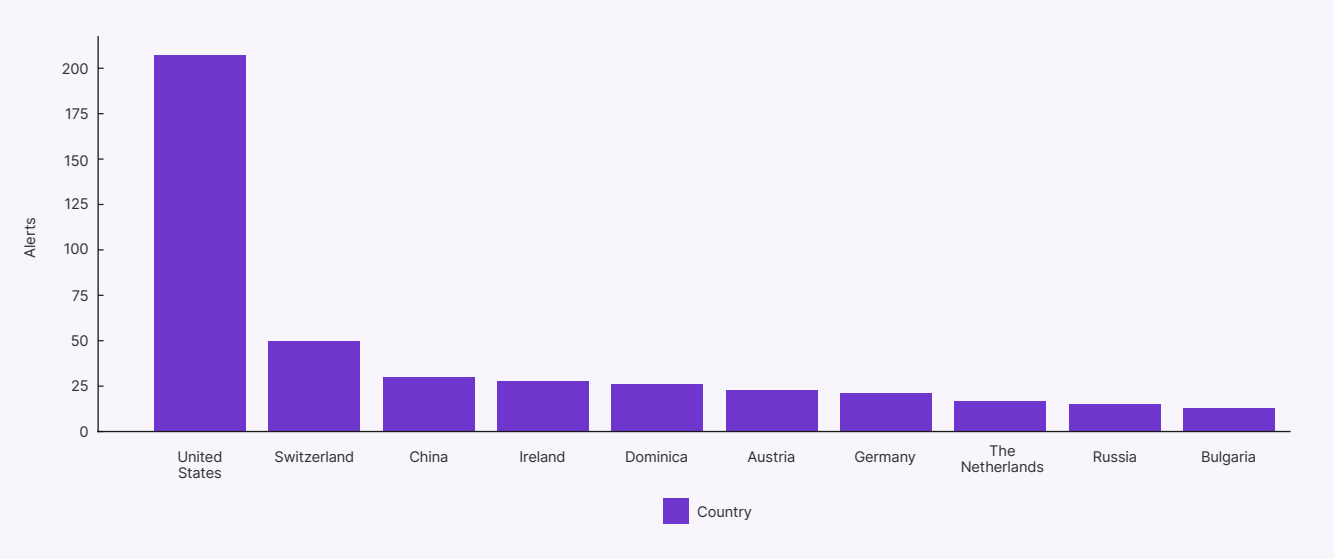
## Top C2 Alert Categories

The graph details the distribution of C2 alert categories, with OST (Offensive Security Tool) and TDS (Traffic Distribution System) exhibiting the highest frequency of alerts, indicating them as the most prevalent infrastructure types observed within our client environments. This aligns with the findings from our previous report, with the most prevalent C2 types consisting of post-exploitation tools and penetration testing utilities, such as Cobalt Strike, Sliver, and Metasploit.




## Top C2 Alert Countries

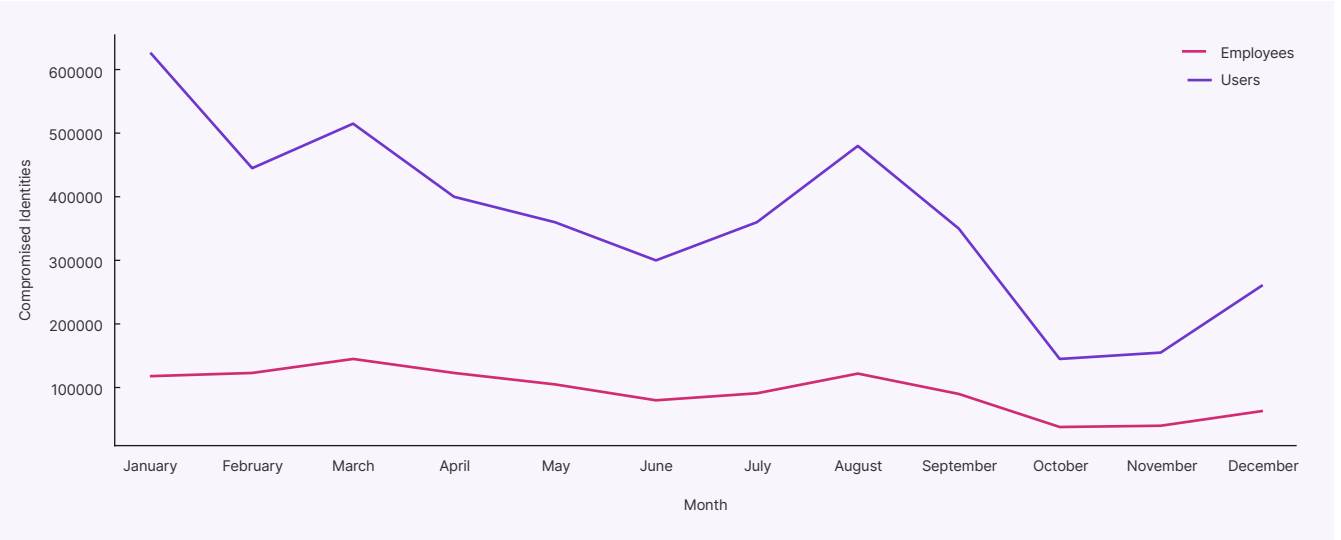
The chart illustrates the top countries associated with C2 server alerts, revealing the United States as the predominant source of these alerts, followed by Switzerland and China. Interestingly, we identified both the United States and China as the top geographic locations hosting C2 servers in 2023.



# Information Stealer Landscape

In 2024, we focused extensively on tracking and analysing the evolving threat of information stealers, which remain a key enabler of cyber crime. Through proprietary intelligence gathering, we have identified trends in how info stealers are deployed, the industries most affected, and the role these threats play in facilitating further attacks such as ransomware.

By monitoring emerging stealer variants and compromised credentials, we have helped organisations proactively defend against credential theft and unauthorised access. The following analysis explores the information stealer landscape, highlighting major malware families, compromise trends and impact.




## Global Information Stealer Landscape

### Rising Trends in Information stealer Compromises

The data for 2024 highlights a fluctuating but persistent volume of global compromises linked to information stealers. The year began with a peak in January, recording over 620,000 incidents. This surge can be attributed to cyber criminals exploiting the post-holiday period, targeting individuals and organisations adjusting back to regular operations. This is a time when awareness may be reduced, making them more susceptible to phishing campaigns and malware infections.

Following this peak, a gradual decline in incidents was observed through mid-year. This downturn aligns with several significant law enforcement operations aimed at disrupting cyber criminal infrastructure.

### Enforcement Action

**Operation Endgame (May-June 2024):** This large international operation targeted over 100 servers used by major malware loader operations like **IcedID, Pikabot, Trickbot, Bumblebee, and Smokeloader.** These loaders are frequently used to deploy various types of malware, including information stealers, onto victim systems. Disrupting their infrastructure makes it harder for threat actors to deliver information stealers.

**Operation First Light (May – June 2024):** A global effort involving 61 countries led to the arrest of approximately 3,950 individuals involved in various online scams, including those distributing information stealers. This operation also resulted in the freezing of 6,475 bank accounts and the seizure of $257 million in illicit assets, thereby disrupting numerous cyber criminals' networks.

**Operation Magnus (October 2024):** This was a

# Information Stealer Landscape

significant international operation led by the Dutch National Police, with support from the Federal Bureau of Investigation (FBI) and other agencies of the US, the National Crime Agency (NCA) in the UK, Belgian Federal Police, Portuguese Federal Police (Polícia Judiciária), and Australian Federal Police (AFP). It successfully dismantled the infrastructure of **Redline Stealer** and **MetaStealer**, two widely used information stealers.

- Servers in the Netherlands used to run the malware were shut down.
- Domains associated with the stealers were seized.
- A database of thousands of clients (cyber criminals using the malware) was retrieved.
- One alleged administrator was charged in the US, and two individuals were arrested in Belgium.
- Telegram channels used to distribute the information stealers were taken offline.
- This operation directly impacted the ability of cyber criminals to deploy these specific stealers and access stolen data from existing infections.

Despite these enforcement actions, a resurgence in information stealer incidents occurred in August, with **480,453** incidents reported. Towards the end of the year, another notable increase in incidents was observed, with **260,670** incidents reported in December.

This cyclical pattern underscores the adaptive strategies of threat actors, who continuously evolve their tactics in response to law enforcement actions and the cyber security community's defensive measures. The mid-year decline reflects the temporary success of global crackdowns, while subsequent resurgences highlight the resilience and resourcefulness of cyber criminal networks in restoring and innovating within their operations.

> **"Towards the end of the year, another notable increase in incidents was observed, with 260,670 incidents reported in December."**

# Information Stealer Landscape

## UK Information Stealer Landscape

The following data comes from our information stealer intelligence provider Hudson Rock which provides a different data set than seen in our infrastructure tracking capability.

### Understanding the Threat to UK Organisations

Our intelligence analysis throughout 2024 has identified a persistent and evolving threat from information stealers targeting UK organisations. These malware families continue to be a key enabler of cyber crime with attackers leveraging them to steal credentials, financial information, and sensitive corporate data. Our monitoring of client environments has provided unique insight into the most active information stealer strains affecting the UK, allowing us to track their prevalence and impact more accurately. The following analysis is based on real-world intelligence gathered from UK clients, providing a representation of the wider UK Information stealer threat landscape.

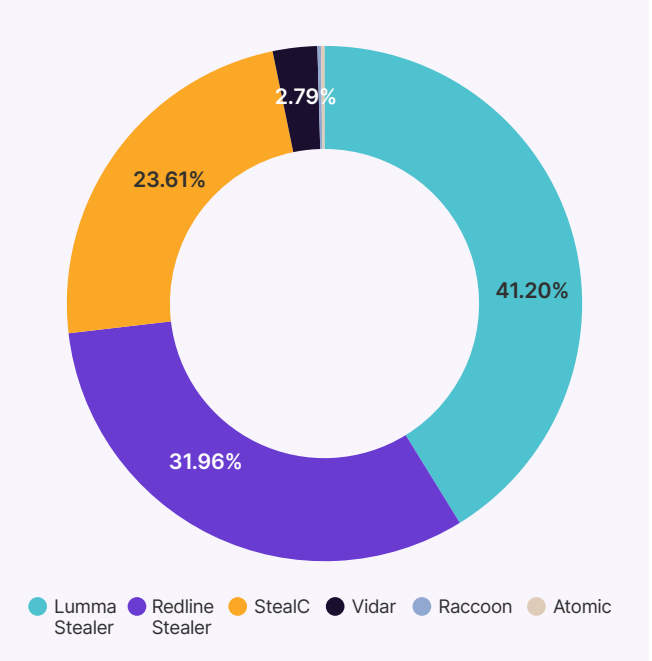
### Dominance of Lumma Stealer and Redline Stealer in UK-Based Attacks

Our analysis shows that Lumma Stealer **(41.2%)** and Redline Stealer **(31.96%)** account for the majority of information stealer infections in UK environments, making them the most dominant malware families in this space.

Lumma Stealer has rapidly grown in prominence due to its ease of deployment and evolving capabilities. Available as a Malware-as-a-Service (MaaS), it is frequently delivered through phishing campaigns, malicious downloads, and compromised websites. Its ability to exfiltrate credentials, session tokens and autofill data makes it a valuable tool for cyber criminals engaging in financial fraud and account takeovers.

Redline Stealer, despite being one of the longest standing information stealers, remains a widely used tool among cyber criminals. Its affordability, versatility, and strong foothold in underground markets continue to drive its widespread use, particularly against UK businesses across finance, retail, and legal sectors.

**Stealer families affecting the UK 2024**



# Information Stealer Landscape

## The Continued Threat of StealC and Emerging Variants

StealC (23.61%) remains a significant player within the UK information stealer landscape. Often deployed as part of a multistage infection chain, it is increasingly used for credential theft and establishing an initial foothold prior to further compromise.

In contrast, Raccoon Stealer activity has significantly decreased now accounting for just 0.29% of UK based information stealer infections. Our internal C2 tracking confirms a steady decline in Raccoon Stealer infrastructure and operational activity throughout 2024, despite a brief resurgence earlier in the year.

Also present, though in lower volumes, are Vidar and Atomic which continue to be used opportunistically in UK-targeted campaigns often as broader MaaS or Initial Access as a Service offerings.

**“StealC (23.61%) remains a significant player within the UK information stealer landscape.”**

# Information Stealer Landscape

## Information Stealers and RaaS Ecosystem

Throughout 2024, we have observed a growing overlap between ransomware-as-a-service (RaaS) operations and information stealer malware. While ransomware groups have traditionally relied on phishing, remote exploits, and initial access brokers to gain entry into networks, the increasing use of information stealers highlights a shift in tactics.

These malware strains enable attackers to harvest credentials, session tokens, and sensitive corporate data, which can then be leveraged to gain access to organisations before deploying ransomware.

To better understand this relationship, we conducted an intelligence-driven analysis, marrying up ransomware breach data with information stealer infections to determine which stealers are most linked to ransomware attacks and how different ransomware groups utilise them.

“These malware strains enable attackers to harvest credentials, session tokens, and sensitive corporate data.”

# Information Stealer Landscape

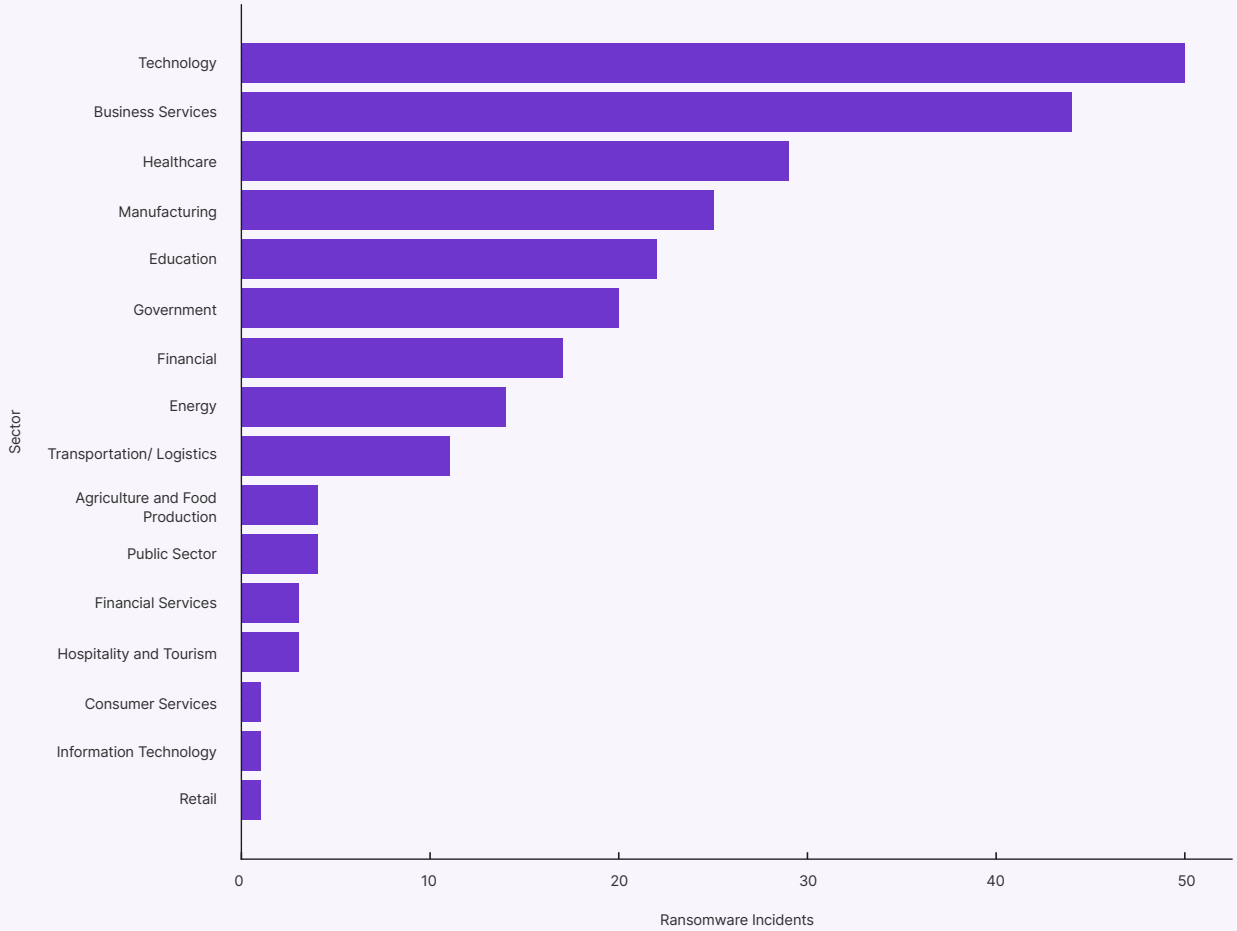
## Ransomware Incidents Involving Information Stealers (2024)

The following section provides insights and figures to illustrate how information stealers have contributed to ransomware incidents across different sectors and regions in 2024.

The first graph shows a breakdown of ransomware incidents linked to information stealers across various industries. The technology sector (20.08%) is the most frequently targeted, followed closely by business services (17.67%) and healthcare (11.65%). These industries store valuable credentials and sensitive client data, making them prime targets for credential-harvesting malware before ransomware deployment.

> **The technology sector is the most frequently targeted, followed closely by business services and healthcare.**

**Sectors 2024**



# Information Stealer Landscape

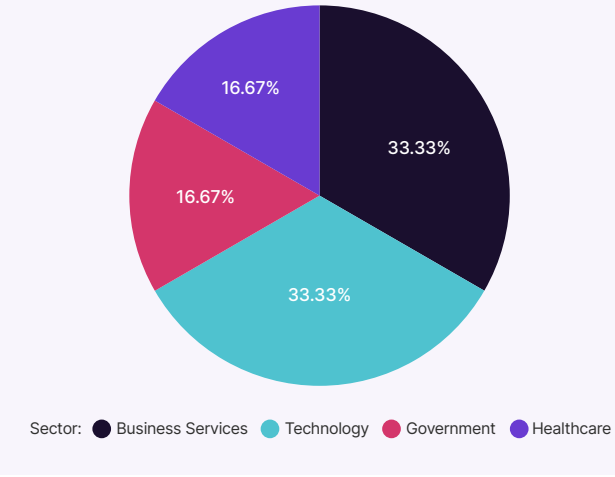
Figure 1 highlights that business services, technology, government, and healthcare were the most affected sectors in the UK. This aligns with broader cyber crime trends where attackers prioritise sectors with a high volume of sensitive records and operational dependencies.

Figure 2 (CNI-related ransomware incidents) shows that Raccoon and StealC were the most common information stealers in ransomware cases affecting CNI. This suggests that threat actors targeting CNI may be leveraging compromised credentials obtained through information stealers before executing ransomware payloads.

Figure 3 reveals that UK government and healthcare sectors were disproportionately affected by ransomware campaigns involving information stealers. Given the reliance on third-party vendors, extensive supply chains, and large data repositories, these sectors remain highly attractive targets for cyber criminals.

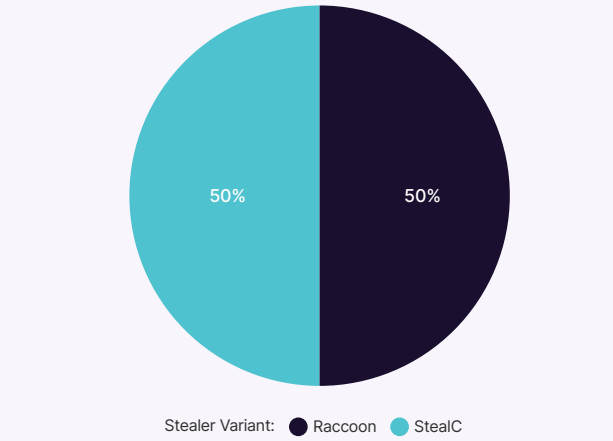
### Information Stealers Affecting UK 2024

Figure 1



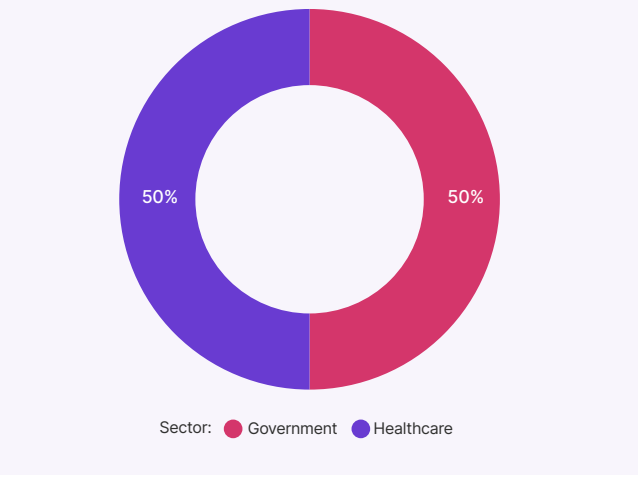

### Ransomware Incidents UK CNI 2024

Figure 2




### UK Sectors Affected by Ransomware involving Information Stealers 2024

Figure 3



# Information Stealer Landscape

## Usage of Information Stealers Across Incidents (2024)

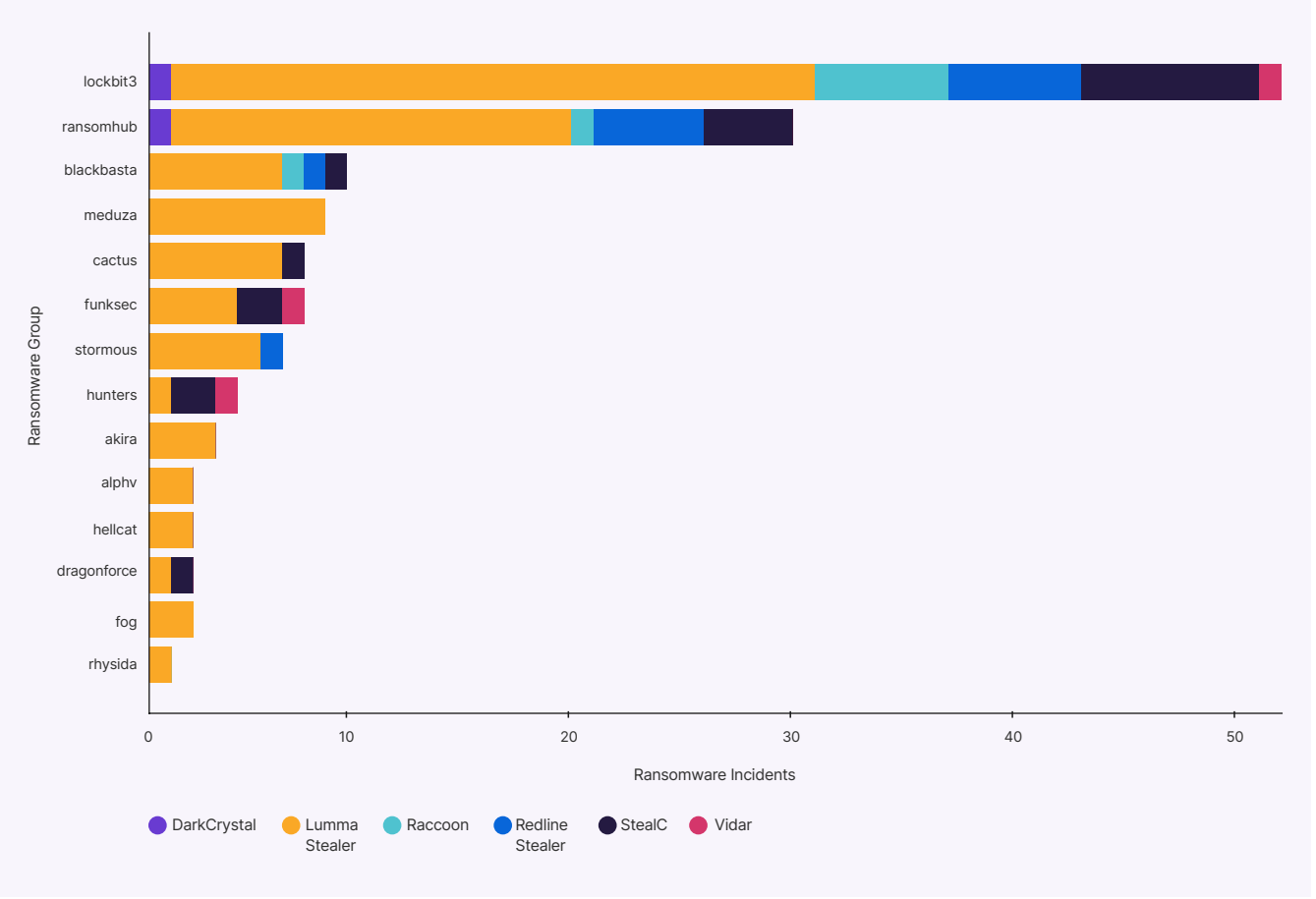
This bar chart provides insight into which ransomware groups have been actively using information stealers as part of their attack chain.

LockBit3 and RansomHub are the most prolific users of information stealers, incorporating strains such as Lumma Stealer, Raccoon, and Redline Stealer into their infection process.

BlackBasta and Meduza Stealer also show strong associations with Lumma Stealer and StealC, indicating that these groups have deep ties to information stealer-based credential harvesting.

The diversity of stealers across different ransomware groups suggests that cyber criminals purchase stolen credentials from various underground sources, rather than relying on a single supplier. The inclusion of Vidar and DarkCrystal among certain ransomware groups suggests that some attackers are experimenting with less commonly detected stealers, potentially to evade security solutions that focus on more well-known strains.

**Ransomware Groups Usage of Information Stealers Across Incidents 2024**



# Information Stealer Landscape

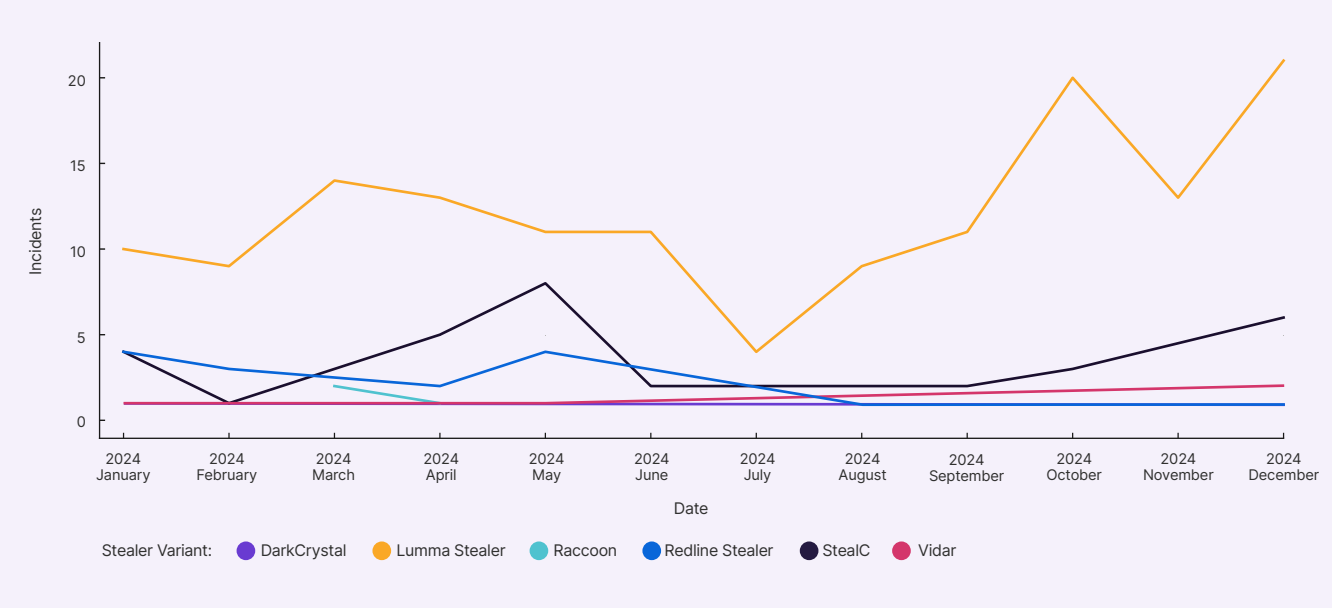
## Information Stealers Used Across Ransomware Incidents (2024)

The timeline chart (right) tracks how the use of different information stealers has evolved in ransomware incidents throughout 2024.

Lumma Stealer saw a major surge in Q3 and Q4, culminating in its highest activity levels in November to December 2024. This suggests that Lumma Stealer has become the information stealer of choice for ransomware operators, likely due to evasive capabilities, ease of deployment, and underground market availability.
Redline Stealer maintained a steady presence throughout the year, reflecting its continued popularity among cyber criminals for credential harvesting.
Raccoon Stealer saw moderate fluctuations, with peaks in May and September, potentially linked to seasonal phishing campaigns and increased dark web sales of stolen credentials.

StealC and Vidar showed lower but consistent usage, suggesting they are primarily used in targeted attacks rather than widespread campaigns.

**Information Stealers Used Across Ransomware Incidents 2024**




## Information Stealer Key Takeaways

Our analysis of information stealer activity highlights the growing threat these malware families pose across global, UK, and CNI sectors. Our research underscores the scale of credential theft, the evolving tactics used by cyber criminals, and the direct risks to organisations reliant on strong identity security.

# Research

In this section, we'll cover three research topics which have persisted through 2024 which we predict with high-moderate confidence will become more prevalent into 2025. These topics include two ongoing trends phishing kits and techniques and EDRKillers, along with an emerging trend: fog ransomware.

## Phishing Kits and Techniques

### Introduction

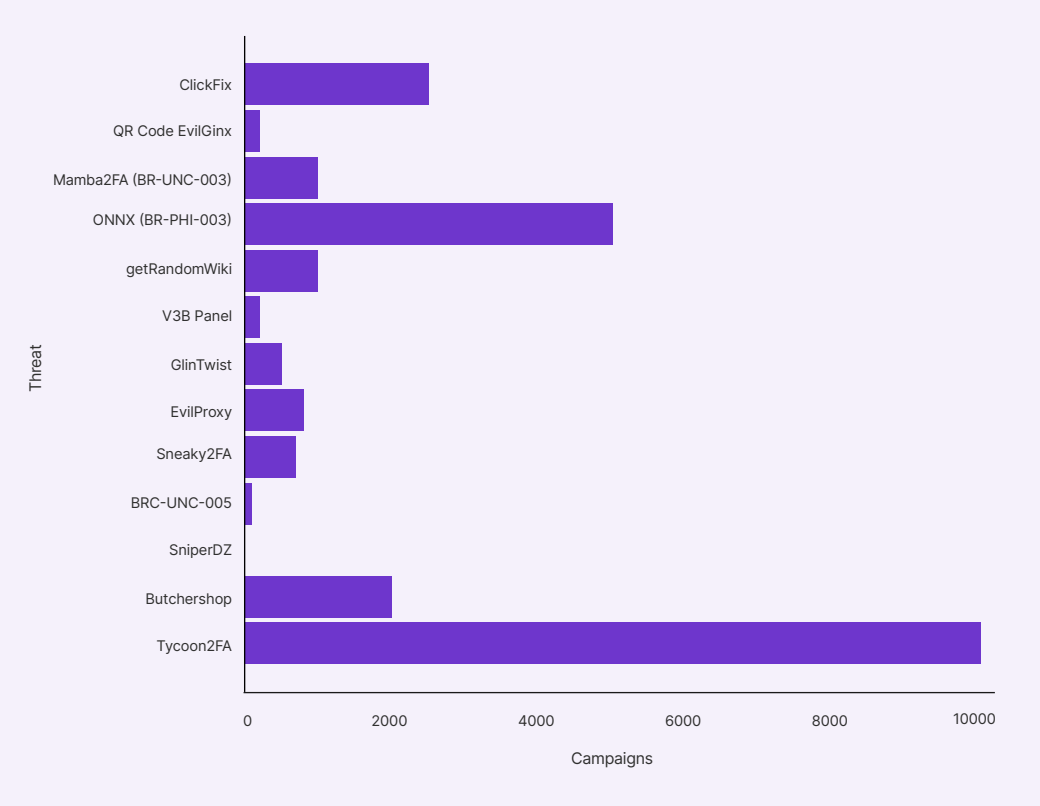
Phishing remains a highly lucrative threat, as seen by the adoption of multiple new phishing kits and phishing techniques in 2024.

2FA has dominated the adversary-in-the-middle (AiTM) space. The phishing kit has led to thousands of ongoing campaigns targeting Microsoft 365 and bypassing Gmail accounts. These stolen cookies enable attackers to circumvent multi-factor authentication (MFA), leading to unauthorised access of a user's accounts, systems, and cloud services, effectively negating even layered security defences.

### ClickFix

Of particular importance is ClickFix, a highly industrious technique favoured by numerous threat actor types and currently being adopted at an accelerated rate. It is now directly responsible for facilitating diverse motive initial access operations on a global scale.

**Key Social Engineering Techniques in 2024**




Our analysis in 2024 revealed the use of it in intrusions by three highly developed nation-state APT groups. Our assessment is that its highly likely that this will become a readily deployable social engineering strategy for threat actors of all sizes throughout the rest of 2025, and we strongly anticipate increased adoption and attack volume.

# Research

## ClickFix

ClickFix is a phishing technique used by multiple threat groups to socially engineer users into running malicious scripts on their machines. ClickFix deceives users into directly downloading and running malware, avoiding web browser involvement in the download process and eliminating the need for manual file execution, thereby bypassing web security and appearing less suspicious.

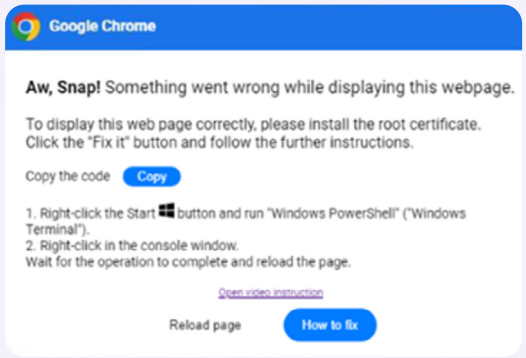
First tracked in the community in early 2024, it remained a steady threat in 2024 with large spikes into early 2025. However, this is not the true picture of threat actor adoption as this shifted many times from a few dedicated cyber crime groups to global cyber criminal activity and even nation-state APTs.

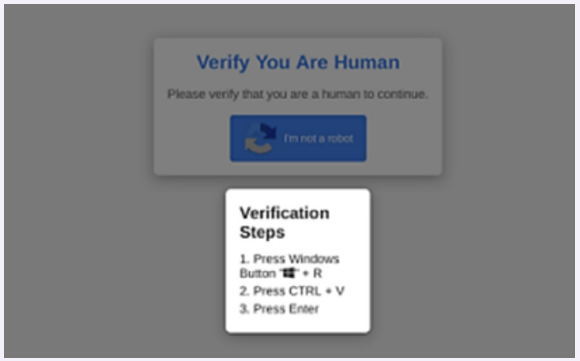
**ClickFix campaigns**

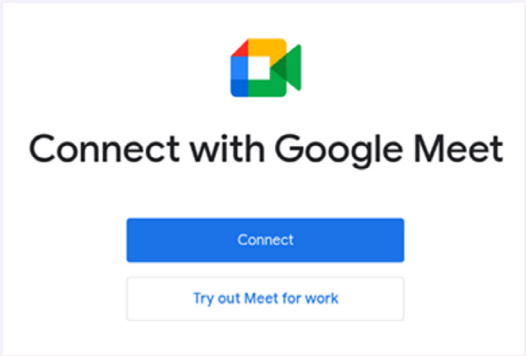

> **ClickFix deceives users into directly downloading and running malware.**

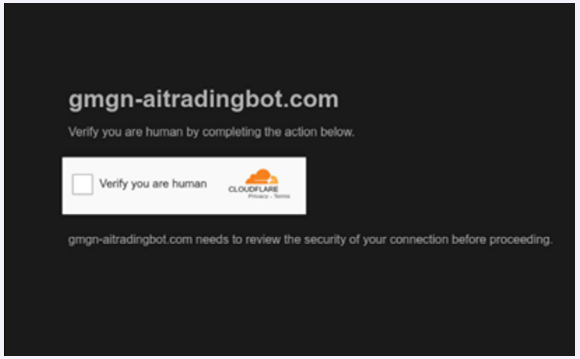
# Research

There have been many variations so far of this technique, beginning with fake errors within a Word document to fake CAPTCHA within Cloudflare. Whilst there has been a spread of diverse targeting such as utilising fake browser alerts, we have also seen groups using this highly successful lure to go after specific sectors and customers such as the transportation sector and booking.com.



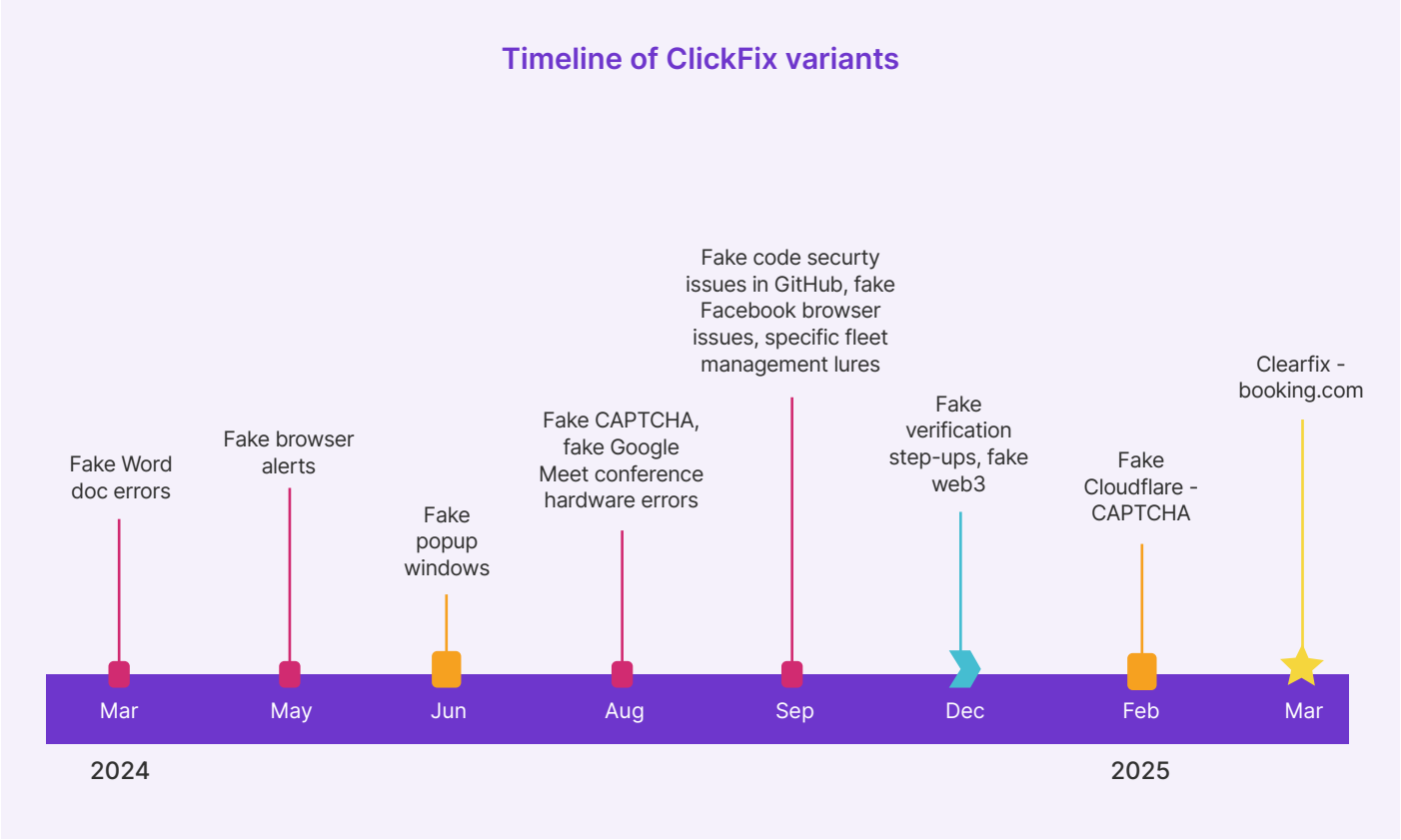




"We have also seen groups using this highly successful lure to go after specific sectors and customers such as the transportation sector and booking.com."

# Research

Below showcases a timeline into the specific variants over the year period from March 2024-March 2025.



# Research

## Notable Events in ClickFix Variants

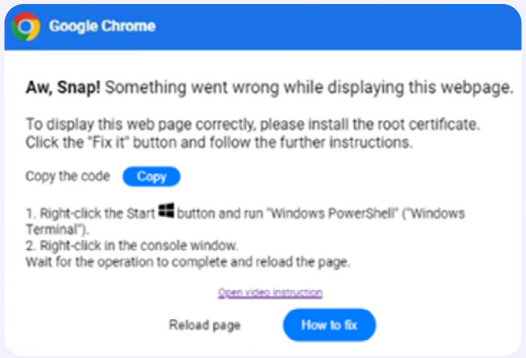
In March 2024, TA571 executed phishing campaigns with HTML attachments designed to appear as Microsoft Word documents. These attachments displayed deceptive error messages to lure users into copying and running malicious PowerShell code that deployed malware. May 2024 saw a threat actor named ClearFake adopt a new social engineering scheme, ClickFix, to trick users into running malicious PowerShell via fake web browser alert pop-ups on compromised websites.

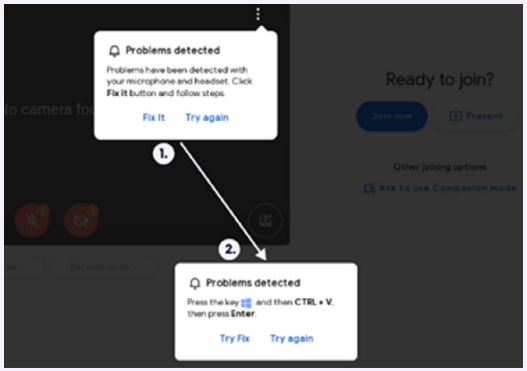
August 2024 had ClickFix operating within a large infrastructure of fake CAPTCHA webpages to deliver payloads, with redirection occurring from malicious distribution networks, including fake cracked software websites.

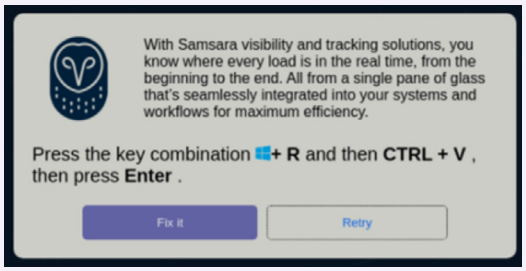
September 2024 found ClickFix being used against North American transport/ logistics, specifically impersonating transport and fleet management software like Samsara, AMB Logistic, and Astra Transport Management Software (TMS) to deliver malware (Lumma Stealer initially, later DanaBot). Users inadvertently ran malicious PowerShell after trying to fix software errors.

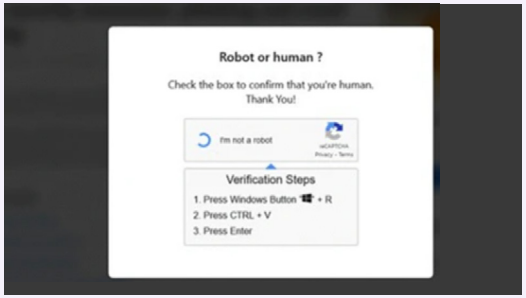
During March 2025, Storm-1865 specifically used ClickFix against booking.com customers using fake CAPTCHA. The command downloaded and launched malicious code through mshta.exe.

Originally being utilised in cyber crime with TA571, we have seen a much wider adoption by nation-state groups such as MuddyWater (Iran), APT28 (Russia), and DPRK intrusion sets namely Contagious Interview and Kimsuky. ClickFix also continues to be persistently used across information stealers. We are yet to see this play out with ransomware intrusions at this time, which we believe is a natural avenue for delivery with or without the use of initial access brokers.



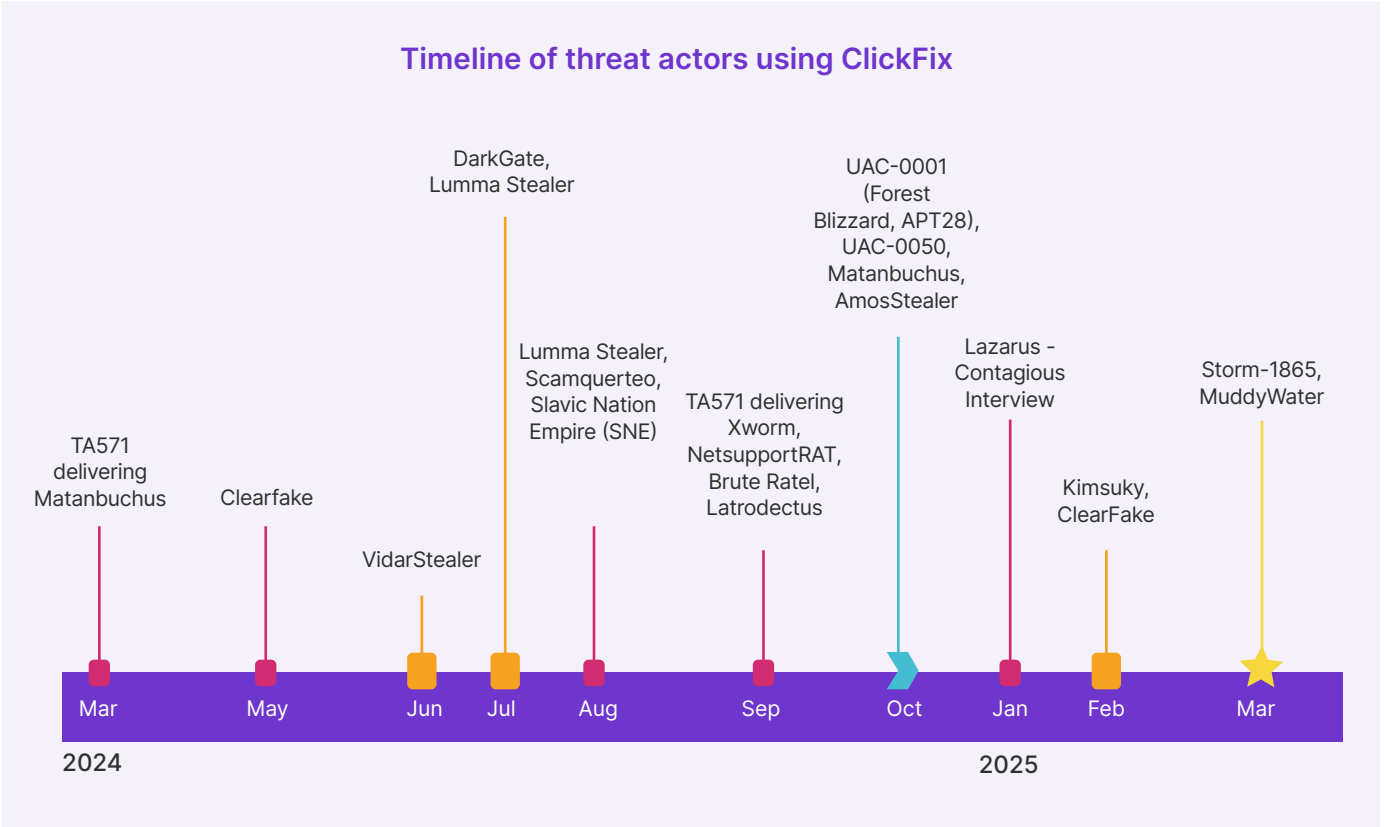



# Research

It should also be highlighted that MuddyWater has previously deployed ransomware with other destructive attacks and may begin to use it more regularly. Moonstone Sleet, a DPRK-nexus group who was observed deploying ransomware in 2024, shares several techniques with Contagious Interview campaigns. With the shared tooling and infrastructure overlaps in North Korea, there may be adjacent groups to Contagious Interview beginning to implement ClickFix as well.





**“It should also be highlighted that MuddyWater has previously deployed ransomware with other destructive attacks and may begin to use it more regularly.”**

# Research

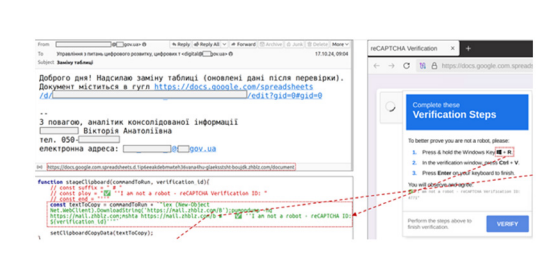
## Notable Threat Actors using ClickFix

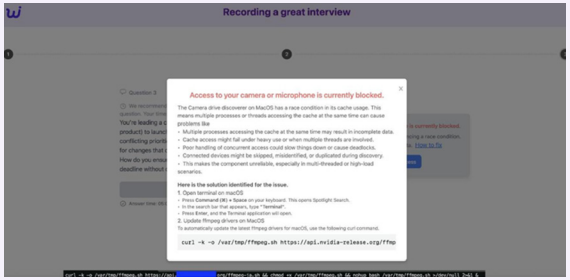
In October 2024, UAC-0001 (APT28, Forest Blizzard) targeted the Ukrainian government mimicking a Google spreadsheet.

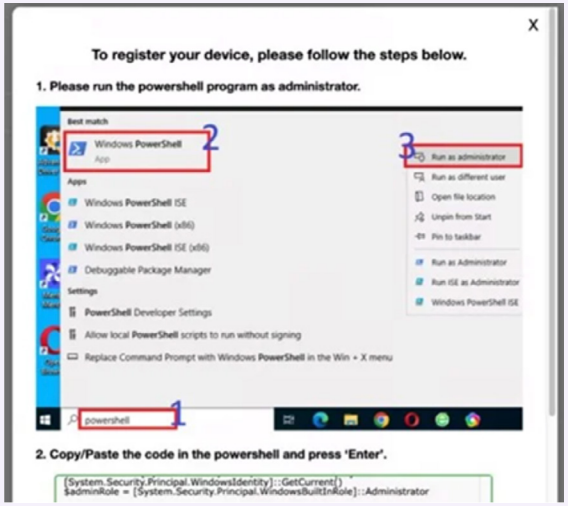
January 2025 saw ClickFix being used via Lazarus's established Contagious Interview operation. This involved inviting candidates to a fake Willo Video Interview where they attempted to execute code on the users' machines under the guise of fixing a falsely blocked camera/ microphone by the web application.

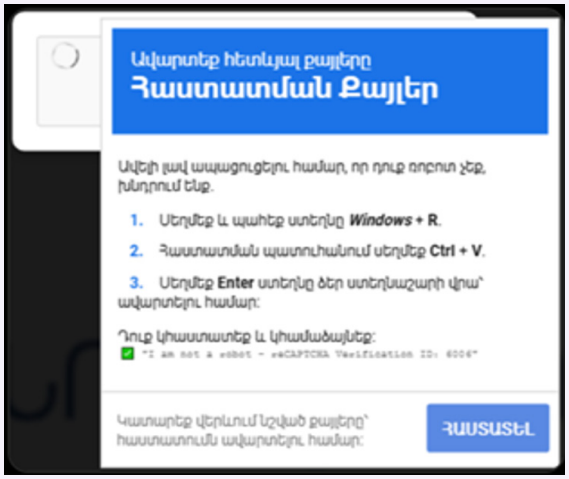
February 2025 had Kimsuky (Emerald Sleet, VELVET CHOLLIMA) pretending to be South Korean government officials. The group were attempting to have victims open up Powershell terminals as an administrator to download a remote desktop tool for data exfiltration.

Finally, in March 2025, MuddyWater (Mango Sandstorm) were seen to be using ClickFix targeting the Armenian Police website delivering RMM tools.



## EDRKillers, and EDRKillShifter

### Introduction

EDRKillers are advanced tools that aim to subvert detection and disable Endpoint Detection and Response (EDR) capabilities. They have in particularly become a trend in ransomware operations such as Ransomhub, AvosLocker, BlackCat, LockBit, Royal Ransomware, Meduza Stealer, BlackByte, and Circada3301, with EDRKillers becoming more available through the RaaS ecosystem.

EDRKillers achieve their goals by exploiting vulnerable drivers, manipulating Windows Filtering Platform (WFP), and altering kernel structures. Techniques such as NT Layer Dynamic Link Library (NTDLL) unhooking and system call (syscall) manipulation pose a serious threat to allowing undetected malware to run.

In 2024, we saw wider adoption of dedicated sophisticated EDRKillers such as AVNeutralizer (AuKill), EDRKillShifter, EDRSandBlast, EDRSilencer, MS4Killer, and Disabler.

Other less advanced toolsets are also still being used across ransomware attacks like Defender Controller and Universal Virus Sniffer. We are also continuing to see legitimate tools being installed such as HRSword, GMER, PowerTool and Process Hacker to force EDR process terminations.

As a result, EDRKillers can terminate/ manipulate EDR processes, facilitate ransomware deployment and ultimately prevent alerts from reaching security administrators resulting in undetected attacks.

### Adoption

Throughout 2024, threat actors increasingly adopted diverse EDR disabling tools. In January, Mimic Ransomware deployed Defender Controller. February saw a surge in activity, with Phobos Ransomware utilising Process Hacker, Universal Virus Sniffer, and PowerTool, alongside ALPHV ransomware employing POORTRY and STONESTOP to terminate security processes.

By April, Masscan Ransomware was observed using HRSword. May marked a significant shift, with BlackByte ransomware operators loading a bespoke vulnerable driver —RtCore64.sys— during intrusions. This exemplified the broader Bring-Your-Own-Vulnerable-Driver (BYOVD) technique, a Living-Off-The-Land (LOTL) tactic favoured by many actors to evade detection by blending in with legitimate system behaviours.

July witnessed FIN7 marketing their AVNeutralizer (AuKill) tool on dark web forums, capable of inducing Denial-of-Service conditions that impeded vital EDR process calls. Notably, AvosLocker, BlackCat, LockBit, Royal Ransomware, Meduza Stealer, and BlackByte have all employed AVNeutralizer.

August saw the emergence of Ransomhub's EDRKillShifter, designed to deliver configurable vulnerable drivers. September saw Cicada3301 utilise EDRSandBlast, which exploits a signed, vulnerable driver to disable EDR and Local Security Authority Subsystem Service (LSASS) protections using both kernel and user-level evasion techniques.

October saw the abuse of EDRSilencer, a red team tool, to create WFP filters blocking outbound EDR traffic.

Simultaneously, Embargo Ransomware adopted MS4Killer, another BYOVD tool. November brought reports of an extortion group deploying "Disabler," an AV/EDR bypass tool with strong similarities to EDRSandBlast.

The rise of BYOVD, coupled with Ransomhub's 2024 dominance, makes EDRKillShifter the most substantial ransomware threat.

# Research

## EDRKillShifter

In August, Ransomhub, the most prevalent ransomware group of 2024, began utilising a new tool – EDRKillShifter. Despite starting operations in February, it was in August that they outlined their desire to be a global player and became the third most prolific group in 2024 at that time.

The group leveraged expertise from affiliates and operators in the marketplace, namely BlackCat/ALPHV, to enhance their intrusions. With this shared portfolio of knowledge, TTPs and capability from BlackCat/ALPHV and other groups, it was clear that they would not only get ahead of other groups, but become a leader who develop novel practices such as their highly successful EDRKillshifter tool.

## Technical Analysis

From Darkweb forums, we were able to view the targeted EDRs by EDRKillShifter. The list covered many common EDRs such as Crowdstrike, Microsoft Defender, TrendMicro and SentinelOne. The malware operates in three stages designed to first deliver and decrypt a malicious embedded resource, which is then executed in memory.

Following this, EDRKillShifter then drops the chosen, vulnerable but legitimate driver. Finally, it exploits the driver to gain higher privileges to unhook and disable the chosen EDR tool.

In Stage 1, the file unpacks and executes a malicious embedded resource directly into memory. Under inspection, the Portable Executable (PE) file contains unique data values such as Company Name: “ARK,” File description: “Loader Config,” and InternalName: “Loader.exe.” All samples require a 64-character based password passed to the commandline to execute into memory.

Spawned file events from the executable were observed, which we reviewed for detections. This logic was taken because there was a decryption routine which creates a file name config.ini, and other file events from this were expected.
In Stage 2, the driver drops. We identified that the EDRKillShifter drops a randomly named ‘.sys’ driver into ‘C:\Users\AppData\Local\Temp. We were also able to gather a list of known malicious vulnerable drivers. This allowed us to develop the driver dropping detection. We additionally added a competing rule for executions at the commandline for the “Killer” executable with parameters such as “-pass” containing drivers with the pattern matching expression that was discovered.

In Stage 3, the driver exploitation elevates privileges to disable the EDR. EDRKillShifter creates a new service on the victim host for the newly dropped driver and then starts the service to load the new driver. The malware then enters a loop which enumerates running processes and terminates them if the process name matches a list of hardcoded process names.

## Key Takeaways

Our analysis indicates a high probability of escalated EDRKiller deployment within ransomware operations, subsequent to observed successful intrusions worldwide. We further anticipate that BYOVD methodologies will represent a key trajectory for threat actors throughout the rest of 2025, facilitating broader exploitation.

# Research

## Rising Prospect: Fog Ransomware

### Introduction

While 2024 saw significant law enforcement victories against major cyber criminal operations, the emergence of Fog Ransomware underscores the persistent evolution of digital threats. Notable actions, including Operation Cronos against LockBit and the disruption of Warzone RAT infrastructure, demonstrated a concerted global effort to combat threat actor intrusion.

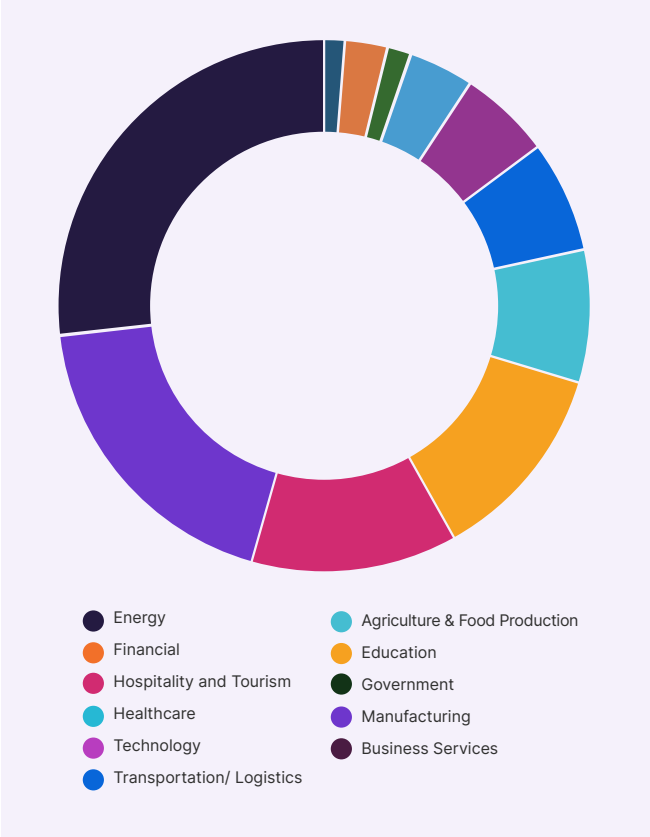
### Targeting and Broad TTPs

Fog ransomware has been observed targeting primarily US educational institutions, though broader victimology reveals attacks across business services, manufacturing, government, and education sectors.

This ransomware variant, a member of the STOP/DJVU family first identified in November 2021, exhibits notable similarities to Akira ransomware. Specifically, shared infrastructure, overlapping tactics, techniques, and procedures (TTPs), and similar initial access methods have been observed.

Given Akira's significant activity and ranking as a top 5 ransomware threat in 2024, the emergence of Fog was closely monitored.

**Fog ransomware count by sectors**




> "While 2024 saw significant law enforcement victories against major cyber criminal operations, the emergence of Fog ransomware underscores the persistent evolution of digital threats."

# Research

Further analysis reveals a connection between Fog affiliates and Storm-0844, a known Akira ransomware affiliate. This connection suggests a shared infection chain, with initial access commonly achieved through the exploitation of VPN vulnerabilities and the use of valid credentials.

The targeting of educational institutions likely stems from their perceived vulnerabilities, including limited cyber security budgets and the potential for high-value data exfiltration. However, victimology indicates a wider reach, with business services, manufacturing, and government also heavily targeted.

Geographically, 50% of attacks targeted the USA, with Germany next at approximately 10%. The rapid evolution of ransomware groups, and the sharing of TTPs, highlights a rise in the enterprise of cyber crime, affiliate programs, and ransomware as a service (RaaS).

Observed post-exploitation activities include the use of common exploitation frameworks such as Metasploit and Cobalt Strike, alongside legitimate remote access tools like AnyDesk and SplashTop. Data exfiltration is conducted using tools such as Rclone and cloud storage platforms like Mega and FileZilla. To hinder recovery efforts, defence evasion techniques, including volume shadow copy deletion via custom Fog ransomware payloads, are employed.

## A Noteworthy Tactical Shift

Fog's TTPs have evolved to include source code exfiltration from GitLab and the public disclosure of victim IP addresses. This newly adopted method poses a risk to intellectual property, software security, and business continuity, impacting diverse industries.

Exposed source code provides attackers with opportunities for security exploits, corporate espionage, and financial gain. We anticipate that its likely they will deliver this as part of future triple extortion attempts.

## Noteworthy Technical Observation: Technique Doppelgänger

T1555.003: Credentials From Password Stores: Credentials From Web Browsers

In Fog Ransomware intrusions, operators were observed using the legitimate Microsoft utility, "Esentutl.exe," to collect and back-up copies of sensitive login data stored on victim host machines.

Further analysis also revealed that this credential access technique is similar, if not identical, to the commands used within intrusions conducted by Akira ransomware operators.

In these attacks, Akira operators used this technique to prepare data for exfiltration.

```
cmd.exe /Q /c esentutl.exe /y "C:\Users\Victim\AppData\Local\Google\Chrome\User Data\Default\Login Data" /d "C:\Users\Victim\AppData\Local\Google\Chrome\User Data\Default\Login Data.tmp"
```

This reflects a trend since 2023, where initial access brokers like Trickbot and Qakbot exploited Esentutl, a legitimate Windows utility, as a Living-Off-The-Land Binary (lolbin) to facilitate browser credential theft.

## Key Takeaways

We can expect to see further development of Fog ransomware, including potentially new variants and expanded targeting. We expect the group be a major player into 2025. As ransomware groups continue to share and refine their techniques, the lines between different families may blur, making attribution and defence more challenging. Additionally, the increased use of affiliate programs may lead to a wider distribution of attacks, targeting a broader range of sectors.

# Outlook for 2025

The following sections cover key cyber threat intelligence observations as we move further into 2025.

## Edge Devices and Vulnerability Exploitation

In 2024, we observed numerous attacks against edge devices across our managed detection and response (MDR) service. In our dataset both Fortinet and Palo Alto Networks devices were targeted by threat actors and, in several cases, incomplete asset inventory and management had ultimately led to a device not being included in patching and vulnerability management programs.

Edge device compromise poses a key threat as many organisations do not onboard edge devices into security logging and monitoring systems and, in some cases, they may not have extensive use cases for the compromise an edge device leading to onward access into internal networks.

To combat this threat, it is important that the following step are taken to protect edge devices:

**Know what's out there:** Understand your asset inventory and ensure edge devices are assessed and onboarded into asset management systems.

**Centralise monitoring for threat detection:** Onboard logs for edge devices into security monitoring programs. Define use cases to detect device compromise such as suspicious file creation, modification, or unexpected behaviour. Where device logs do not provide the opportunity for granular use cases, implement use cases from other telemetry such as detecting network enumeration or scanning, or remote access connections into your internal network from edge devices.

**Secure by design:** Ensure that both the procurement and deployment of devices and architecture follows secure by design principles.

**Harden edge devices:** Ensure that edge devices are deployed with a secure configuration disabling insecure or unnecessary features, ports, and services. Make sure that management interfaces are not directly accessible from the public internet.

**Implement strong authentication:** Ensure strong access controls are in place, using strong credentials and implementing phishing-resistant MFA.

**Continuously monitor for vulnerabilities:** Edge devices need to be continuously monitored for new vulnerabilities. When zero-day vulnerabilities are announced or identified on an edge device patching the issue is not enough. A compromise assessment should be performed on the edge device to identify any suspicious creation or modification of files, or other unexpected activity on the appliance. Vendors can provide support or provide scripts to be able to perform these activities. Where virtual appliances are being used, there may be the possibility to capture forensic images for analysis by threat hunt and incident response professionals. The NCSC and other global agencies have released guidance on securing edge devices which can used to prepare organisations for incidents involving edge devices.

# Outlook for 2025

## Operational Relay Box (ORB) Networks

In 2024, we observed increased reporting on the use of ORB networks by threat actors in their operations. ORB networks are mesh networks typically comprised of vulnerable or obsolete routers or leased virtual private servers (VPS) found on the global internet. They are geographically independent decentralised networks that are used by both APT and cyber crime threat actors, most notably Chinese APT groups.

We continue to observe ORB networks being leveraged by threat actors to evade defences, increase complexity for detection, ultimately reducing the likelihood of defenders performing successful attribution against this infrastructure usage.

Understanding how ORB networks are used by threat actors and being able to consume relevant threat intelligence to detect and investigate ORB networks is becoming a key requirement for defenders to be able to deal with this growing threat to their organisations.

**“ORB networks are mesh networks typically comprised of vulnerable or obsolete routers or leased virtual private servers (VPS) found on the global internet”**

# Outlook for 2025

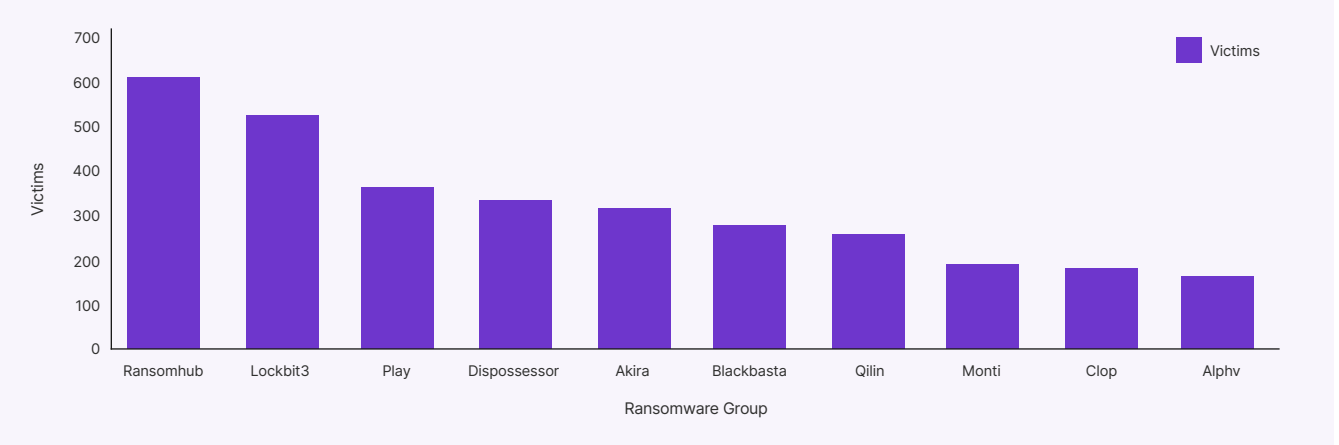
## Cyber Crime and Ransomware Ecosystem

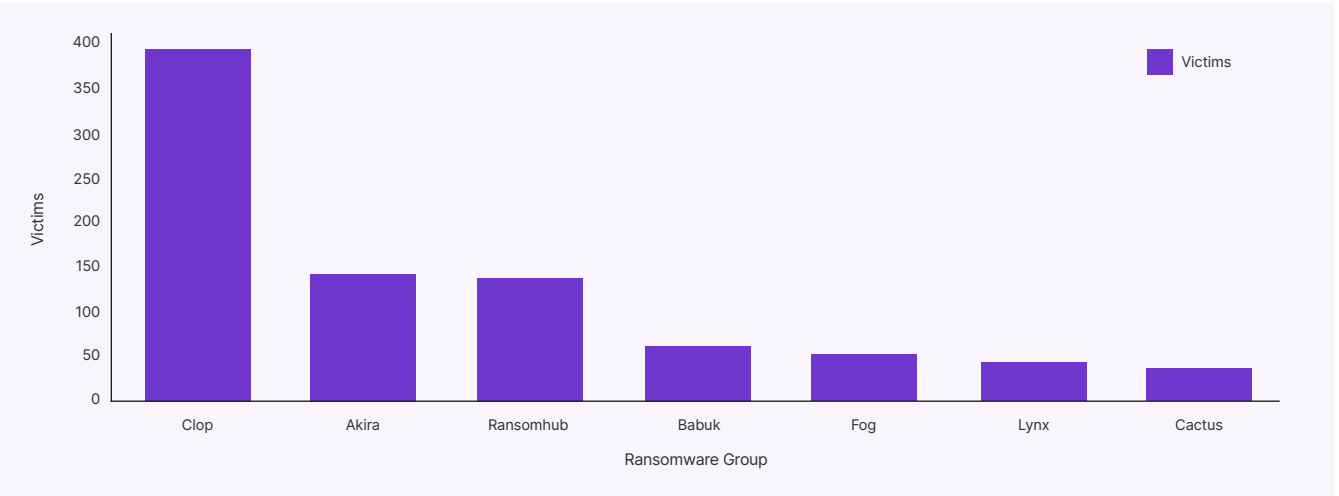
Cyber crime continued to thrive in 2024, during which the ransomware ecosystem continued to grow. There were several notable trends observed in the period.

- Law enforcement takedowns to disrupt and impose cost on ransomware groups continued. Most notably LockBit who were disrupted by a multinational policing effort.
- Exit scams were also observed, most notably ALPHV (BlackCat) who allegedly received a large multi-million-dollar ransom from the Change Healthcare attack and then failed to pay out the affiliates behind the attack.
- Cyber crime networks were disrupted by police including Operation Destabilise in the UK.
- There was a major crackdown of Cobalt Strike under the Digital Millennium Copyright Act (DMCA). Operation MORPHEUS, a three-year long investigation culminated in a coordinated global effort to takedown unauthorised versions of Cobalt Strike. A total of 690 IP addresses were flagged to online service providers in 27 countries. In total, 593 of these addresses were taken down.
- The 'as a service' model was thriving with the introduction of new malware, phishing/ delivery, traffic, access/ credentials, and infrastructure services popping up on both clear and dark web sources.

Leveraging data from Coveware and Ransomware.live, we anticipate that this trend will continue. The victim claims by ransomware operators continues to rise approximately with 6130 victims claimed in 2024.

The top groups in 2024 were RansomHub, LockBit3, Play, Dispossessor, Akira, Qilin, Monti, Clop, and AlphV (BlackCat).



# Outlook for 2025

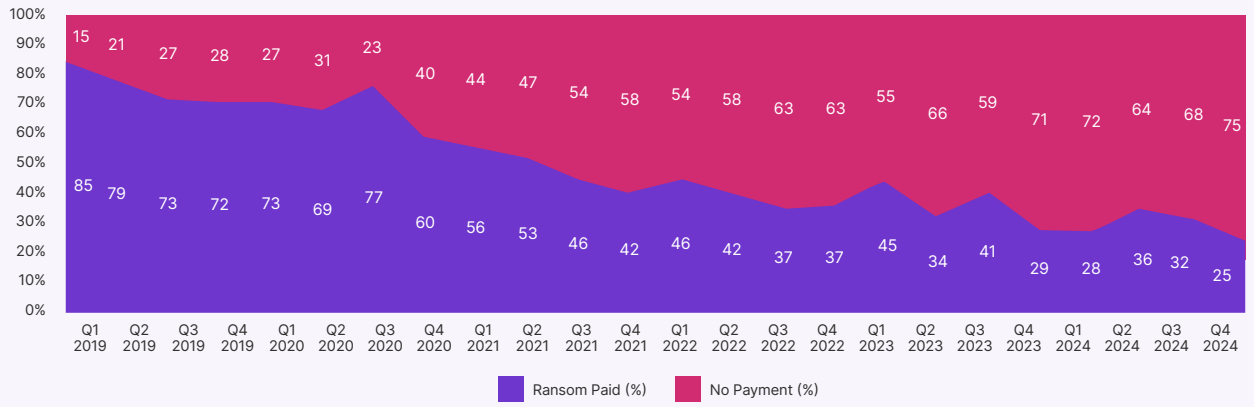
In the first two months of 2025, we have observed Clop as the front runner, joined by Akira, RansomHub, Babuk2, Fog, Lynx, and Cactus ransomware groups. Clops mass exploitation approach has seen them claim a considerable number of victims in this recent period.

We have also seen some interesting trends in the ransomware payments scene since the start of 2019. The first trend being a steady decline in the number of companies paying ransoms. In 2024, this dropped to a record low of 25%. This suggests that companies may have more robust security measures in place, including backups that are making encryption-only based attacks less effective than in previous years.

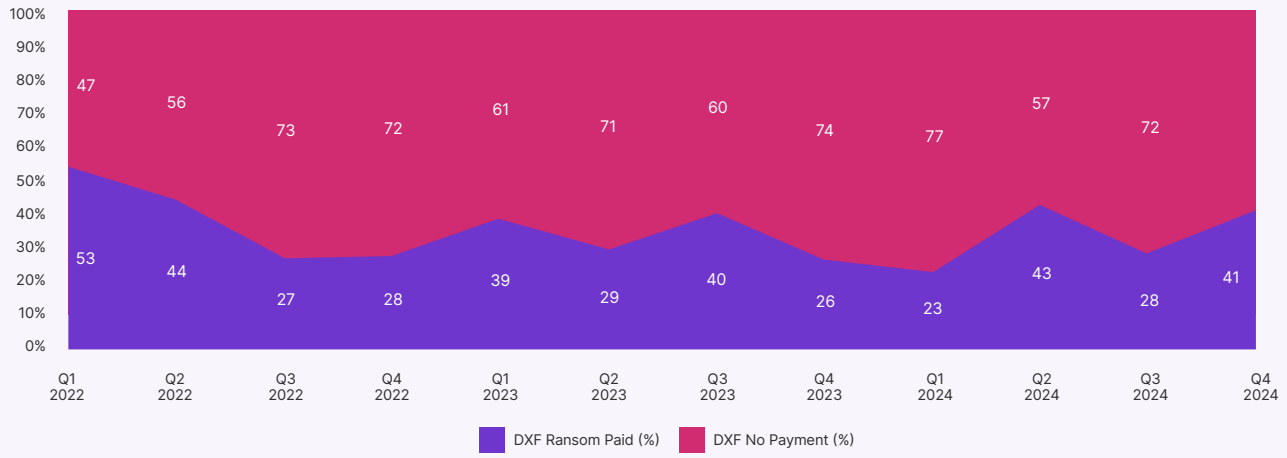
The second trend highlights how threat actors have pivoted to data theft-only attacks, which are proving to be more successful than encryption-based attacks. These stats align with our view that organisations are becoming better at withstanding ransomware attacks using encryption. However, it does highlight that the threat of data being leaked publicly still remains a bigger concern for organisations involved in these attacks.

Sources: ( https://www.coveware.com/blog/2025/1/31/q4-report, https://www.linkedin.com/pulse/ransomware-2024-insights-from-ransomwarelive-julien-mousqueton-2cfve/?trackingId=anbiqDtPSfGYB4%2FvdCs13Q%3D%3D)

**Ransomware (Encryption) Payment Resolution Rates**




**Data Exfiltration Only (DXF) Payment Resolution Rates**



# Outlook for 2025

## Cryptocurrency Theft

Cryptocurrency's inherent characteristics, including its decentralised nature and potential for anonymity, have fostered an environment where cyber crime has not only flourished but also become increasingly lucrative. This is a trend we project to continue throughout the rest of 2025.

We have high confidence that cryptocurrency cyber crime will escalate in 2025, driven by increasingly sophisticated attacks targeting cross-chain bridges, decentralised finance (DeFi) platforms, and exchanges. DPRK-linked actors will remain a significant threat, demonstrating enhanced abilities to accumulate and launder stolen funds through evolving tactics. Evidence includes rising attack success rates and growing DPRK unlaundered holdings, alongside observed shifts in money laundering methods.

We are moderately confident that global regulatory bodies will strengthen collaborative efforts against cryptocurrency cyber crime in 2025. Increased international dialogues and emphasis on anti-money laundering (AML)/ know your customer (KYC) procedures indicate a trend towards greater coordination. Evidence includes growing regulatory participation in policy discussions and stricter compliance measures. However, variations in regulatory maturity and cross-border enforcement challenges introduce uncertainty. Proactive security will be essential for cryptocurrency exchanges and DeFi platforms in 2025. Attackers are continuously adapting, demanding robust security protocols, audits, and user education. Evidence includes successful attacks exploiting known vulnerabilities and industry emphasis on preventative measures. The persistent targeting of these platforms underscores the urgent need for enhanced security.

(Sources: Analysis and insights derived from the "2025 Crypto Crime Report" and "Recap Quarterly Crypto Policy Roundtable Q1 2025", and "Now Live: The 2025 Crypto Crime Report")

**"Cryptocurrency's inherent characteristics, have fostered an environment where cyber crime has not only flourished but also become increasingly lucrative."**

# Outlook for 2025

## Generative AI

The integration of generative artificial intelligence (AI) into cyber attack methodologies is rapidly transforming the threat landscape, posing a significant challenge to defenders. Generative AI (Gen AI) empowers lower end cyber criminals with enhanced capabilities for automation, sophistication, and evasion, leading to more effective and damaging attacks. This trend is expected to accelerate, as Gen AI tools become more accessible and better understood by users.

Analysis of recent reports reveals a growing trend of AI-powered attacks, including the use of AI for generating highly realistic phishing emails, automating vulnerability scanning and exploitation, and creating heavily obfuscated malware that can evade certain security controls. Evidence includes warnings from the FBI and cyber security firms about the increasing use of AI in social engineering attacks, malware development, and network intrusion.

AI's ability to analyse vast datasets and learn patterns enables attackers to identify and exploit vulnerabilities more efficiently. Large Language Models (LLMs) are being used to generate sophisticated malware code and social engineering campaigns. Since the release of LLM and Gen AI tools, we have observed a marked increase in the sophistication of phishing campaigns and malware obfuscation, with attacks becoming more personalised and difficult to detect, directly mirroring the trends highlighted in these reports.

Voice phishing (vishing) has seen a dramatic surge in effectiveness, largely due to advancements in AI voice cloning tools like ElevenLabs, which now enable attackers to convincingly mimic the voices of trusted individuals. While deepfake video technology continues to improve, and despite remaining telltale signs, its rapid development poses a growing threat, as the ability to create believable visual impersonations becomes increasingly accessible to cyber criminals.

The use of AI in cyber attacks presents a multifaceted threat, impacting various sectors, including healthcare, finance, and critical infrastructure. AI-driven social engineering attacks, such as those used by groups like Scattered Spider, are becoming increasingly effective at manipulating human behaviour and bypassing security controls.

The automation of offensive procedures allows for faster and more widespread attacks, increasing the potential for large-scale disruptions. The ability to create highly targeted and personalised attacks further amplifies the risk.

To counter these threats, organisations must build strategies and policies to address AI and to adopt AI in their own defensive security controls to help them defend against growing attacker automation and sophistication.

# Outlook for 2025

## Geopolitical Events

We expect cyber attacks tied to global tensions and conflicts to increase throughout the rest of 2025. We have moderate confidence that Russia will continue to develop and express capabilities against critical infrastructure in Ukraine and allied countries. Iranian-backed groups will continue targeting organisations and individuals linked to Israel, including targeting industrial control systems leveraging Israeli technology and programmable logic controllers (PLCs).

Hacktivist groups, both pro-Russian and pro-Iranian collectives like the Holy League, will use disruptive Distributed Denial-of-Service (DDoS) attacks in politically-motivated targeting. They continue to leverage social media and messengers such as Telegram to spread their message. Service providers have shown appetite to ban and block abusive channels, however they continue to reappear after takedown actions.

We expect more attacks on essential services and businesses, driven by global politics. It's important for organisations to strengthen defences with the threat of politically-motivated targeting based on region or industry sector. Well architected network infrastructure and DDoS mitigation services are growing in importance due to the prevalence of DDoS attacks being observed.

## The Expanding Threat: DPRK's Exploitation of Deceptive Employment Tactics

In 2024, we observed an increase in reporting related to threat actors using fake job applicants to infiltrate western organisations.

The use of deceptive employment tactics by nation-state actors, particularly the DPRK, is a growing trend that poses a significant threat to global organisations. These tactics involve the strategic deployment of fake job applicants and overseas "laptop farms" to infiltrate targeted companies for espionage and financial gain, which directly supports the DPRK's weapons programs. This approach allows the DPRK to bypass traditional cyber security defences by leveraging human vulnerabilities and exploiting the trust inherent in employer-employee relationships.

Analysis of recent cases reveals a consistent pattern of DPRK operatives creating convincing fake online personas and resumes to secure remote IT positions. They often blend into legitimate workforces, gaining access to sensitive internal systems and data. Evidence includes numerous indictments and advisories from U.S. government agencies, cyber security firms, and technology companies, detailing instances where DPRK nationals have successfully infiltrated organisations.

These operatives engage in a range of activities, including stealing intellectual property, conducting espionage, and generating revenue through fraudulent IT work. The use of "laptop farms" in overseas locations further amplifies their reach, allowing them to scale their operations and obfuscate their true identities. Reports indicate these operations are used to generate revenue to bypass sanctions and fund DPRK weapons programs.

The increasing sophistication of these tactics necessitates a heightened awareness and proactive security posture from organisations. The DPRK's ability to adapt and refine its methods, coupled with its persistent pursuit of financial resources, suggests that this trend will continue to escalate. Evidence of this adaptation can be seen in the use of fake recruitment processes, even mimicking security firms, to gain access to sensitive information.

Furthermore, The US Department of the Treasury's Office of Foreign Assets Control (OFAC) sanctions and Department of Justice (DOJ) indictments highlight the financial nature of these operations, directly linking them to the DPRK's attempts to bypass sanctions. Companies must implement stringent vetting processes, conduct thorough background checks, and monitor employee activity to mitigate the risk of infiltration.

(Sources: CrowdStrike, U.S. Department of Justice, KnowBe4, The Register, BBC News, Google Cloud, OFAC, Palo Alto Networks Unit 42, Sasha Ingber Substack)

# Outlook for 2025

## Cloud Native Attacks

We are moderately confident that the cloud attack surface is expanding rapidly due to the continued adoption of cloud-native and hybrid environments. This is a trend we've directly observed across our managed security services clients.

Attacks are increasingly targeting cloud misconfigurations, Identity and Access Management (IAM) flaws, and container vulnerabilities, with a growing sophistication shown by container escapes, serverless hijacking, and lateral movement between on-premises and cloud systems. We've witnessed a corresponding rise in data breaches and ransomware incidents within client cloud workloads, mirroring broader industry trends. Actors such as Octo Tempest have directly been seen abusing cloud resources such as virtual compute to evade enterprise security controls and provide a foothold for the adversary inside of the compromised network.

Hybrid environments exacerbate these issues, creating opportunities for attackers to exploit shared accounts, services, and applications. We also observed API's and network vulnerabilities being exploited for lateral movement.

This is reflected in our clients' experiences with misconfigured hybrid connectivity and attacks targeting the cloud control plane. The insider threat also remains significant as privileged access is exploited, a pattern we've consistently seen both in public reporting and within our client base.

To combat these threats, a holistic security approach is essential, encompassing both on-premises and cloud environments. We've consistently advised clients to implement robust controls, continuous monitoring, and automated threat detection. Zero trust architecture and strong identity management are critical, especially given the observed prevalence of IAM-related compromises. We recommend cloud security posture assessments to ensure the use of cloud is secured effectively, in line with well architected security best practices.

(Sources: Microsoft Digital Defense Report 2024, CrowdStrike Insider's Playbook: Defending Against Cloud Threats, Check Point Security Report 2025, Splunk State of Security 2024, Fortinet Cloud Security Report 2025, Aqua Security Blog, Netskope Cloud and Threat Report 2025, and observations from our managed security services client engagements.)

"To combat these threats, a holistic security approach is essential, encompassing both on-premises and cloud environments."

# Outlook for 2025

## RMM Tools

Living-Off-The-Land (LOTL or LOL) was a popular approach by threat actors within 2024. Both nation-state and cyber crime threat actors have used LOL tactics. Most notably, we observed consistent use of RMM tools by threat actors in both public and internal intrusions. We have moderate to high confidence based on analysis of both open source and internal Bridewell telemetry that these tools are being used to bypass security controls such as web filtering and EDR, allowing threat actors to blend into regular environmental traffic.

Throughout 2024, we observed over 50 instances that involved RMM tools in our threat intelligence dataset. These tools were often deployed by threat actors after successfully obtaining access through phishing techniques, external remote services, and the use of valid credentials. In one particular incident, we observed multiple RMM tools being used by the threat actor after gaining initial access.

As we move further into 2025, there have been numerous public reports that RMM usage is on the rise. One such report by Proofpoint has also indicated that RMM tools are increasingly being used as first stage payloads as opposed to other malware variants. We again have moderate confidence based on the available reports that this is an attempt to bypass anti malware security controls.

To mitigate the threat posed by RMM tools organisations need to maintain a comprehensive inventory of all authorised RMM tools and their legitimate users. Robust monitoring and logging of RMM tool usage, including connection origins, accessed systems, and executed commands is required to identify suspicious or malicious activity.

Establishing baseline usage patterns for legitimate RMM activity can also help defenders identify anomalies. Organisations should implement application control to restrict the execution and installation of unauthorised software, and ensure threat hunting is performed regularly for RMM usage where it may not be possible for organisations to implement the previously mentioned controls.

It's important that organisations are aware of the threats posed by RMM tools and take appropriate action to assess and where appropriate mitigate the associated risks.

(Sources: Remote Monitoring and Management (RMM) Tooling Increasingly an Attacker's First Choice | Proofpoint US, and observations from our managed security services client engagements.)

**"To mitigate the threat posed by RMM tools organisations need to maintain a comprehensive inventory of all authorised RMM tools and their legitimate users."**

Bridewell

Cyber Security. Where it Matters.

## About Bridewell Threat Intelligence

Committed to our clients' security, Bridewell Threat Intelligence is a threat research and client-focused team determined on disrupting attacks and delivering robust protection against advanced threats for the organisations we manage.

To discuss how our Threat Intelligence team can help your organisation, get in touch via:

+44 (0)3303 110 940 hello@bridewell.com bridewell.com