Bridewell

Cyber Security. Where it Matters.

Bridewell Threat Intelligence

2026 Cyber Threat Intelligence Report

Your complete view of the cyber threat landscape

Contents

Foreword 3

Executive Summary 4

Intelligence Gaps 5

Adversary Infrastructure Tracking 6

Overview of Dedicated Malicious Infrastructure 6

Top 10 Tracked Threats 7

Landscape Overview 8

Key Findings and Family-Level Behaviour 9

Summary 10

Global Hosting Distribution 11

US 12

China 12

Germany 12

Year-on-Year Observations 12

Offensive Security Tooling (OSTs) 13

Key Observations 13

Cobalt Strike 14

Sliver and Brute Ratel 14

Sliver 15

Brute Ratel 16

Spotlight – AdaptixC2 17

Information Stealers 18

2025 Law-enforcement Operations 18

2025 Overview 19

WhiteSnake Stealer 21

RedLine 22

Rhadamanthys Stealer 23

StealC 24

Year-on-year Summary 25

Spotlight: Emerging Stealer Upgrade - Vidar Stealer v2.0 25

Information Stealer Ecosystem 26

Global Information Stealer Landscape 26

Rising Trends in Infostealer Compromises 26

Global Disruption of Lumma Stealer (May 2025) 27

Operation Endgame & Continued Pressure on Cyber Crime Enablers (2025) 28

Infostealer Tradecraft Evolution in 2025 28

UK Information Stealer Landscape 29

Understanding the Threat to UK Organisations 29

Dominance of Redline and Lumma in UK-Based Attacks 30

The Continued Threat of Raccoon and Emerging Variants 30

Information Stealers and RaaS Ecosystem 31

Ransomware Incidents Involving Information Stealers (2025) 31

Usage of Information Stealers Across Incidents (2025) 34

Information Stealers Used Across Ransomware Incidents (2025) 35

Information Stealer Key Takeaways 36

CNI SOC/MDR Service Detection Analysis 37

Intelligence Gaps 37

Top C2 Threat Alerts 37

Top 5 Alerts 38

Top C2 Alert Categories 39

Geographic Distribution 40

Ransomware in 2025 41

Ransomware Overview 41

Most Active Ransomware Groups 43

Industries Under Pressure 46

Payment Trends & Resolution Rates 47

Incidents of Significance 50

Research 51

Phishing Kits and Techniques 51

Introduction 51

Frameworks 51

EvilGinx 51

Tycoon2FA 52

Key Takeaway 53

Fix Style Attacks 53

Evolution of Phishing and “Fix Style” Attacks 54

Widespread Adoption and Emerging Techniques: FileFix Attack 55

“Fix Style” Attacks Continue to Change: ConsentFix 56

Bridewell Targeted Ransomware Research 58

DragonForce and RansomHub 58

Hellcat Ransomware Emerges 59

Converging Ransomware Tradecraft 60

Nation-State Collaboration with Ransomware Groups 60

Akira: SEO Poisoning and VPN Software Abuse 61

CL0P’s 2025 Enterprise Software Exploitation Campaigns 62

Cyber Crime Operations 63

Initial Access Brokers: Development in Threat Clusters – STAC5777, STAC5143 63

Operation Deceptive Prospect: RomCom Campaign Targeting UK Orgs 64

Supply Chain Compromise: Scattered Spider Coordinated Attacks on UK Retail Orgs 66

Conclusion 68

Nation State Spotlight: DPRK 68

Infrastructure Hosting Insights 69

Insights from a DPRK Attributed Campaign 70

Outlook and Closing Remarks 74

Edge Devices and the AI-Accelerated Threat Landscape 74

Cyber Crime and Ransomware Ecosystem 75

Gen AI 75

Assessment of Generative AI Threat Capabilities 75

Evolution of Obfuscation and Exploit Generation 75

The Emergence of Agentic AI and Critical Sector Impact 76

The AI Threat Evolution Matrix 76

Geopolitical Events 78

Iran 78

Russia 79

DPRK 80

Key Foreign Policy Objectives 80

Objectives for Offensive Cyber Operations 80

Targeted Areas and Sectors of Interest 80

Identity Attacks 82

Foreword

Throughout 2025, Bridewell's Cyber Threat Intelligence team worked alongside clients to deliver timely, relevant, and actionable intelligence, enabling threat-informed defence and effective detection and response to credible cyber threats. This report distils that intelligence into a structured view of how adversaries operated over the year, the tooling and infrastructure they relied upon, and the trends shaping the threat landscape as organisations move into 2026.

At its core, the 2025 threat landscape was defined by continuity rather than disruption. Mature command-and-control frameworks such as Cobalt Strike and Sliver continued to dominate adversary infrastructure, information stealers remained a primary enabler of cyber crime and ransomware operations, and hosting patterns showed persistent concentration in a small number of geographies and providers. At the same time, several meaningful shifts were observed beneath that surface stability, including increased diversification in hosting models, growing fragmentation within malware-as-a-service and ransomware ecosystems, and the accelerated adoption of social-engineering-led and identity-centric attack techniques.

This report draws on intelligence from Bridewell's adversary infrastructure tracking programme, Security Operations Centre (SOC), Managed Detection and Response (MDR), Incident Response activity, and targeted research conducted throughout the year. Analysis focuses on the early stages of the intrusion lifecycle - including pre-ATT&CK infrastructure, initial access methods, and post-exploitation tooling - to provide insight into how threat actors prepare, scale and sustain operations before victim-side compromise becomes visible.

Key findings for 2025 include the continued dominance of offensive security tooling, the increasing strategic importance of information stealers as a source of identity compromise and initial access, and clear evidence of rotation rather than eradication following law-enforcement disruption. The report also highlights the growing overlap between cyber crime and state-aligned activity, the expanded use of trusted platforms and first-party services for defence evasion, and the accelerating role of generative AI as a force multiplier rather than a replacement for existing tradecraft.

While the structure of the threat landscape remains familiar, the speed, scale, and resilience of adversary operations continue to increase. As attackers place greater emphasis on identity abuse, edge infrastructure, and data-exfiltration-driven extortion models, organisations must adapt defensive strategies accordingly. This report is intended to provide security leaders and practitioners with the context and evidence needed to prioritise those efforts and build more threat-informed, resilient defences in the year ahead.

Gavin Knapp
Head of Cyber Threat Intelligence

By Gavin Knapp, Head of Cyber Threat Intelligence; Tom Igoe, Senior Cyber Threat Intelligence Analyst; Joshua Penny, Senior Cyber Threat Intelligence Analyst; Yashraj Solanki, Senior Cyber Threat Intelligence Analyst; Nathan Richards, Cyber Threat Intelligence Analyst; and Daniel Whitcombe, CTI Analyst.

Executive Summary

In 2025, our CTI team continued to mature and expand its adversary infrastructure tracking and analytical capabilities, building on the foundations established in the previous year. Throughout the reporting period, our intelligence drew on sustained monitoring of malicious infrastructure, client telemetry, incident response activity, and targeted research to assess how threat actors adapted their tradecraft in response to disruption, defensive controls, and wider geopolitical pressure.

Analysis of our 2025 malicious infrastructure tracking data revealed a threat landscape defined by continuity in core tooling, increased diversification in hosting and delivery models, and persistent reliance on commodity frameworks and malware as a service (MaaS) ecosystems. The key findings, detailed below, include:

- The global hosting landscape was dominated by a small number of countries. The US retained its position as the primary hosting location for malicious infrastructure, while China remained a significant but declining contributor. Germany saw the most notable year on year increase, moving into third place globally.
- Command and control (C2) frameworks and offensive security tooling continued to dominate the tracked threat landscape. Cobalt Strike remained the most prevalent framework overall, while Sliver consolidated its position as the leading alternative and continued to gain share through broader and more distributed use.
- Malware and tooling historically associated with Chinese nexus activity, including PlugX, ShadowPad and SuperShell C2, remained prominent within the annual top tracked threats, reinforcing the persistence of espionage linked infrastructure alongside cyber crime tooling.
- The post exploitation ecosystem showed further diversification, with frameworks such as Brute Ratel, Havoc and emerging tooling such as AdaptixC2 reflecting sustained operator interest beyond the most heavily monitored platforms.
- Information stealers remained a critical enabler of modern cyber crime and ransomware operations, continuing to function as a primary initial access mechanism feeding downstream intrusion and extortion activity.

Within the information stealer landscape, several important shifts were observed during 2025:

- Law enforcement operations, including multiple phases of Operation Endgame, materially disrupted parts of the ecosystem and contributed to short term declines in activity. However, the dominant pattern observed was rotation rather than eradication, with suppression of one family frequently followed by redistribution into others.
- The infrastructure tracking dataset for 2025 showed a move away from the Lumma led environment described in the previous report, toward a more fragmented market, led by families such as WhiteSnake, RedLine and Rhadamanthys.
- Hosting patterns for leading information stealers became more geographically distributed year on year, with reduced dominance of Russia-centric infrastructure and increased use of Western cloud and European hosting environments.
- In the UK, information stealers continued to feature prominently in ransomware and cyber crime activity, with RedLine, Lumma, Raccoon and StealC remaining key families impacting UK organisations and critical national infrastructure.

Executive Summary

From a research perspective, several thematic trends defined the 2025 reporting period:

- Social engineering driven initial access techniques continued to evolve. “Fix style” attacks such as ClickFix, FileFix and ConsentFix demonstrated how adversaries increasingly bypass technical controls by manipulating user behaviour, shifting execution away from traditional malware delivery and into trusted system and identity workflows.
  - ClickFix style techniques expanded beyond cyber crime and were adopted by multiple nation state actors during the year.
  - Subsequent variants further reduced reliance on endpoint execution, reinforcing the trend toward identity centric compromise.
- Endpoint Detection and Response (EDR) evasion remained a significant focus across ransomware and cyber crime operations. Dedicated EDR-killer tooling and Bring Your Own Vulnerable Driver (BYOVD) techniques continued to be adopted to disable or degrade defensive visibility.
- Ransomware activity throughout 2025 reflected ongoing fragmentation within the ransomware as a service (RaaS) ecosystem, with affiliate mobility, rapid emergence of new groups, and increasing overlap between cyber crime and state aligned activity.
- Information stealers and initial access brokers remained tightly coupled with ransomware operations, reinforcing the role of credential theft, session hijacking and identity compromise as precursors to extortion.
- Generative AI increasingly acted as a force multiplier for threat actors, accelerating reconnaissance, exploit development, social engineering and operational scale, rather than replacing existing tradecraft outright.

In our ‘Outlooks’ and ‘Closing Remarks’, we examine how these trends are expected to shape the threat landscape moving forward. Key observations include the continued exploitation of edge devices and identity infrastructure, the expansion of data exfiltration only extortion models, the growing abuse of trusted platforms and developer ecosystems, and the impact of geopolitical instability on both state aligned and criminal cyber activity. These themes, alongside advances in AI enabled tradecraft and persistent ransomware ecosystem fragmentation, form our core CTI observations as organisations prepare for an increasingly adaptive and identity-focused threat landscape in 2026.

Intelligence Gaps

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, so both 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

Bridewell's Adversary Infrastructure program tracks threat groups in the PRE-ATT&CK stage, leveraging various sources of telemetry to identify traffic from C2, botnets, remote access trojans (RATs), initial access brokers (IABs), advanced persistent threats (APTs), phishing, ransomware groups, open directories, traffic distribution systems (TDS) and operational relay box (ORB) networks. Gathering proactive indicators of attack (IOAs) allows our product offering, Cybiquity Defend, to hunt for those indicators within our client environments.

Overview of Dedicated Malicious Infrastructure

In 2025, Bridewell CTI tracked over 40,000 servers associated with malware C2 servers, phishing, payload hosting, threat actor-controlled infrastructure and Offensive Security Tooling (OSTs) used by financially motivated threat actors and nation-state groups. Feeding this intelligence into our Managed Detection and Response (MDR) services and hybrid Security Operations Centre (SOC) helps our clients defend from cyber criminals and APTs.

This section will provide a summary of our Adversary Infrastructure Tracking capability by: Infrastructure Geolocation, Infrastructure Hosting Providers, Top Tracked Threats, OSTs, Information Stealers, and Remote Access Trojans.

Adversary Infrastructure Tracking

Top 10 Tracked Threats

The 2025 top tracked threats list continues to reflect a landscape dominated by C2 frameworks, post-exploitation tooling, dual-use security utilities, and a smaller number of espionage-linked malware families. As in previous reporting periods, the annual ranking is led by mature and widely adopted frameworks that support remote access, payload delivery, lateral movement, persistence, and post-compromise operations at scale. The most prevalent malware families observed in 2025 are Cobalt Strike, Sliver, Metasploit, Burp, PlugX, SuperShell C2, Havoc, Panda C2, Brute Ratel, and ShadowPad.

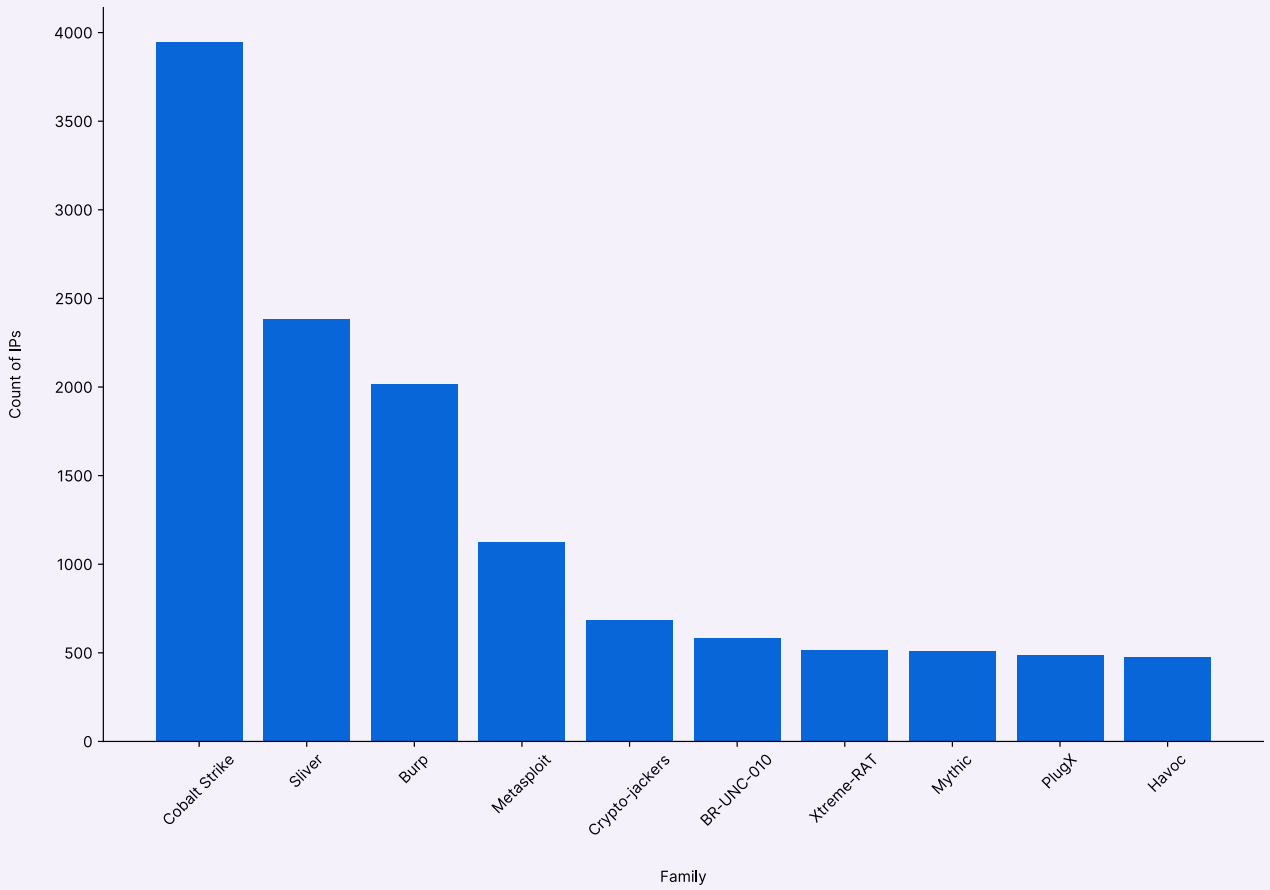


Figure 1. Top 10 Tracked Threat Families - Unique IPs (2025)

Adversary Infrastructure Tracking

Landscape Overview

Throughout 2025, the tracked threat landscape heavily centred around offensive tooling and C2 infrastructure. Cobalt Strike remains dominant by a considerable margin, with Sliver retaining its position as the most significant alternative framework. Additionally, Metasploit and Burp also maintain substantial visibility, reflecting the continued relevance of dual-use tooling that can support both legitimate security testing and malicious intrusion activity.

Alongside these are several malware families associated with more specialised, operational use cases. PlugX, SuperShell C2, and ShadowPad continue to represent malware and tooling commonly linked to espionage-focused activity, while Panda C2, Brute Ratel, and Havoc reinforce the depth of the wider post-exploitation ecosystem. Collectively, these families indicate that the 2025 threat landscape is defined by a mixture of established operator tradecraft, adaptable framework use, and persistent visibility of infrastructure associated with state-aligned or espionage-linked activity.

A key characteristic of the 2025 dataset is the concentration of observed infrastructure within a small number of malware families. Cobalt Strike remains ahead of all others by total unique IPs, with the remainder of the top 10 distributed across a relatively compressed second tier. This continues to suggest that although operators have diversified their tooling choices, the overall landscape remains anchored by a small number of highly effective and operationally flexible frameworks.

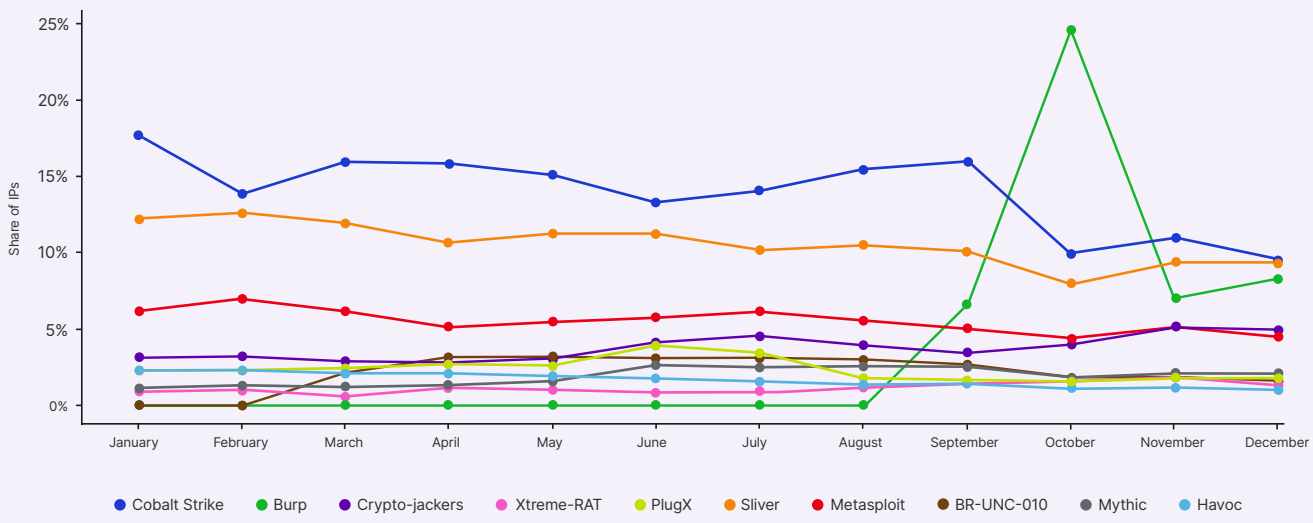


Figure 2. Top 10 Threat Families – Monthly Activity

Adversary Infrastructure Tracking

Key Findings and Family-Level Behaviour

Cobalt Strike

Cobalt Strike remained the most prevalent tracked family in 2025 by a substantial margin, with total infrastructure exceeding 6,000 unique IPs throughout the year. Monthly activity remained consistently high, peaking in June before declining gradually through the second half of 2025. Despite this, Cobalt Strike remained the dominant family across the reporting period and continued to underpin a significant share of observed post-exploitation activity.

Sliver

Sliver continued to be the second most prominent malware family and alternative to Cobalt Strike. Its activity remained comparatively stable with a clear increase in June and July, before easing off in the final quarter of the year, indicating a continued reliance on Sliver by operators as an established C2 framework with sustained operational relevance.

Metasploit

Metasploit remained one of the most consistently observed families in 2025, with increased activity in the first half of the year, declining sharply from August and stabilising at a lower level in the final quarter. Its continued presence in the top tier reflects its enduring utility as a flexible framework for reconnaissance, payload delivery and exploitation.

Burp

Burp remained within the top tracked families in 2025, although at a materially lower scale than Cobalt Strike, Sliver, and Metasploit. Burp activity grew progressively through the first half of the year, peaking in May, before declining. Its continued visibility is consistent with the dual-use value of the tool across both benign assessment activity and malicious intrusion workflows.

PlugX

PlugX remained in the annual top 10 and showed a stable but gradually declining profile across 2025. Activity was strongest at the start of the year and softened through the middle and latter months. Although lower in overall volume than the leading frameworks, its continued inclusion remains strategically significant given its longstanding association with espionage-focused intrusion activity.

SuperShell C2

SuperShell C2 remained a significant presence in 2025 with activity peaking in May before declining for the remainder of the year. The family maintained a clear operational footprint throughout the reporting period and continued to feature prominently among the second tier of tracked infrastructure.

Havoc

Havoc entered 2025 in the top 10 as a notable post-exploitation framework, maintaining a modest but persistent presence across the year, with activity being strongest in the early months and declining gradually over time. Its inclusion reinforces the continued breadth of the alternative post-exploitation ecosystem beyond the most established families.

Panda C2

Panda C2 remained in the top 10 with moderate activity throughout the year and stable monthly volumes without the spikes or collapses seen amongst other malware families. This suggests that Panda C2 has retained an established, if smaller role, within the wider C2 ecosystem.

Brute Ratel

Brute Ratel's monthly volumes remained below those of leading frameworks, with activity building through the first half of the year, stabilising at a broadly consistent level. Its continued presence reflects sustained operator interest in alternative post-exploitation tools designed to complement or replace more heavily monitored frameworks.

ShadowPad

ShadowPad continued to hold a top 10 position, albeit at the lower end of the ranking by unique IPs. Its activity remains limited in comparison with the dominant C2 frameworks, but its continued use and longstanding links to Chinese-nexus intrusion activity give it strategic significance despite its relatively small footprint.

Adversary Infrastructure Tracking

Summary

The 2025 dataset shows strong continuity with last year's report, with C2 frameworks, post-exploitation tools and dual-use utilities continuing to dominate the threat landscape, with very little change year-on-year.

Cobalt Strike remains the clearest point of continuity. In our previous report, it was the most prevalent tracked family, dominating observed infrastructure despite increasing diversification in operator tooling. The shift away from exclusive reliance on Cobalt Strike, first noted in our 2025 report, is still evident in the rising prominence of Sliver and Brute Ratel. However, our latest dataset shows no indication that Cobalt Strike has been fundamentally displaced from its leading position.

The newest dataset also reinforces our previous assessment that Metasploit and Burp remain consistent fixtures in the annual rankings. Their ongoing prominence reflects their flexibility, extensibility and sustained use across legitimate security testing and malicious intrusion activity, underscoring the operational value of widely available dual-use tooling.

Continuity is also evident in the prominence of families associated with Chinese-nexus activity. PlugX, ShadowPad and SuperShell featured prominently in 2024 and that pattern remained unchanged in 2025 with these families retaining top 10 positions. This highlights the sustained scale and resilience of infrastructure linked to espionage-focused operations.

The most notable change year on year appears at the lower end of the rankings rather than in the overall structure of the threat landscape. Havoc enters the top 10, highlighting continued diversification within the post-exploitation and C2 ecosystem. Conversely, the disappearance of Qakbot and Racoon Stealer, first noted in the 2025 report, remains consistent, with neither family reemerging as a significant presence.

Overall, our latest dataset supports the main conclusions made in our previous report. The threat landscape remains centred on maturing C2 frameworks, adaptable post-exploitation tooling and persistent, APT-linked malware families. Operator tooling continues to diversify. However, this change remains evolutionary rather than transformative, with annual rankings showing more continuity than disruption.

Adversary Infrastructure Tracking

Global Hosting Distribution

	Jan 2025	Feb 2025	March 2025	April 2025	May 2025	Jun 2025	Jul 2025	Aug 2025	Sep 2025	Oct 2025	Nov 2025	Dec 2025	Total
United States	29.04%	28.91%	27.38%	27.21%	26.92%	27.25%	26.97%	27.05%	32.51%	26.85%	33.48%	34.22%	**27.89%**
China	14.13%	11.01%	13.49%	14.27%	13.73%	12.12%	13.93%	13.57%	11.40%	15.08%	9.38%	9.46%	**13.55%**
Germany	9.71%	10.82%	9.77%	7.66%	7.81%	7.66%	7.40%	7.53%	8.17%	8.66%	8.40%	8.62%	**8.74%**
Hong Kong	6.34%	6.10%	6.79%	7.53%	7.27%	7.78%	7.49%	6.43%	6.68%	8.12%	4.93%	4.86%	**7.22%**
Netherlands	8.32%	8.94%	8.32%	7.63%	7.29%	6.86%	6.66%	6.56%	6.25%	5.49%	6.64%	6.18%	**6.51%**
Russian Federation	4.50%	5.27%	5.09%	4.95%	6.46%	6.33%	4.91%	3.61%	3.21%	3.23%	3.06%	3.22%	**4.17%**
Singapore	3.65%	3.89%	3.68%	4.02%	3.67%	3.78%	3.74%	3.82%	3.57%	3.48%	3.60%	3.47%	**3.50%**
United Kingdom	2.68%	2.72%	1.92%	1.98%	2.13%	2.42%	2.33%	2.24%	2.63%	2.89%	3.16%	2.89%	**2.64%**
Korea, Republic of	1.90%	2.34%	2.16%	2.86%	2.84%	2.74%	2.70%	2.98%	2.55%	2.12%	2.63%	2.23%	**2.23%**
France	2.00%	1.99%	1.87%	1.66%	1.67%	1.66%	1.64%	1.72%	2.05%	2.03%	1.97%	2.01%	**1.69%**
Turkey	0.75%	0.81%	0.68%	0.61%	0.60%	0.92%	1.12%	1.34%	1.02%	0.64%	0.41%	0.54%	**0.98%**
Spain	0.61%	0.74%	0.72%	0.59%	0.61%	0.58%	0.61%	0.61%	0.58%	0.49%	0.52%	0.53%	**0.45%**
Indonesia	0.32%	0.27%	0.27%	0.23%	0.30%	0.41%	0.42%	0.39%	0.29%	0.54%	0.39%	0.46%	**0.40%**
Saudi Arabia	0.05%	0.03%	0.24%	0.33%	0.25%	0.23%	0.20%	0.13%	0.15%	0.14%	0.13%	0.15%	**0.23%**
Argentina	0.05%	0.06%	0.23%	0.28%	0.30%	0.31%	0.33%	0.46%	0.40%	0.24%	0.19%	0.16%	**0.21%**

Figure 3. Global Distribution Table

In 2025, 27.89% of all infrastructure we tracked was hosted in the US, an increase from 23.63% in 2024. China remained the second largest hosting location at 13.55%, down from 17.57% the previous year. Germany increased to 8.74%, becoming the third largest hosting location and overtaking both Hong Kong (7.22%) and the Netherlands (6.51%).

The overall distribution remains consistent with previous reporting, with the US and China continuing to dominate global hosting. However, the balance between the two shifted in 2025. While their combined share remained broadly stable at 41.44%, a greater proportion of infrastructure is now hosted in the US.

The US showed steady dominance throughout the year, with a notable increase in the final quarter, exceeding 33% in both November and December. China's share was more variable, peaking at 15.08% in October before declining to below 10% in November and December. Germany maintained a consistent contribution across the year, supporting its position as the third largest hosting location.

Analysis of Autonomous System Numbers (ASNs) shows that infrastructure remains concentrated among a small number of providers within each region, although the degree of concentration varies significantly.

Adversary Infrastructure Tracking

US

The top three hosting providers were DigitalOcean (AS14061), Kaopu Cloud HK Limited (AS138915) and COLOCROSSING (AS36352), which together accounted for 23.4% of malicious infrastructure hosted in the US. The US continues to demonstrate a relatively distributed hosting model.

While these providers represent the largest contributors, a substantial proportion of infrastructure is spread across a wider range of ASNs. DigitalOcean and COLOCROSSING contributed consistently throughout the year. Kaopu Cloud HK Limited showed a stronger presence in the first half of 2025 before declining in later months. Other providers, including Amazon (AS14618 & AS16509), also contributed consistently but did not feature in the top three overall.

China

The top three hosting providers were ALIBABA (AS37963), TENCENT (AS45090) and HWCSNET Huawei Cloud Service (AS55990), which together accounted for 75.0% of malicious infrastructure hosted in China. China remains the most concentrated of the top hosting regions, with the majority of infrastructure hosted on a small number of providers. Although these providers remain dominant, their combined share has decreased compared to 2024, indicating a modest broadening of infrastructure across additional ASNs.

Germany

The top three hosting providers were AEZA GROUP LLC (AS210644), Hetzner (AS24940) and DigitalOcean (AS14061), which together accounted for 35.2% of malicious infrastructure hosted in Germany. Germany represents the most significant regional change in 2025, increasing its share and moving into third place, globally.

Its hosting distribution shows moderate concentration, sitting between the highly concentrated model observed in China and the more distributed model seen in the US. AEZA GROUP LLC contributed heavily during the early part of the year, while Hetzner and DigitalOcean maintained more consistent contributions. Contabo (AS51167) also remained a significant contributor, narrowly outside the top three.

Year-on-Year Observations

The overall structure of global hosting remains broadly consistent with 2024, with the same core group of countries accounting for the majority of infrastructure. However, the internal balance has shifted. The US increased its share significantly, while China declined. Germany's rise to third place represents the most notable positional change and reflects sustained activity across multiple providers rather than a short-term spike.

China continues to show the highest level of concentration, although this has reduced slightly compared to the previous year. The US remains the least concentrated of the top regions, indicating a broader distribution of infrastructure across providers. Additional regional shifts were also observed. The Republic of Korea entered the top ten for the first time, while Mexico showed a marked increase in the final quarter of the year.

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.

In 2025, offensive security tooling (OST) continued to form a core component of adversary infrastructure. Across the 2025 dataset, we tracked 10,272 OST instances in total. Cobalt Strike remained the most widely observed tooling, accounting for 38.4% of all tracked OST output, followed by Sliver at 23.2% and Metasploit at 11.0%. A second tier of tooling, including Mythic (5.0%), Havoc (4.7%), SuperShell C2 (4.5%) and Meterpreter (4.3%), also demonstrated sustained usage throughout the year. Brute Ratel accounted for 3.1% of total OST output, while AdaptixC2 accounted for 1.5%.

Compared with our 2025 report, the overall OST picture is smaller but more distributed. The 2025 report described 15,000+ unique IPs associated with C2 frameworks and recorded Cobalt Strike at 42% of OST, Sliver at ~15%, and Brute Ratel at 4%. In 2025 however, Cobalt Strike fell to 38.4% of total OST output, while Sliver rose to 23.2%, and Brute Ratel fell to 3.1%.

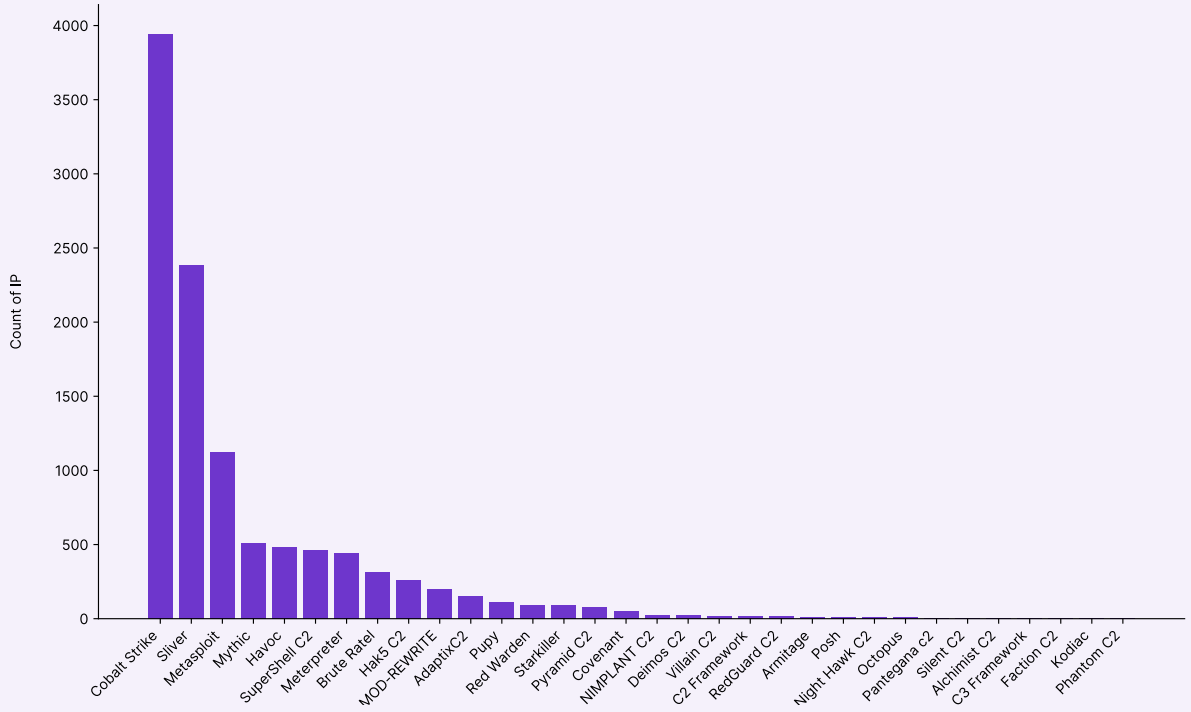


Figure 4. OST Distribution 2025

Key Observations

The most important shift in 2025 is not that Sliver has become a primary framework, but that it is being used more often. Cobalt Strike remains the largest single contributor to total OST output, but it no longer dominates the field to the same extent. Sliver has taken a materially larger share of the ecosystem, while the remaining activity is spread across a broader set of mid-tier and emerging tools.

At the infrastructure level, there remains a clear split between highly concentrated and more distributed hosting models. Cobalt Strike continues to be concentrated within a small number of China-based cloud providers, Sliver is far more geographically distributed, while Brute Ratel remains smaller and more fragmented than both. AdaptixC2 is still small on a full-year basis, but its late-year monthly activity makes it more important than its annual percentage alone suggests.

Adversary Infrastructure Tracking

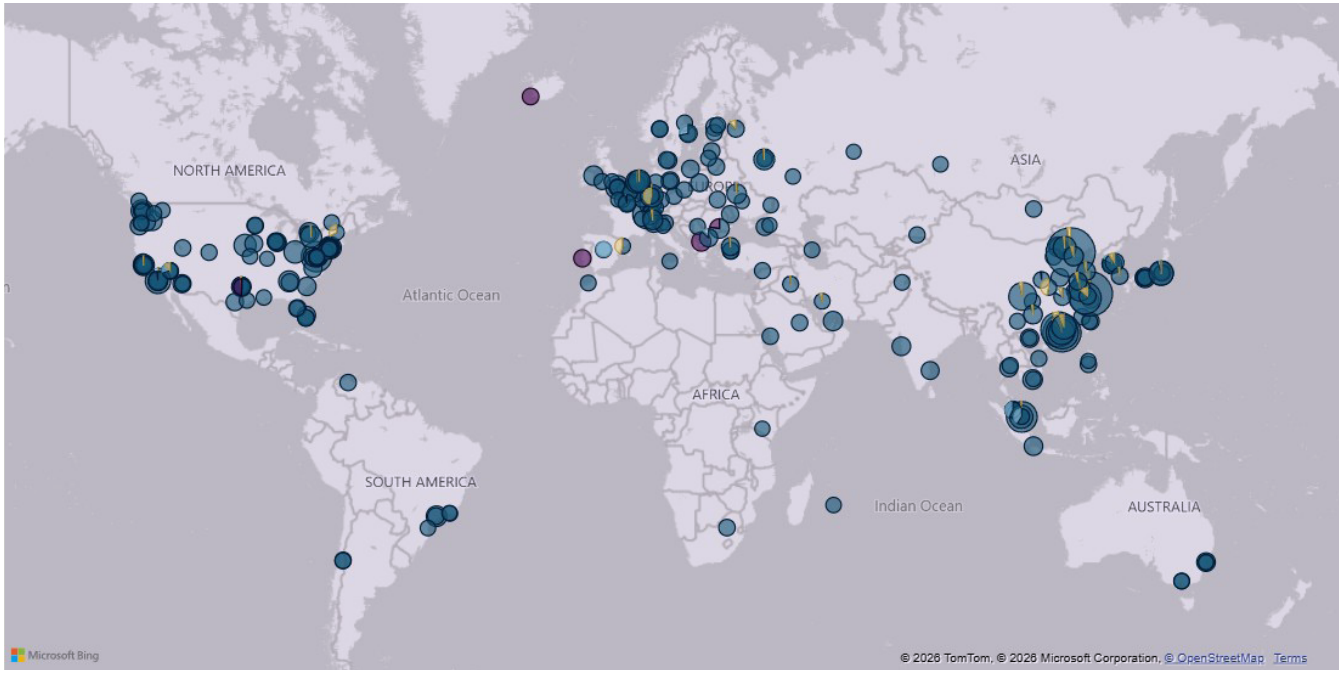
Cobalt Strike

Cobalt Strike, a commercial framework initially designed for adversary simulation and penetration testing, remained the most dominant OST in 2025. It accounted for 38.4% of all OST output (3,944 of 10,272 tracked OST instances), maintaining its position as the primary adversary framework.

China hosted 42.3% of all tracked Cobalt Strike infrastructure, the US hosted 18.9%, and Hong Kong hosted 15.8%. Combined, those three locations accounted for 77.0% of all observed Cobalt Strike activity in 2025. Measured against total OST output, China-hosted Cobalt Strike alone represented 16.2% of all OST activity, while the US contributed 7.3% and Hong Kong 6.1%.

At the ASN level, Cobalt Strike remained heavily concentrated within a small number of China-based providers. Hangzhou Alibaba Advertising Co., Ltd. (AS37963) accounted for 18.0% of all global Cobalt Strike infrastructure, Shenzhen Tencent Computer Systems Company Limited (AS45090) accounted for 13.2%, and Huawei Cloud Service data centre (AS55990) accounted for 6.2%. Together, those three ASNs accounted for 37.4% of all Cobalt Strike activity globally, and 88.4% of all China-hosted Cobalt Strike. In the US, the leading providers were Google LLC (AS396982) at 4.1% of all global Cobalt Strike, Amazon.com, Inc. (AS14618) at 2.1%, and HostPapa (AS36352) at 1.9%. Together, those three ASNs accounted for 8.1% of all global Cobalt Strike, and 42.8% of all US-hosted Cobalt Strike, which is materially more distributed than the Chinese hosting picture.

Figure 5. C2 Infrastructure Mapping



Compared with 2024, Cobalt Strike's share of total OST output fell from 42.0% to 38.4%, a decline of 3.6%. In absolute terms, last year's report stated that Cobalt Strike "topped 6000" servers, which means the 2025 total of 3,944 is down by at least 2,056 servers year on year, or at least 34.3%. The broad international picture shifted only modestly: China fell from ~45% of all Cobalt Strike infrastructure in 2024 to 42.3% in 2025, the US rose from 17% to 18.9%, and Hong Kong rose from 11% to 15.8%.

The continued concentration of Cobalt Strike within the same core Chinese cloud providers suggests those environments continue to offer operational advantages for threat actors, including scale and continuity.

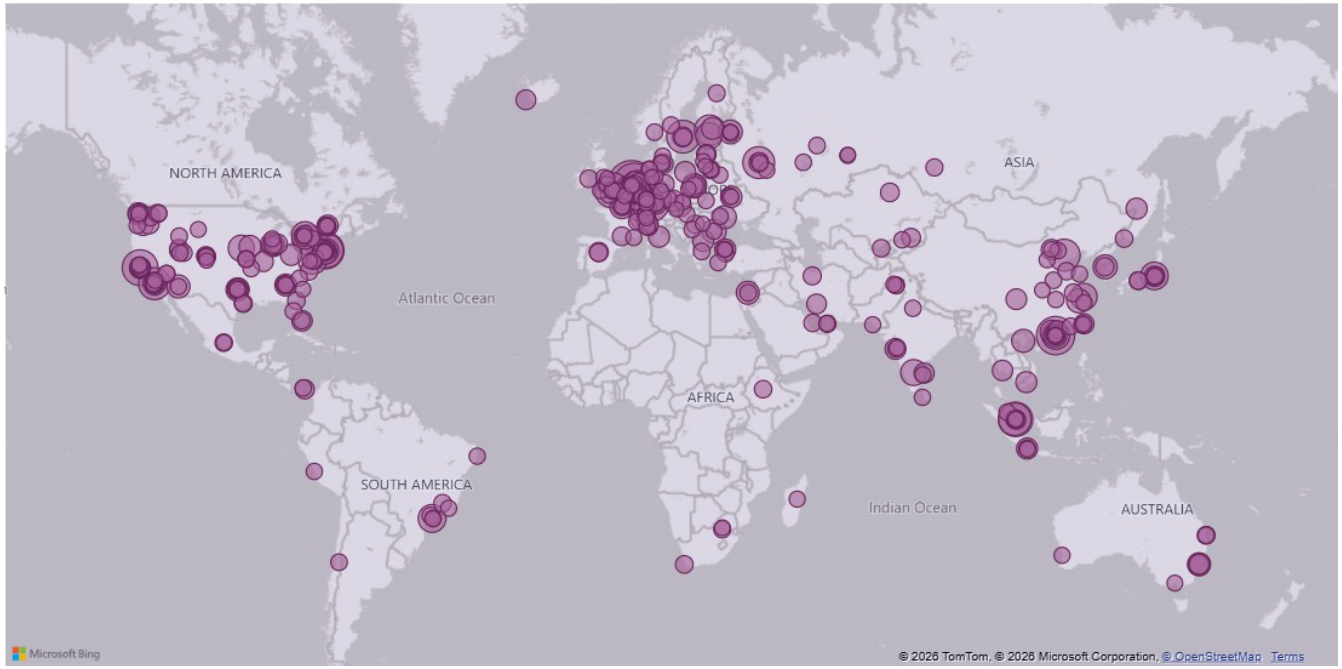
Sliver and Brute Ratel

Sliver and Brute Ratel represent two different patterns within the 2025 OST landscape. Sliver is now taking a larger share of total OST output, but it is doing so with a much more distributed international and ASN footprint. Brute Ratel remains smaller and more fragmented.

Adversary Infrastructure Tracking

Sliver

Figure 6. C2 Infrastructure Mapping



Sliver accounted for 23.2% of total OST output in 2025 (2,381 of 10,272 tracked OST instances), making it the second most prevalent framework in the dataset.

Within the Sliver set itself, the US hosted 23.5% of all tracked Sliver infrastructure, followed by the Netherlands at 11.8%, Germany at 11.5%, Hong Kong at 6.4%, Russian Federation at 5.8%, China at 4.8%, and Singapore at 4.7%. This is a materially more distributed hosting picture than the one observed for Cobalt Strike.

In terms of total OST output, US-hosted Sliver represented 5.4% of all OST activity, while the Netherlands and Germany each contributed 2.7%.

At the ASN level, the largest Sliver concentrations were still limited compared with Cobalt Strike. In the US, the leading providers were DigitalOcean, LLC (AS14061) at 5.5% of all global Sliver, HostPapa (AS36352) at 2.5%, and Akamai Connected Cloud (AS63949) at 1.3%. Together, those three ASNs accounted for 9.3% of all Sliver activity globally and 39.5% of all US-hosted Sliver.

In China, the leading providers were Hangzhou Alibaba Advertising Co., Ltd. (AS37963) at 2.1% of all global Sliver, Shenzhen Tencent Computer Systems Company Limited (AS45090) at 1.1%, and Huawei Cloud Service data centre (AS55990) at 0.5%. Together, those three ASNs accounted for 3.7% of all Sliver activity globally and 75.7% of all China-hosted Sliver.

Compared with 2024, Sliver's share of total OST output increased from ~15% to 23.2%, an increase of 8.2 percentage points. The overall geographic distribution remains consistent with last year's report: the US is still the largest hosting region, the Netherlands and Germany remain important, and China remains present but not dominant. In that respect, Sliver has not shifted from "secondary" to "primary"; it was already a core framework in 2024 and is simply being used more heavily in 2025.

Threat actors observed using Sliver C2 in 2025 included UNC3569, TeamPCP, Shadow Syndicate, Nitrogen Ransomware and HellCat.

Adversary Infrastructure Tracking

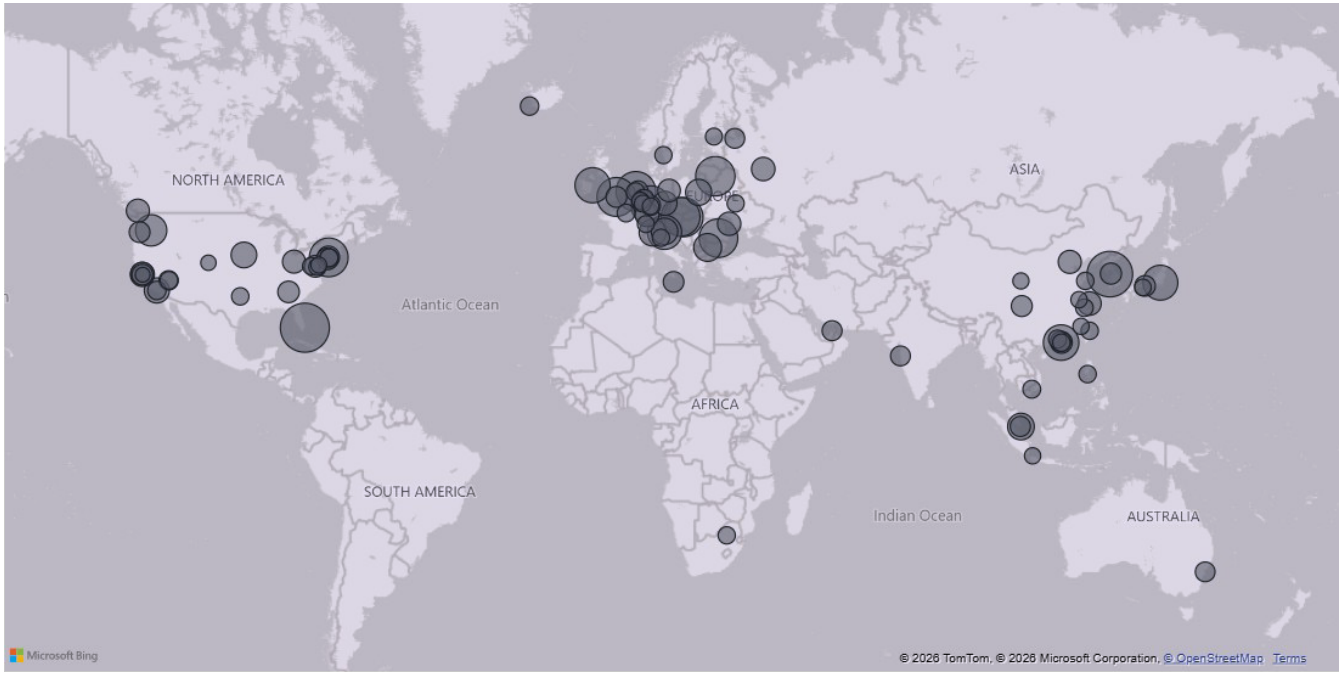
Brute Ratel

Brute Ratel accounted for 3.1% of total OST output in 2025 (315 of 10,272 tracked OST instances), down from 4.0% in 2024.

Within the Brute Ratel set itself, the US hosted 15.9% of all tracked Brute Ratel infrastructure, followed by Japan at 10.5%, Germany at 7.0%, China at 6.7%, Hong Kong at 5.1%, and the Netherlands at 4.1%. This is a substantially more diffuse picture than the one described in our previous report, where 64% of Brute Ratel infrastructure was hosted in China for the year overall. In terms of total OST output, the US contributed 0.49%, Japan 0.32%, Germany 0.21%, and China 0.20%.

At the ASN level, the US hosted the strongest single clusters. DigitalOcean, LLC (AS14061) accounted for 3.8% of all global Brute Ratel activity, Amazon.com, Inc. (AS16509) accounted for 3.2%, and The Constant Company, LLC (AS20473) accounted for 1.3%. Together, those three ASNs hosted 8.3% of all Brute Ratel activity globally, and 52.0% of all US-hosted Brute Ratel. In China, the leading providers were Hangzhou Alibaba Advertising Co., Ltd. (AS37963) at 2.5% of all global Brute Ratel, Shenzhen Tencent Computer Systems Company Limited (AS45090) at 1.6%, and CHINANET SiChuan Telecom Internet Data Center (AS38283) at 0.6%. Together, those three ASNs accounted for 4.8% of all Brute Ratel activity globally, and 71.4% of all China-hosted Brute Ratel.

Figure 7. C2 Infrastructure Mapping



Compared with 2024, the most important change is not simply that Brute Ratel's overall share is slightly smaller, but that its hosting is no longer dominated by China in the same way. That is a material change from last year's report and is one of the clearest structural differences in the 2025 Brute Ratel dataset.

Examples of actors seen using Brute Ratel in 2025 included Emissary Panda, Midnight Blizzard, BlackBasta and Earth Lusca.

The more diffuse 2025 country profile suggests Brute Ratel may be being used in a more selective and regionally varied way than in 2024.

Adversary Infrastructure Tracking

Spotlight – AdaptixC2

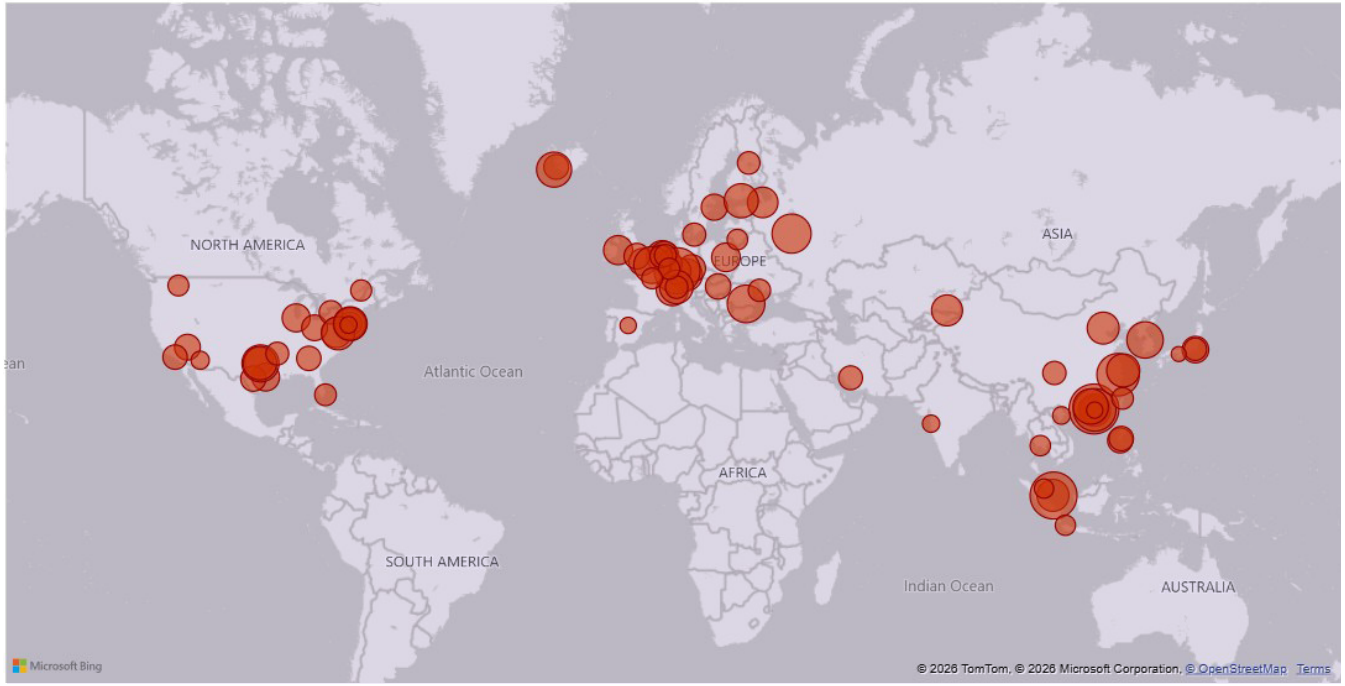
AdaptixC2 accounted for 1.5% of total OST output in 2025 (153 of 10,272 tracked OST instances). On a full-year basis, that places it below Havoc and Brute Ratel. However, the annual figure needs to be interpreted carefully.

AdaptixC2 is a new rule created in 2025. As a result, its annual totals are not directly comparable with full-year totals for other OST families, and its full-year percentage is likely to understate its relative prominence when viewed over an annual timeline.

Within the AdaptixC2 set itself, the US hosted 20.3% of all tracked AdaptixC2 infrastructure, followed by China at 18.3%, Germany at 9.8%, Singapore at 7.2%, and Hong Kong at 6.5%. The US and China together therefore accounted for 38.6% of all AdaptixC2 activity. In terms of total OST output, US-hosted AdaptixC2 contributed 0.30%, China 0.27%, Germany 0.15%, Singapore 0.11%, and Hong Kong 0.10%.

At the ASN level, the clearest concentration was in China. Beijing Baidu Netcom Science and Technology Co., Ltd. (AS38365) accounted for 6.5% of all global AdaptixC2 activity, Shenzhen Tencent Computer Systems Company Limited (AS45090) for 5.9%, and Hangzhou Alibaba Advertising Co., Ltd. (AS37963) for 3.3%. Together, those three ASNs accounted for 15.7% of all AdaptixC2 activity globally, and 85.7% of all China-hosted AdaptixC2.

Figure 8. C2 Infrastructure Mapping



In the US, the leading providers were Cogent Communications, LLC (AS174) at 2.6% of all global AdaptixC2, Eonix Corporation (AS62904) at 2.0%, and Amazon.com, Inc. (AS14618) at 1.3%. Together, those three ASNs accounted for 5.9% of all AdaptixC2 activity globally, and 29.0% of all US-hosted AdaptixC2.

The late-year trend is more important than the annual total. From October through December, we tracked more AdaptixC2 than Havoc or Brute Ratel each month.

In October, AdaptixC2 recorded 94 instances compared with 84 for Havoc and 73 for Brute Ratel. In November, AdaptixC2 recorded 90 compared with 70 for Havoc and 72 for Brute Ratel. In December, AdaptixC2 recorded 93 compared with 65 for Havoc and 63 for Brute Ratel. In our data, we have seen AdaptixC2 being used by Fog, Akira and BlackBasta. Even with the rule-coverage caveat, AdaptixC2 should be treated as an emerging OST to watch closely in the coming year.

Adversary Infrastructure Tracking

Information Stealers

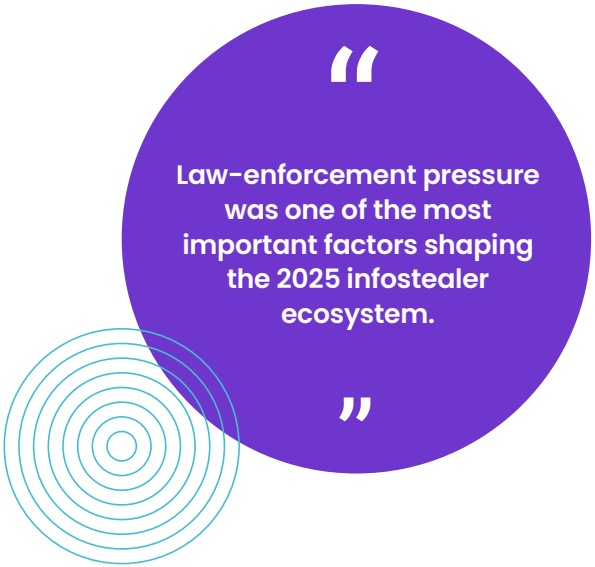
Information stealers (infostealers) remained a core component of adversary infrastructure in 2025, continuing to provide financially motivated threat actors with a reliable path to credential theft, session hijacking, cryptocurrency wallet access, and follow-on ransomware activity. As with our previous report, the infrastructure picture differs materially from the OST landscape: infostealer activity remains concentrated around mainstream cloud providers, European hosting, and recurring bulletproof or cyber crime-tolerant environments, rather than the China-heavy concentration seen across several OST families. In keeping with the structure of our previous report, the analysis below is based primarily on infrastructure-tracking data rather than victim compromise counts.

2025 Law-enforcement Operations

Law-enforcement pressure was one of the most important factors shaping the 2025 infostealer ecosystem. The most significant ecosystem-wide action was Operation Endgame 2.0, carried out between 19 and 22 May 2025. Eurojust said the operation (which was targeting initial-access malware at the beginning of the kill chain) took down more than 300 servers, neutralised 650 domains, and hit malware families including Bumblebee, Qakbot, DanaBot, HijackLoader, Trickbot, and WarmCookie. That matters for this dataset because loader and access-malware disruption can depress downstream infostealer deployment even when the stealer family itself is not named.

The most relevant direct infostealer action in May was the LummaC2 disruption. The US Department of Justice said it seized five internet domains used to operate the LummaC2 malware service and that the FBI had identified at least 1.7 million instances where LummaC2 was used to steal information, in addition to Microsoft simultaneously having moved against 2,300 related domains. Although Lumma is not a major driver in the specific 2025 workbooks used here, this was still the most important direct US action against an active infostealer service in 2025.

The clearest direct law-enforcement action against a family present in the 2025 workbooks came later in the year. On 13 November 2025, Eurojust and Operation Endgame announced a new phase, targeting Rhadamanthys, VenomRAT, and Elysium. Authorities reported 1,025 servers taken down worldwide, 20 domains seized and eleven searches conducted. For this dataset, that operation provides the strongest direct explanatory anchor for late-year disruption in a named infostealer family.



Adversary Infrastructure Tracking

2025 Overview

Across the uploaded 2025 infostealer workbooks, we tracked 3,843 infostealer instances in total. WhiteSnake Stealer was the most widely observed family, accounting for 31.6% of all tracked output, followed by RedLine at 23.9%, Rhadamanthys at 17.1%, and StealC at 6.9%. A second tier of activity included Mispadu at 4.8%, Ficker Stealer at 2.4%, ObserverStealer at 2.2%, Vidar at 2.1%, and Medusa Stealer at 1.8%. Within these workbooks, Lumma C2 accounted for only 0.6% of total tracked output.

Compared with our previous report, 2025's data presented a notably different picture. Last year's report described Lumma, RedLine, StealC and Meduza Stealer as the preferred infostealers of the year, with Lumma Stealer leading the way. It also highlighted a broad geography in which 30% of tracked infostealer C2 was located in the US, 20% in the Netherlands, and 16% in Russia. In 2025 however, the uploaded workbooks instead show a market led by WhiteSnake, while Lumma contributes only a very small share within this specific dataset. That does not necessarily mean Lumma ceased to be operationally relevant. Rather, it indicates that the infrastructure picture captured in these 2025 workbooks is less Lumma-centric and more distributed than in 2024. The same applies to geography. Across the four

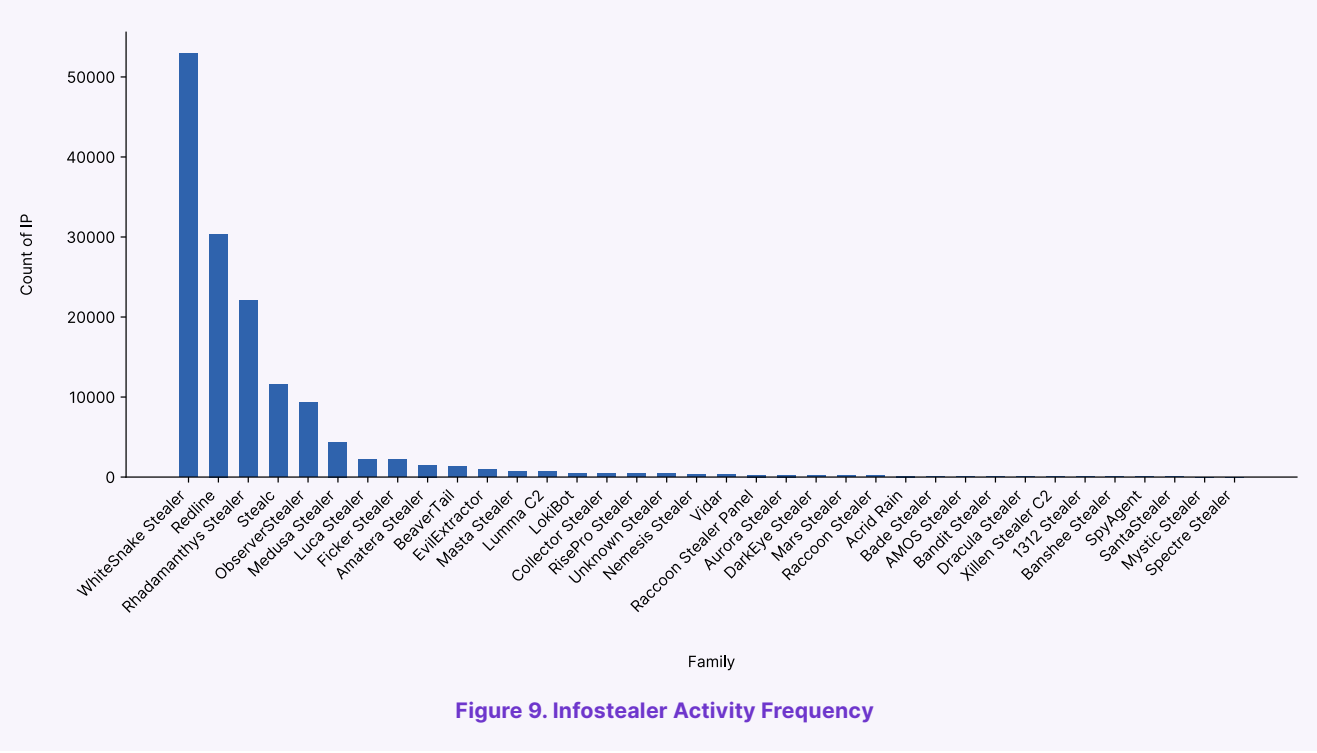


Figure 9. Infostealer Activity Frequency

families with dedicated country workbooks - WhiteSnake, RedLine, Rhadamanthys, and StealC - which together account for roughly 79.5% of all 2025 tracked infostealer output, the combined hosting picture is led by the US at roughly 19.0%, followed by Germany at 16.7%, the Netherlands at 13.2%, Russia at 10.1%, and China at 5.5%. These findings are still Western-cloud and Europe heavy, but reflect a more distributed picture than the 2024 US / Netherlands / Russia pattern found in last year's report.

Adversary Infrastructure Tracking

Key Observations

The most important change in 2025 was not simply that one family replaced another at the top of the table. The larger shift is from a Lumma-led 2024 environment to a more fragmented 2025 infrastructure market in which WhiteSnake, RedLine, and Rhadamanthys all occupy meaningful share, and where law-enforcement pressure appears to drive redistribution and substitution as much as outright suppression. The dominant pattern towards the end of the year is not collapse but rotation. Disruption affecting one family in November-December was offset by renewed growth in another.

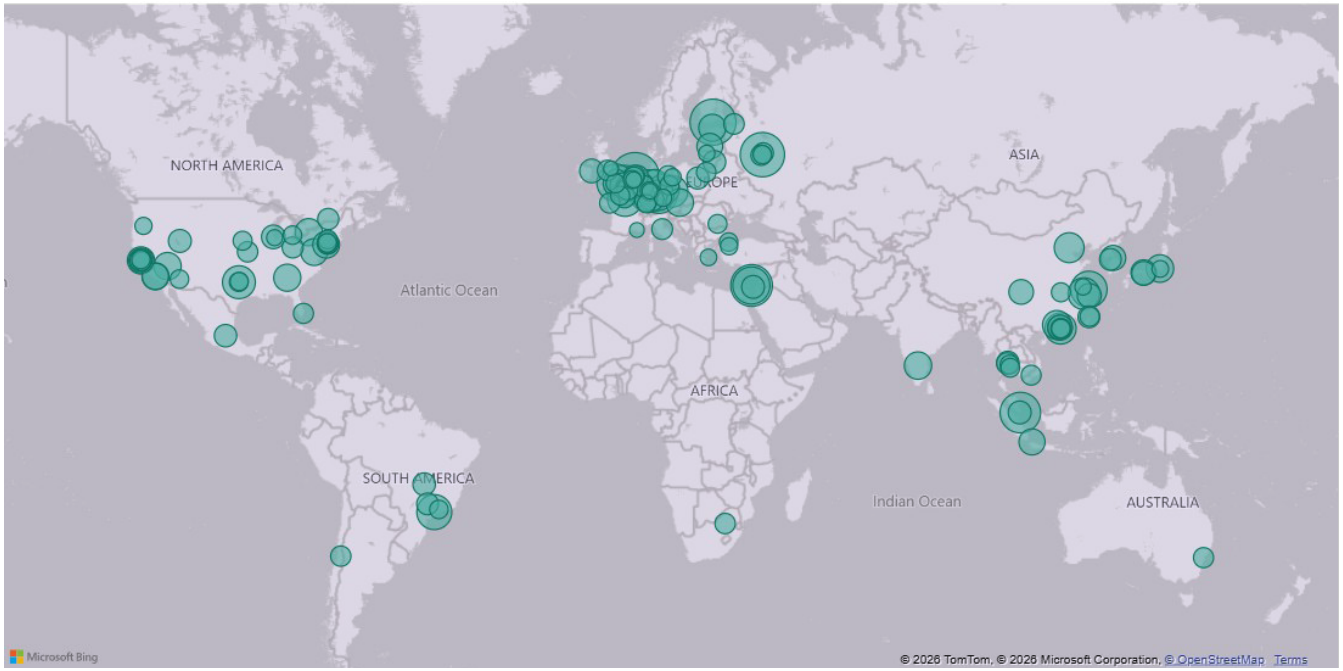
A second important change is that the 2025 leading families are, on the whole, less overtly Russia-centric than the 2024 RedLine picture. Our last report described RedLine as heavily Russia-hosted, with 55% of its backend infrastructure in Russia overall and 63% of RedLine C2 hosted in Russia after Operation Magnus. In 2025, RedLine remained important, but its country distribution was far more mixed, and the other leading families show stronger representation in the US, Germany, and the Netherlands.

A third important observation is that law-enforcement effects show up unevenly in infrastructure data. Mid-month disruption rarely produces a neat, same-month collapse. The more common pattern is a failed rebound, a country-mix shock, or a shift into adjacent families and ASNs in the following month.

Adversary Infrastructure Tracking

WhiteSnake Stealer

Figure 10. Infostealer Infrastructure Mapping



WhiteSnake Stealer was the single largest infostealer family in the 2025 dataset, accounting for 31.6% of all tracked output. Monthly share remained high throughout the year: 33.7% in January, 39.1% in February, 34.1% in August, 39.5% in September, and a peak of 41.8% in October, before declining to 28.8% in November and 18.6% in December. Within the WhiteSnake set itself, the US hosted 17.3% of all tracked WhiteSnake infrastructure, Germany hosted 15.3%, China hosted 12.7%, the Netherlands hosted 7.2%, and Russia hosted 5.9%.

Measured against total infostealer output, US-hosted WhiteSnake alone represented 5.5% of the full 2025 dataset, while Germany contributed 4.8% and China 4.0%. At the ASN level, WhiteSnake was comparatively distributed rather than concentrated in one or two ultra-dominant providers. AS24940 accounted for 9.7% of all WhiteSnake activity, followed by AS16276 at 5.8%, AS14061 at 5.5%, and AS37963 at 5.2%. That combination suggests a family operating across a mix of established European and global hosting environments rather than through a single dominant infrastructure basin.

Compared with last year's report, WhiteSnake is the clearest structural shift in the 2025 workbook set. Our previous report's infrastructure narrative was dominated by Lumma, which it described as the most dominant stealer on the market. In the 2025 workbooks, WhiteSnake takes that place instead. Because our previous report did not track WhiteSnake as a leading family, the comparison here is less about direct year-on-year continuity and more about market replacement: the top slot in the infrastructure dataset is no longer occupied by Lumma.

The late-year decline in WhiteSnake does not align with a verified direct WhiteSnake takedown. The more plausible explanation is second-order disruption following the November Operation Endgame phase and normal affiliate switching. In practical terms, WhiteSnake's November-December decline more closely resembles ecosystem turbulence than a named seizure.

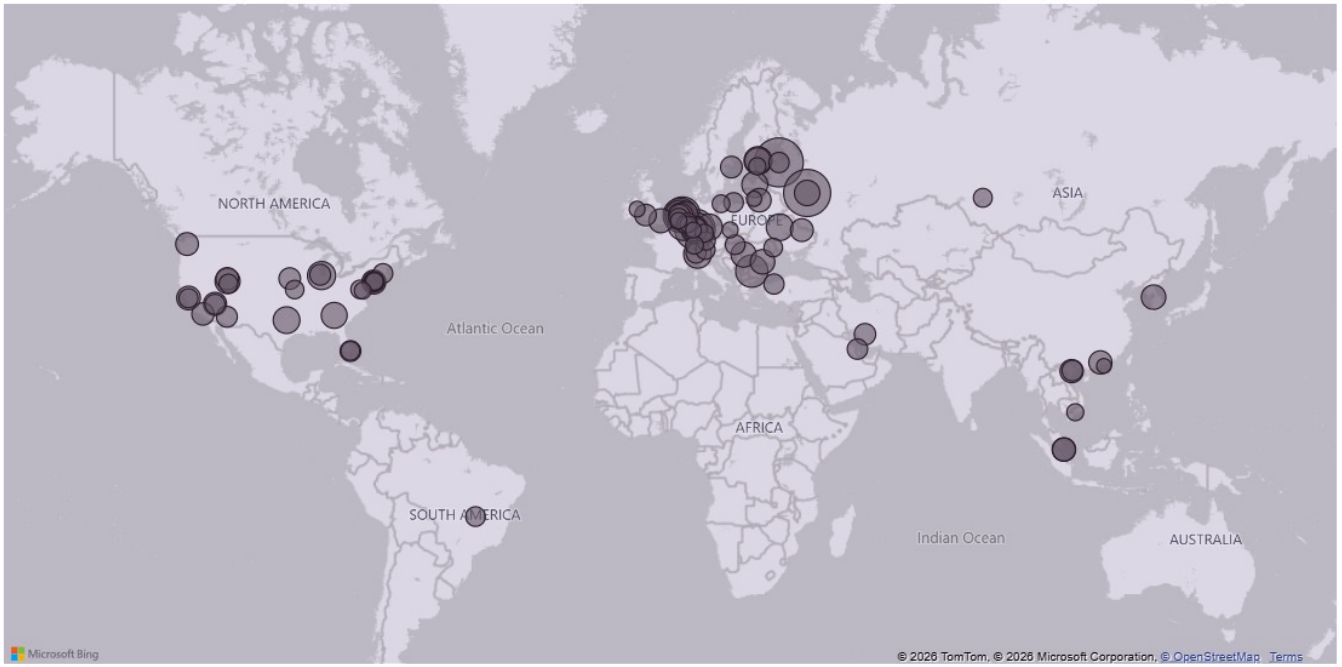
Adversary Infrastructure Tracking

RedLine

RedLine remained one of the most important infostealer families in 2025, accounting for 23.9% of all tracked output. Its monthly share rose steadily through most of the year, from 10.9% in January to 18.3% in April, 26.6% in August, and 36.9% in October, before easing to 27.3% in November and 24.8% in December. Within the RedLine data, we observed that Russia hosted 20.1% of all tracked infrastructure, followed by the US at 18.2%, the Netherlands at 17.0%, and Germany at 12.7%. Measured against the total infostealer output, Russia-hosted RedLine represented 4.8%, while the US contributed 4.3% and the Netherlands 4.1%. At the ASN level, the strongest annual concentrations were AS206728 at 7.4% of all RedLine activity, AS14956 at 7.1%, and AS207566 at 4.8%. The continued prominence of AS206728 and AS207566 matters because both show continuation of the broader RedLine pattern already described in last year's report.

Compared with 2024, RedLine's most important change is geographic. Our previous report described RedLine as heavily concentrated in Russia (55%), followed by Germany (10%) and Finland (9%), and further noted that 63% of all RedLine C2 was hosted in Russia after Operation Magnus, suggesting operators had simply shifted locations rather than disappeared. In the 2025 workbook set, Russia remains the single largest country, but only at 20.1%, while the US, Netherlands, and Germany all take far larger shares than they did in 2024. That is a material structural shift away from the Russia-heavy picture described last year.

Figure 11. Infostealer Infrastructure Mapping



The monthly pattern reinforces that point. Russia's share of RedLine falls sharply across the year, while the US, Netherlands, and Germany take more of the mix. That does not look like a fresh 2025 law-enforcement signature. It looks more like re-homing, diversification, and post-Magnus adaptation. In other words, RedLine in 2025 appears resilient not because it avoided pressure, but because it absorbed earlier pressure and redistributed.

Adversary Infrastructure Tracking

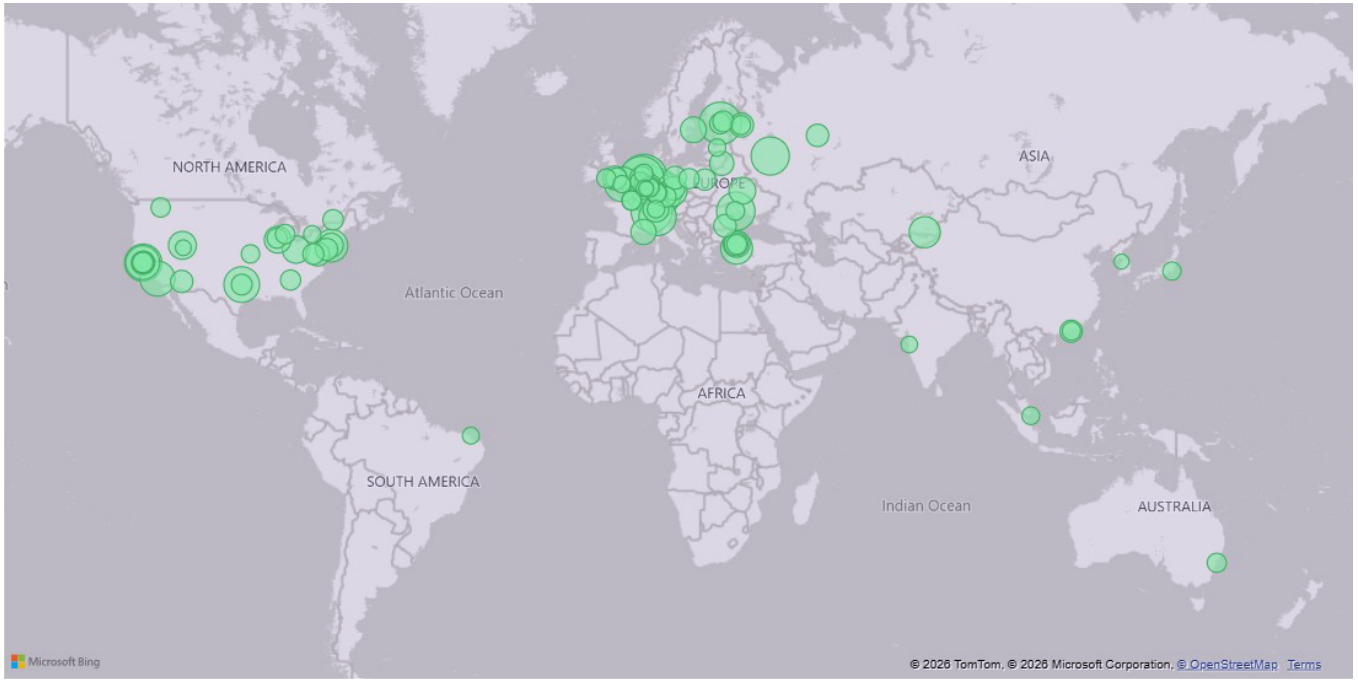
Rhadamanthys Stealer

Rhadamanthys was a new major family in the 2025 workbook set, accounting for 17.1% of all tracked output, where its monthly share rose from 11.1% in March to 20.0% in April and 24.7% in June, peaking at 32.3% in July. It then fell sharply from 22.8% in August to 5.7% in October, before rebounding to 32.2% in November and declining again to 14.8% in December. The data showed that Germany hosted 25.9% of all tracked infrastructure, while the Netherlands and US each hosted 19.0%. Measured against total infostealer output, Germany-hosted Rhadamanthys represented 4.4% of the full 2025 dataset, while the Netherlands and US each contributed 3.3%.

At the ASN level, Rhadamanthys too, was fragmented. AS44592 accounted for 6.7% of all Rhadamanthys activity, followed by AS24940 at 5.6%, AS41111 at 5.2%, and AS396073 at 5.0%. No single ASN dominated the family in the way certain providers do in more concentrated malware ecosystems.

Rhadamanthys also gives the clearest direct 2025 law-enforcement correlation. The November Operation Endgame phase explicitly targeted Rhadamanthys and removed 1,025 servers, 20 domains, and supported eleven searches. Importantly, the decline in Rhadamanthys begins before the November action, so the August-October collapse should not be attributed to law enforcement alone.

Figure 12. Infostealer Infrastructure Mapping



The stronger signal is that the November rebound does not hold and is followed by a sharp December decline, alongside a visible country-mix shock. That makes Rhadamanthys the strongest example of failed recovery after direct intervention, rather than a simple same-month collapse.

Adversary Infrastructure Tracking

StealC

StealC accounted for 6.9% of all tracked infostealer output in 2025, however, the annual figure obscures a very changeable monthly pattern. Moving from 6.2% in February through 5.1%, 4.2%, 13.7% and 12.5% from March to May respectively. It then dropped again to 4.8% in June and remained suppressed between roughly 1.6% and 2.5% from July through November, before showing another surge to 19.1% in December. The US hosted 29.5% of all tracked StealC infrastructure, followed by Germany at 14.1%, the Netherlands at 12.8%, Russia at 8.3%, and China at 4.5%. Measured against total infostealer output, US-hosted StealC contributed 2.0% of the total 2025 dataset. At the ASN level, StealC showed a clear concentration in AS37963, which accounted for 14.0% of all StealC activity. It was followed by AS132203 at 5.7%, AS25820 at 4.5%, and AS24940 at 4.2%. Relative to its modest annual size, that makes AS37963 unusually important for the family.

StealC is also one of the best examples of an indirect law-enforcement effect in the 2025 workbooks. Its sharp post-May decline aligns closely with Operation Endgame 2.0, which targeted the initial-access layer used to enable wider malware deployment. That is exactly the type of ecosystem-wide action that can suppress a family such as StealC without naming it. The December resurgence then suggests delivery-path recovery, affiliate rotation, or infrastructure substitution, rather than a return to uninterrupted continuity.

Figure 13. Infostealer Infrastructure Mapping

Adversary Infrastructure Tracking

Year-on-year Summary

The overall infostealer picture in 2025 shows both continuity and structural change. Continuity remains in the sense that information stealers still form a primary initial-access mechanism for cyber crime and ransomware operations, just as our previous report assessed. Last year's report highlighted Lumma, RedLine, StealC and Meduza as the dominant families, emphasised the importance of US, Dutch and Russian hosting, and noted that law-enforcement pressure reduced activity but did not prevent later resurgence. That broader logic still holds.

What changed in 2025 is the composition of the market. WhiteSnake replaced Lumma as the largest family in the associated datasets. RedLine remained a core family, but with a far more distributed annual geography than the Russia-heavy picture described in 2024. Rhadamanthys emerged as the clearest direct law-enforcement story of the year, while StealC provides the strongest example of indirect ecosystem disruption following loader takedowns. Most importantly, the late-year data suggests rotation rather than eradication. After November pressure, total tracked output did not collapse; instead, family shares shifted. Taken together, the 2025 dataset points to a more diversified, substitution-driven, and operationally resilient infostealer ecosystem than the one observed previously.

Spotlight: Emerging Stealer Upgrade - Vidar Stealer v2.0

Vidar is a relatively new entrant in this dataset, with the rule only appearing in December 2025. However, its early infrastructure profile is already notable. Although it accounted for only a small share of 2025, the hosting pattern in the CTI datasets is distinctive when compared to other stealer families reviewed here. Rather than clustering primarily around the US, the Netherlands, or Russia, Vidar is concentrated most heavily in Finland and Germany. From our data, Finland accounts for 42.7% of tracked Vidar infrastructure and Germany for 23.4%, with the US a distant third at 9.8%, making Vidar one of the clear outliers in this year's infostealer dataset from a hosting perspective.

The monthly pattern is also important, as it first appears in December 2025, then expands rapidly into early 2026. Specifically for Finland, it accounts for 42.0%, 52.8%, 49.4% and 38.1% of activity each month between December and March. Germany remains the second most associated location, accounting for 27.2% in December, 14.7% in January, 19.8% in February, and 26.6% in March. This consistency suggests that this is not random/short-term noise, but likely the early shape of an infrastructure pattern that differs from the broader 2025 stealer market. Looking at the ASN data, Vidar also shows a stronger concentration than might be expected for a newly observed family. AS24940 alone accounts for 32.9% of all tracked Vidar activity, including 17.6% hosted in Germany and 32.9% overall through Finland-linked infrastructure, suggesting that its early footprint is not only geographically unusual, but also tied to a relatively narrow infrastructure base.

Open-source reporting gives useful context for why this family may be becoming more relevant. On 6 October 2025, the developer known as "Loadbaks" announced Vidar Stealer v2.0 on underground forums. Trend Micro reported that the new version had been fully rewritten from C++ into pure C, introduced multithreaded architecture, and added improved anti-analysis and browser-credential theft capabilities, including techniques to bypass newer browser protections through memory injection. Trend Micro also assessed that Vidar 2.0's release coincided with the decline in Lumma Stealer activity, with threat actors increasingly looking at alternatives (i.e., Vidar & StealC). Vidar's importance here is not its absolute 2025 share, but the fact that it appears late, expands quickly and does so with a hosting geography that looks overtly different from the consistently active 2025 families, and therefore, we expect Vidar to continue presenting as an emerging infostealer variant through 2026.

Information Stealer Ecosystem

In 2025, Bridewell has continued to track and analyse the evolving threat of information stealers, which remain a primary enabler of modern cyber crime. Across the year, we observed information stealer operations becoming more industrialised: MaaS ecosystems matured, credential and session-token theft became a routine precursor to intrusions, and disruption operations increasingly targeted both infrastructure and the wider criminal supply chain.

The following analysis explores the 2025 infostealer landscape, highlighting major malware families, compromise trends, and the impact on downstream threats such as ransomware and business email compromise.

Global Information Stealer Landscape

Since its emergent popularity began to take form across the broader cyber security industry, the infostealer has proven itself a scalable and effective skeleton key among routine tools used by threat actors. It has steered attackers from primarily hacking for access to identity exploitation, functioning as an inherent mechanism for detection evasion from the outset. This mirrors insider-threat behaviour, which is a well-known investigative challenge for security teams.

Additionally, the transactive nature of harvested credentials seamlessly fits the increasingly commoditised nature of cyber crime, which serves any and all manner of willing parties across a myriad of anonymised forums and channels. The nature of valid account credentials is now a logical element within the established threat actor economy.

Where measures to detect insider threats are typically aligned to internal user monitoring, those for the presence of infostealers primarily focus on the external devices of users. Proactively scanning known and publicised breaches is now an encouraged approach to monitor for users' credentials to swiftly close active sessions and issue password resets on identification. However, the scale of the problem increases again when factoring in organisations who are operationally accessible to critical supply chains and third-party relationships.

Rising Trends in Infostealer Compromises

Across 2025, infostealer activity continued to be defined by high-volume infections, rapid operational recovery, and constant tradecraft iteration. Rather than relying on exploitation alone, many infostealer campaigns leaned heavily on social engineering and consent-based execution, with the aim of harvesting credentials, browser data, and session tokens/cookies that can enable account takeover, even where MFA is in place.

The data for compromised devices throughout 2025 shows a consistent pattern of incidents, with notable fluctuations in certain months. The most significant anomaly occurred in March 2025, when the number of compromised devices spiked dramatically, particularly due to a major cyber attack on Amazon. During this month, users were hit the hardest, with over 5.3 million affected.

Employees were also impacted, with 7,849 compromised, while third-party entities saw 8,519 incidents. This surge can be traced to the discovery of a cyber attack by the Babuk2 ransomware group, which utilised infostealer malware to steal sensitive data from both employees and users, as well as external partners.

Following March, the number of compromised devices dropped sharply, with April and subsequent months showing much lower figures. For example, April saw a significant reduction in incidents, with only 1,074 employees, 19,097 users, and 1,329 third parties compromised. The rest of the year exhibited relatively stable levels of activity, though there were slight increases in certain months, such as June and December. These fluctuations emphasise that while the March spike was an outlier, the overall threat landscape remained active, with occasional peaks in certain months driven by ongoing cyber incidents and threats.

Information Stealer Ecosystem

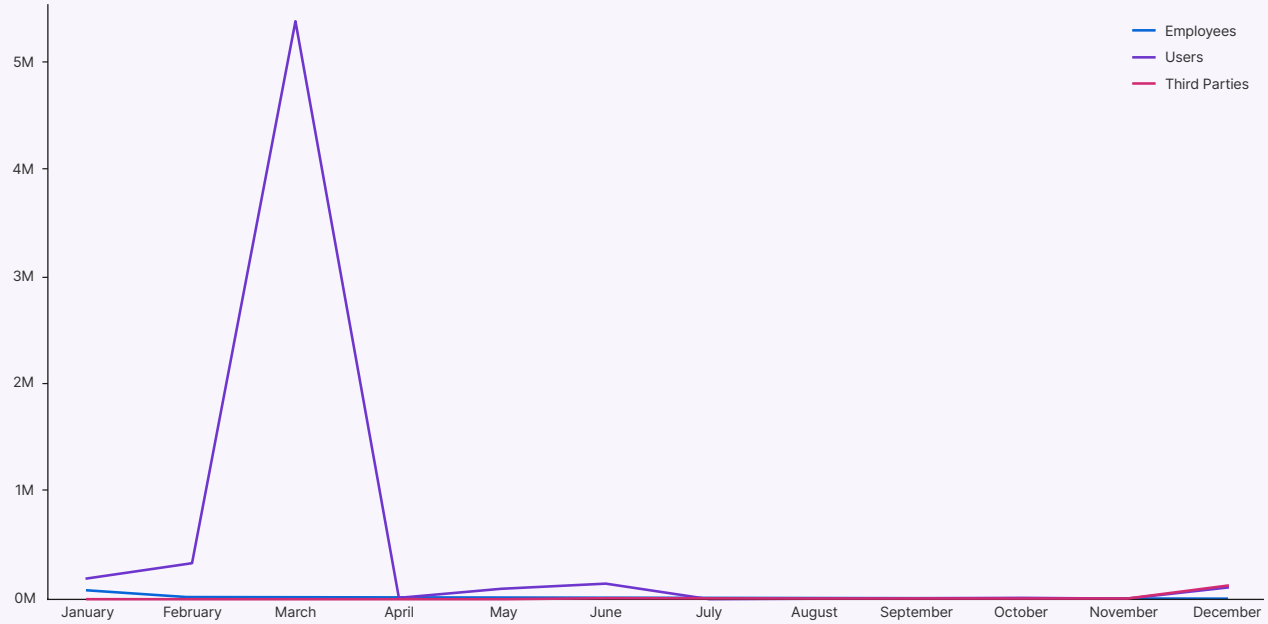


Figure 14. Compromised Devices Throughout 2025

When comparing the 2025 compromised device data to 2024, there are notable differences in both the patterns and scale of incidents. In 2024, the number of compromised devices remained relatively high throughout the year, with users being consistently impacted in large numbers, peaking in July with over 600,000 compromised. The employee data in 2024, represented by the lighter blue line (see Figure 15), showed a much lower volume compared to users, maintaining a steady trend with smaller peaks, especially in January and December. This contrasts with 2025, where we saw a massive spike in March, driven by a significant cyber attack on Amazon, affecting both employees and users on an unprecedented scale. Overall, 2025 was marked by a singular, dramatic event that caused an extraordinary spike, while 2024 demonstrated more gradual, persistent activity.

Two trends were especially notable:

1. Industrial-scale MaaS disruption and recovery in 2025 demonstrated that takedowns can materially reduce attacker capability in the short term, but also that top-tier MaaS operators and affiliates can adapt quickly and reconstitute delivery and command infrastructure.

2. Infostealers increasingly prioritised browser artefacts (cookies, saved sessions, autofill, wallet extensions) and environmental profiling to support follow-on access and fraud, demonstrating a shift in credential theft objectives from passwords to authenticated sessions.

Global Disruption of Lumma Stealer (May 2025)

A defining moment in 2025 was the coordinated action against Lumma Stealer (LummaC2) - one of the most prevalent infostealers in the cyber criminal ecosystem. Microsoft's Digital Crimes Unit (DCU) reported seizing and facilitating the takedown, suspension, and blocking of approximately 2,300 malicious domains underpinning Lumma's infrastructure, alongside broader partner activity targeting Lumma's ecosystem and marketplaces.

Microsoft also stated that it identified over 394,000 Windows computers globally infected within the period 16 March to 16 May 2025 and described actions to sever communications between victims and the malicious tool. Lumma's scale and ease-of-use made it a key commodity infostealer that frequently fed credentials into wider criminal workflows (fraud, account takeover & initial access brokering). Disrupting its domains and control mechanisms increased friction and imposed rebuild costs on both operators and customers

Information Stealer Ecosystem

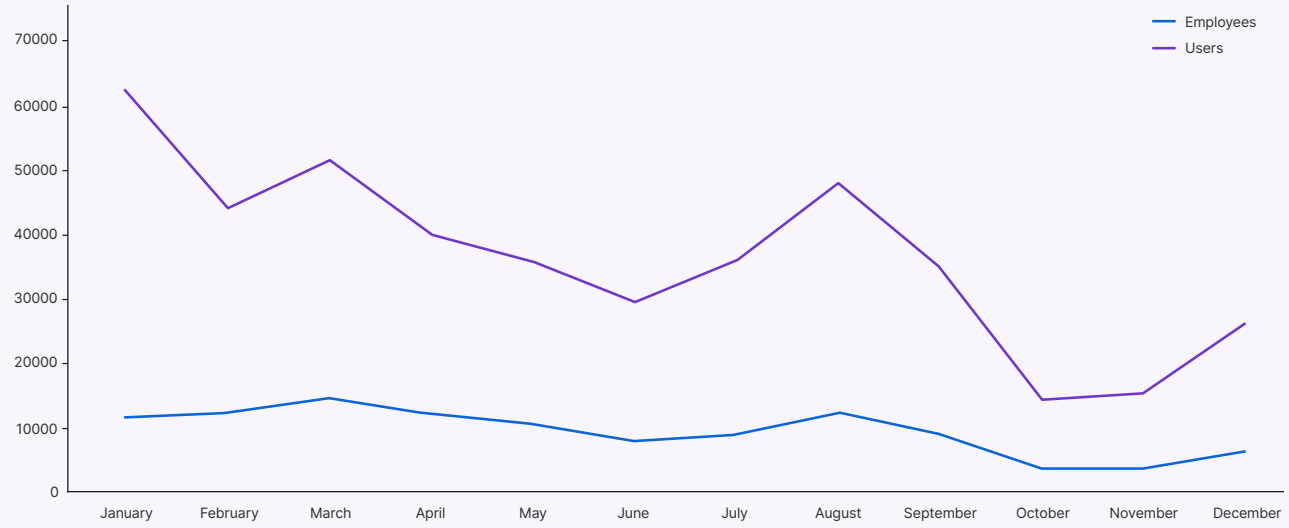


Figure 15. Compromised Devices Throughout 2024

Operation Endgame & Continued Pressure on Cyber Crime Enablers (2025)

Law enforcement momentum against ransomware enablers continued through 2025, including actions aimed at malware services and infrastructure that facilitate mass compromise and secondary payload delivery. A latter phase of Operation Endgame (coordinated from Europol HQ between 10–13 November 2025) explicitly targeted the Rhadamanthys infostealer, VenomRAT, and the Elysium botnet, reporting 1,025+ servers taken down or disrupted and 20 domains seized, alongside arrests and searches. Rhadamanthys is often positioned as a high-value infostealer within the MaaS ecosystem; taking down infrastructure at this scale can reduce log availability, disrupt log shop supply, and degrade the reliability of initial access pipelines used by wider cyber criminal operations.

Infostealer Tradecraft Evolution in 2025

Lumma's adaptation: Even after major disruption, top infostealers showed an ability to evolve. Trend Micro reported that Lumma activity rebounded later in 2025 and highlighted the emergence of browser fingerprinting as part of Lumma's updated C2 approach, which now incorporated collecting system and browser characteristics to support evasion and victim profiling. This reflects a broader 2025 pattern of infostealers increasingly behaving less like smash-and-grab malware and more like intelligence-gathering tools designed to maximise the value of stolen sessions and facilitate follow-on access decisions.

ClickFix / FakeCAPTCHA-style lures: ESET's H2 2025 reporting tied Lumma distribution strongly to FakeCAPTCHA sites used in ClickFix-style social engineering illustrating how infostealers continued to benefit from user-driven execution paths rather than exploits. ESET also noted a material reduction in Lumma detections later in 2025 after earlier disruption, while pointing to the prevalence of FakeCAPTCHA lures as a key vector.

Information Stealer Ecosystem

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

Bridewell's intelligence analysis throughout 2025 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 infostealer strains affecting UK business, 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 infostealer threat landscape. Figure 16 shows the top five stealer families affecting the UK in 2025.

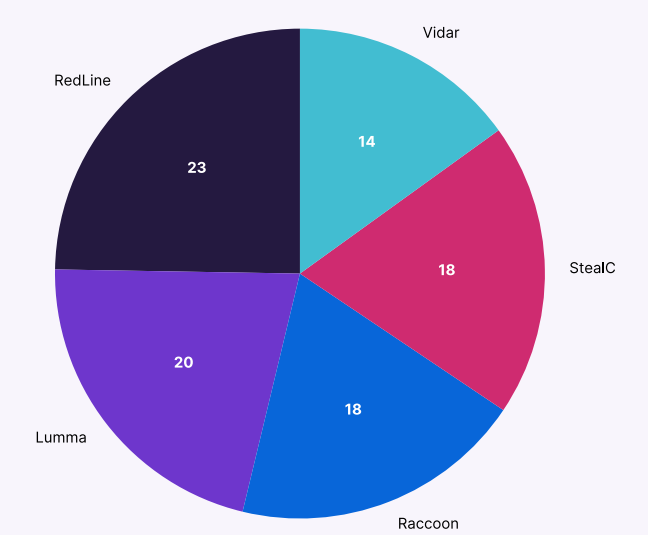


Figure 16. Top 5 Stealer Families Affecting the UK in 2025

Information Stealer Ecosystem

Dominance of Redline and Lumma in UK-Based Attacks

In both 2024 and 2025, Lumma and RedLine have remained the most prominent infostealers in UK-based cyber crime, though there is a noticeable shift in their relative popularities. In 2024, Lumma was the dominant tool, accounting for 41.2% of the compromised devices, followed by RedLine at 31.96%. Lumma's significant share can be attributed to its rapid growth as a MaaS tool, offering ease of deployment and a wide range of capabilities that made it highly effective in stealing credentials, session tokens, and autofill data. Its prevalence during this period reflects a shift towards more accessible, MaaS-based attacks.

However, by 2025, RedLine had seen a rise in usage, growing to 15.86%, while Lumma experienced a decline, dropping to 13.79%. This shift indicates that RedLine continues to maintain its position as a highly versatile and affordable tool in the cyber criminal market. Despite being one of the longest-standing infostealers, RedLine's affordability and adaptability make it a reliable choice for cyber criminals targeting a range of sectors, including finance, retail, and legal.

The data suggests a trend where RedLine is increasingly favoured, possibly due to its effectiveness in compromising large volumes of data. Meanwhile, Lumma, despite its earlier dominance, appears to be losing ground to newer or evolving tools.

The Continued Threat of Raccoon and Emerging Variants

In 2025, Raccoon Stealer has experienced a resurgence, becoming the third most prevalent infostealer in the UK, accounting for 12.41% of total incidents, rising from 0.29% in 2024. Raccoon is known for its versatility and ability to exfiltrate a wide range of sensitive information, including credentials and cookies.

Meanwhile, StealC, which had accounted for 23.61% of infections in 2024, has seen a decrease in 2025, dropping to 12.41%. This decrease, however, may be partly due to the 2025 dataset including a larger variety of infostealer families compared to the more limited set in 2024. In 2024, there were only six prominent malware families, with StealC taking up a larger share. In 2025, with a broader range of infostealers, StealC's relative percentage has declined. Despite that decline, StealC continues to be an important player in multistage infection chains, often deployed to steal credentials and establish an initial foothold for further compromise. Bridewell's internal C2 tracking confirms a steady rise in StealC infrastructure and operational activity throughout 2025, despite a brief resurgence earlier in the year.

Other infostealers like Vidar and Atomic still appear in UK-targeted campaigns, but they remain less common, often used opportunistically in MaaS or Initial Access-as-a-Service operations.

"Despite being one of the longest-standing infostealers, RedLine's affordability and adaptability make it a reliable choice for cyber criminals targeting a range of sectors, including finance, retail, and legal."

Information Stealer Ecosystem

Information Stealers and RaaS Ecosystem

Throughout 2025, Bridewell observed a growing overlap between 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 infostealers 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, Bridewell 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.

Ransomware Incidents Involving Information Stealers (2025)

The following section provides insights and figures to illustrate how information stealers have contributed to ransomware incidents across different sectors and regions in 2025.

Figure 17 shows a breakdown of ransomware incidents linked to information stealers across various industries. The technology sector (12.69%) is the most frequently targeted, followed closely by manufacturing (11.46%) and healthcare (6.98%). These industries store valuable credentials and sensitive client data, making them prime targets for credential-harvesting malware before ransomware deployment.

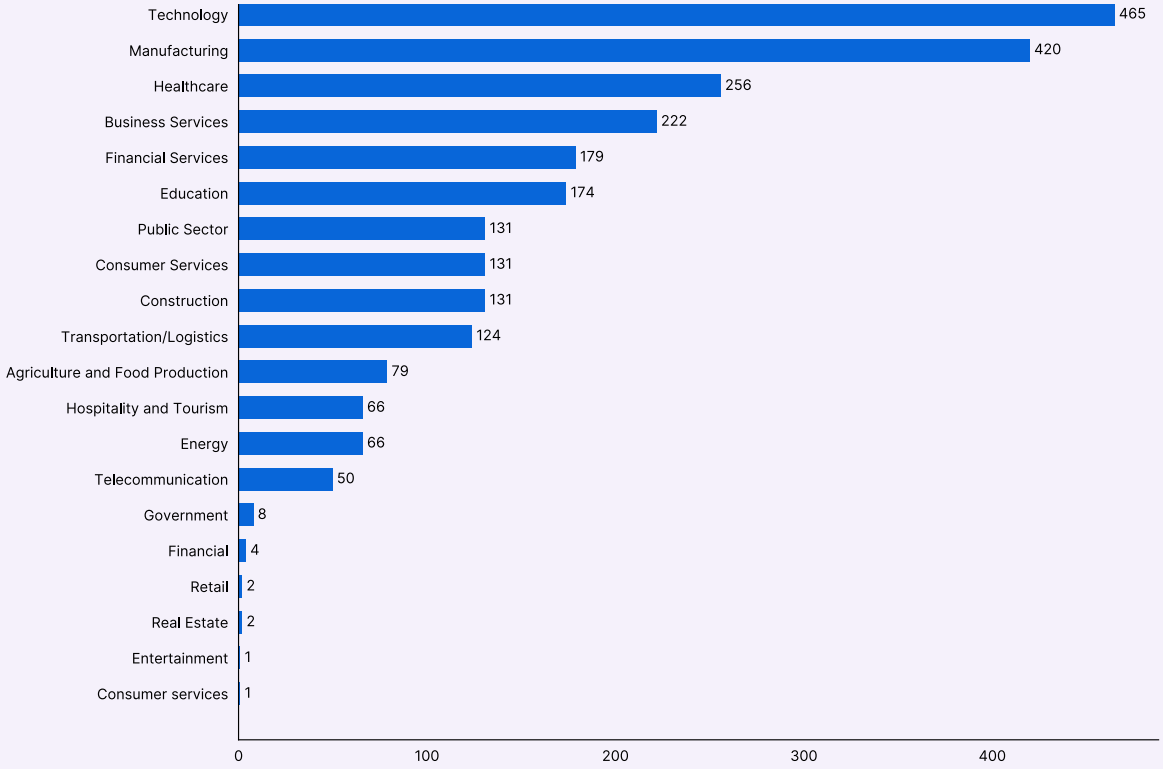


Figure 17. Impacted Sectors Throughout 2025

Information Stealer Ecosystem

Figure 18 uses UK-specific data to highlight that financial services, telecommunication, technology, transportation and healthcare were the top five 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.

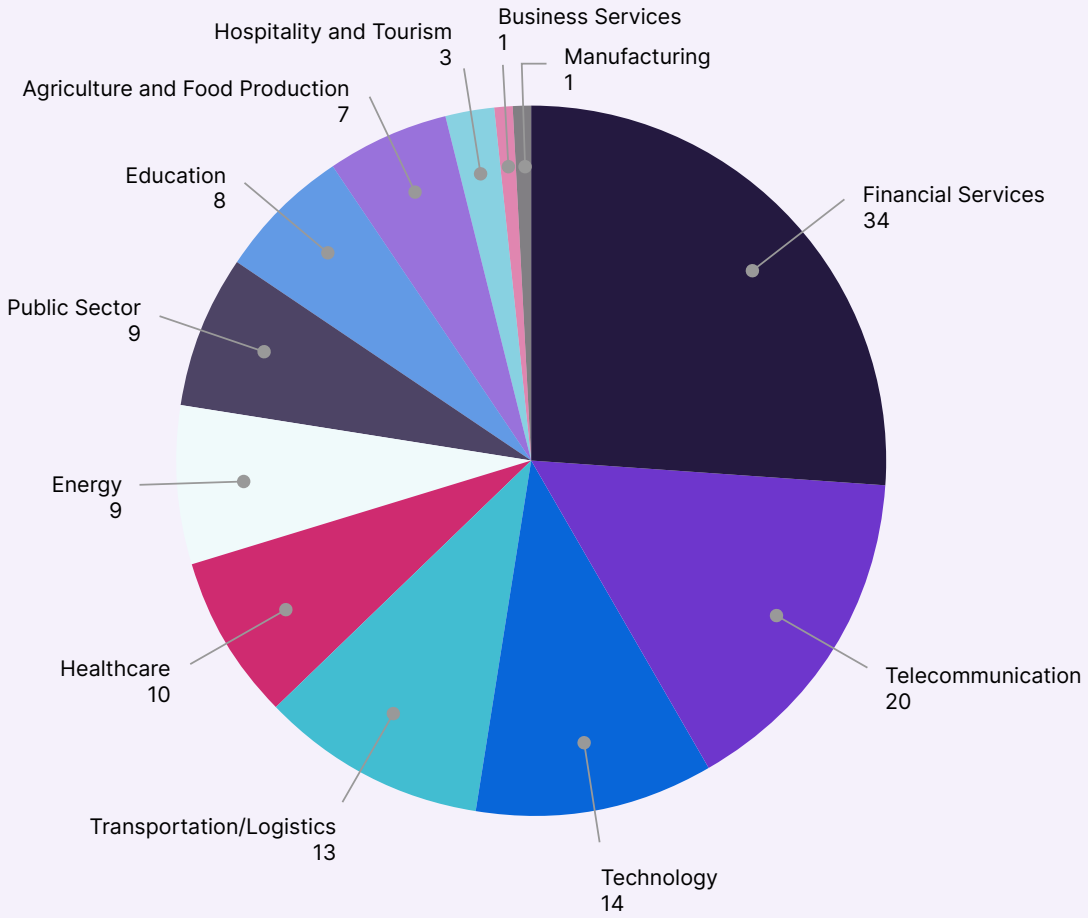


Figure 18. UK Sectors Impacted by Information Stealers in 2025

Information Stealer Ecosystem

Figure 19 shows that Redline, Raccoon, StealC, Lumma and Vidar were the top five 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.

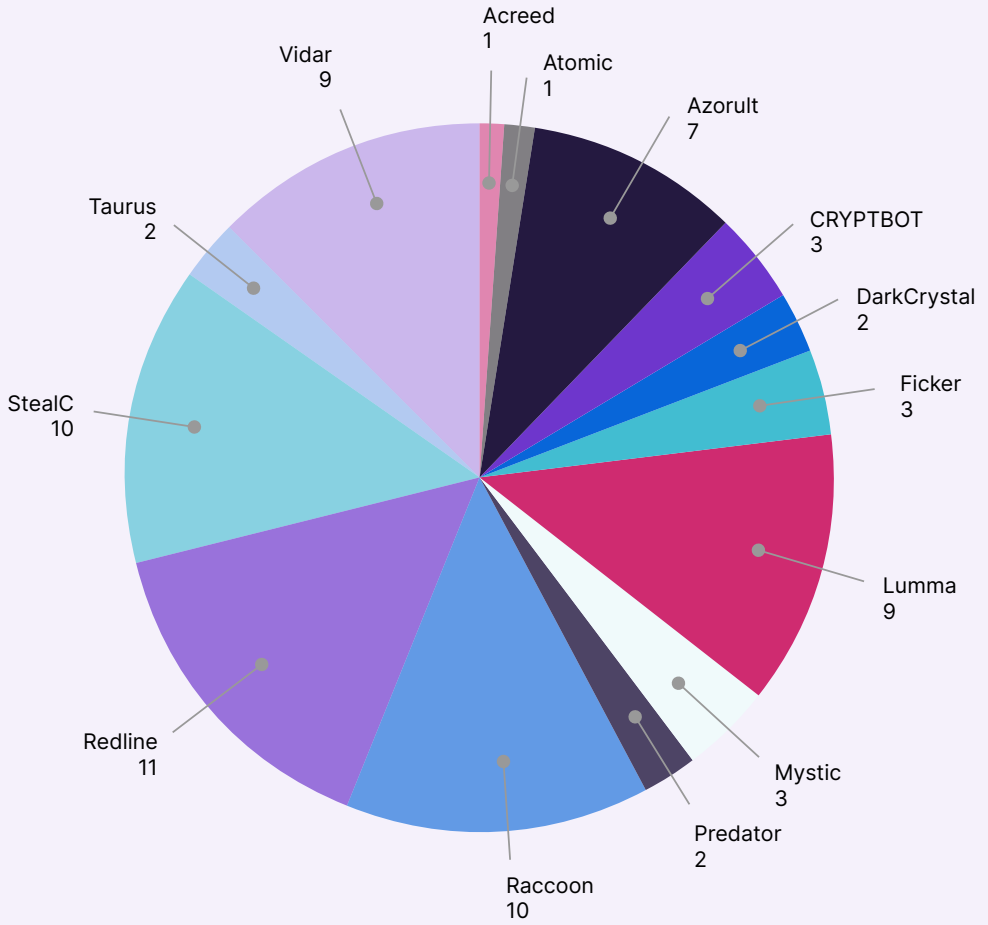


Figure 19. Ransomware Related Incidents Affecting CNI in 2025

Information Stealer Ecosystem

Figure 20 reveals that UK financial services, telecommunication, healthcare, energy and public 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.

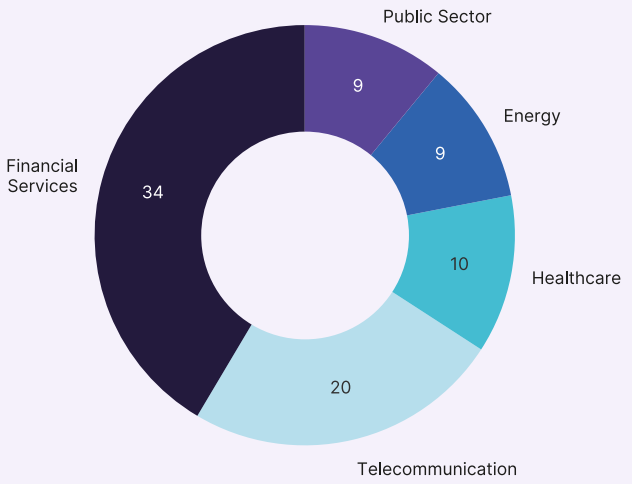


Figure 20. UK Sectors Impacted by Ransomware Involving Information Stealers

Usage of Information Stealers Across Incidents (2025)

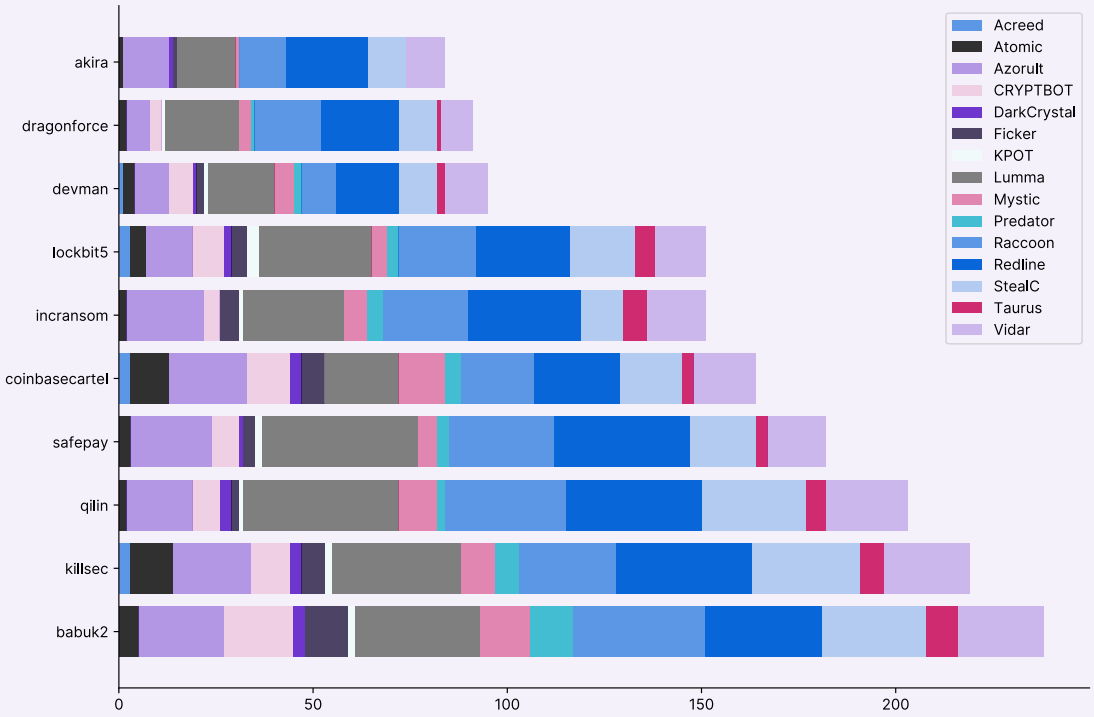


Figure 21. Ransomware Groups Usage of Information Stealers in 2025

Figure 21 provides insight into which ransomware groups have been actively using infostealers as part of their attack chain. Babuk2 and Killsec are the most prolific users of infostealers, incorporating strains such as Raccoon, Lumma, Redline, StealC and Vidar into their infection process. Qilin and Safepay also show strong associations with Lumma and StealC, indicating that these groups have deep ties to infostealer-based credential harvesting.

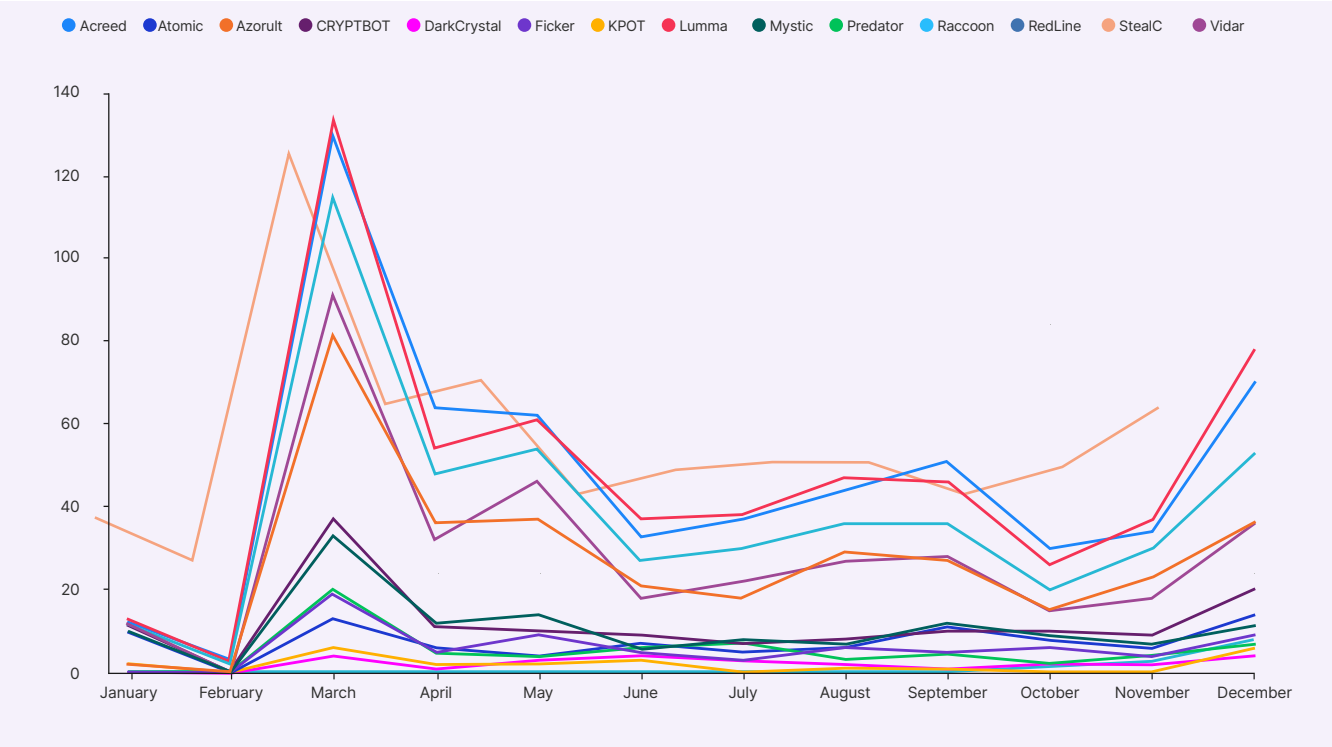
The diversity of infostealers across different ransomware groups suggests that cyber criminals purchase stolen credentials from various underground sources, rather than relying on a single supplier. The inclusion of Vidar and DarkCrystal among certain ransomware groups suggests that some attackers are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

Information Stealer Ecosystem

Information Stealers Used Across Ransomware Incidents (2025)

Figure 22 tracks how the use of different information stealers evolved in ransomware incidents throughout 2025.

Figure 22. Information Stealers Used Across Ransomware Incidents Throughout 2025



Throughout 2025, information stealer activity was heavily concentrated around a core group of families, consisting of RedLine, Vidar, Raccoon, Lumma, StealC, and Azorult which drove ransomware-related incidents across the year. All six stealers show a sharp and simultaneous spike in March, far exceeding activity in any other month, indicating a coordinated surge in campaigns or increased affiliate adoption. Unlike many other stealer families, these leading stealers maintain a steady baseline of activity in the months that follow, reinforcing their role as dependable tooling for credential harvesting and initial access. RedLine remains particularly consistent throughout the year, while Vidar and Raccoon closely mirror each other's usage patterns. Lumma, StealC, and Azorult also contribute significantly to the March peak and maintain sustained, moderate activity across subsequent months, with a noticeable uptick again toward the end of the year.

Other infostealers, including DarkCrystal, Atomic, KPOT, Mystic, and Predator, follow a similar overall pattern, with visible spikes in March and smaller increases later in the year, but at significantly lower volumes. Their activity is less consistent, often dropping to minimal levels between peaks, suggesting they are used more sporadically or in more targeted operations rather than being widely adopted across ransomware affiliate ecosystems.

Information Stealer Ecosystem

Information Stealer Key Takeaways

Bridewell's analysis of information stealer activity in 2025 highlights the continued central role these malware families play in enabling ransomware and wider cyber crime operations. A core group of stealers such as RedLine, Vidar, Raccoon, Lumma, StealC, and Azorult consistently drove activity throughout the year, demonstrating both resilience and sustained adoption across threat actor ecosystems. The data also reflects how infostealer usage is increasingly tied to campaign-driven surges, with significant spikes followed by periods of stabilisation, rather than purely continuous growth.

Beyond the dominant families, a broader set of stealers continues to operate at lower volumes, aligning with the same campaign cycles but lacking the consistency and scale of leading tools. This reinforces the trend that while the infostealer landscape remains diverse, a relatively small number of mature, MaaS-enabled families underpin most of the credential theft and initial access activity, posing ongoing risks to organisations reliant on identity, session security, and endpoint visibility.

> **"Infostealer usage is increasingly tied to campaign-driven surges, significant spikes followed by periods of stabilisation, rather than purely continuous growth."**

CNI SOC/MDR Service Detection Analysis

C2 Detection Analysis 2025

We use our malicious infrastructure tracking dataset to enable our MDR customers to detect and prevent threats. The following sections provide insight into the C2 detection alerts we observed within our client environments throughout 2025.

Intelligence Gaps

During onboarding, it is common for untrusted or public networks to be connected prior to ongoing tuning and alert management activity. This can impact the dataset, but we currently include all alerts and call this out as a limitation of the current collection process.

Bridewell's C2 detection capability identified 42 unique C2 families operating across 118 distinct IP addresses during the reporting period. Offensive security tools and remote access trojans (RATs) together comprised 61.7% of all observed C2 activity (262 OST + 93 RAT of 575 total alerts), marking a shift from 2024 where traffic distribution systems held the secondary position.

Top C2 Threat Alerts

The table below displays the top 10 C2 threat alerts observed in client environments in 2025 as a proportion of total alert volume. The top five threats alone accounted for 73.91% of all alerts, with the remaining 37 C2 families sharing the other 26.09%. The threat landscape shifted considerably from the prior year, with RATs displacing traffic distribution systems as the second most prevalent category we tracked.

Rank	Threat	Alerts	% of Total
1	Burp	223	38.78%
2	Xtreme-RAT	78	13.57%
3	ApateWeb	47	8.17%
4	BR-UNC-009	45	7.83%
5	SocGholish	32	5.57%
6	Web Skimmer	19	3.30%
7	Shadow Syndicate	18	3.13%
8	Collector Stealer	14	2.43%
9	Sliver	11	1.91%
10	Deimos C2	9	1.57%

Table 1. Alerting for C2 Threats

CNI SOC/MDR Service Detection Analysis

Top 5 Alerts

1. Burp Collaborator

38.78% (223 alerts)

The most prominent C2 alert observed was Burp Collaborator, representing 38.78% of all alerts – more than a third of the annual total. Burp Collaborator provides custom implementations of various network services used for out-of-band vulnerability detection. Critically, 79.4% of its annual activity was concentrated in a single month (August) with 177 of 223 alerts occurring during this period. We assess with low confidence that this could indicate a coordinated reconnaissance campaign across monitored environments for a zero-day vulnerability related to Oracle that was targeted at the time. Burp alerts were detected across 81.0% of all monitored MDR environments, making it the most broadly distributed threat observed.

2. Xtreme-RAT

13.57% (78 alerts)

Ranking second was Xtreme-RAT at 13.57%, a commodity RAT that was exclusively concentrated in Q4 (100% of alerts occurred in Q4). Remarkably, 82.1% of its annual alerts occurred in December alone (64 of 78 alerts), detected across approximately 66.7% of MDR environments. Xtreme-RAT was not present in the 2024 top 10, marking it as a significant emerging threat amongst the dataset.

3. ApateWeb

8.17% (47 alerts)

Third was ApateWeb at 8.17%, a network of domains containing embedded JavaScript redirectors used to deliver victims to pages containing scams, scareware, and potentially unwanted programmes. Unlike other top threats which exhibited sharp temporal spikes, ApateWeb maintained a consistent presence across all four quarters:

- Q1: 8 alerts (17.0%)
- Q2: 9 alerts (19.1%)
- Q3: 14 alerts (29.8%)
- Q4: 16 alerts (34.0%)

ApateWeb was detected in approximately 66.7% of environments. This persistent, gradually increasing pattern is characteristic of ongoing TDS operations.

4. BR-UNC-009

7.83% (45 alerts)

Fourth was BR-UNC-009 at 7.83%, a Bridewell-tracked uncategorised threat cluster that has not yet been attributed to a known threat actor or malware family. Approximately 62.2% of BR-UNC-009 alerts occurred during a single spike in October (28 of 45 alerts), detected across 61.9% of client environments. This cluster is under active investigation by the Bridewell Threat Intelligence team for attribution analysis.

5. SocGholish

5.57% (32 alerts)

Completing the top five was SocGholish at 5.57%, a JavaScript-based malware delivery framework that uses fake browser updates as a delivery mechanism. Activity was concentrated in Q1 and Q2, with 22 alerts in Q1 and reduced activity thereafter. SocGholish was detected across 38.1% of client environments.

CNI SOC/MDR Service Detection Analysis

Top C2 Alert Categories

C2 alerts were classified into 17 operational categories based on 575 total records. OSTs represented the largest share at 45.57% (262 intrusions), followed by RATs at 16.17% (93 intrusions), and TDS at 8.35% (48 intrusions). Together, OST and RAT accounted for 61.7% of all observed activity.

This represents a notable composition where OST dominates the threat landscape. Phishing activity accounted for 8.17% (47 intrusions), while the IAB represented 5.57% (32 intrusions), indicating active threat actor operations to establish footholds in client environments.

Quarterly composition reveals distinct seasonal patterns:

Quarter	Total Alerts	Top Category	Dominant Threat
Q1	98 (17.0%)	OST - 32.7%	SocGholish (22 intrusions)
Q2	78 (13.6%)	OST - 39.7%	Web Skimmer (17 intrusions)
Q3	222 (38.6%)	OST - 85.6%	Burp Collaborator (189 intrusions)
Q4	177 (30.8%)	RAT - 44.1%	Xtreme-RAT (78 intrusions)

Table 2. Quarterly Threat Distribution

Q3 represented the highest activity period with 222 alerts, where OST accounted for 85.6% of all activity driven by the Burp Collaborator spike (189 intrusions representing 85.1% of Q3).

RAT activity showed strong presence in Q4, with Xtreme-RAT alone accounting for 44.1% (78 intrusions) of Q4 alerts. The phishing category's proportional share grew significantly between Q1 (5.1% of quarterly volume, 5 intrusions) and Q4 (18.6%, 33 intrusions) a 3.6-fold increase driven primarily by the BR-UNC-009 cluster, which accounted for 45 total intrusions (7.83% overall) with 33 occurring in Q4.

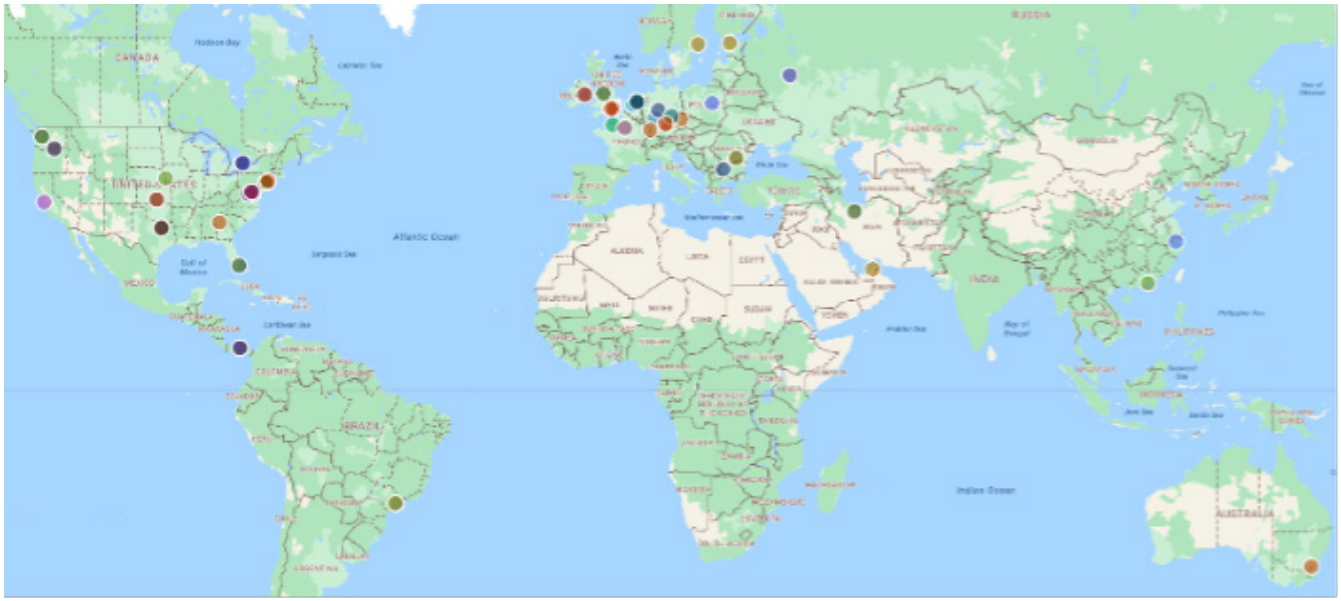
Remaining category breakdown:

- **TDS/Redirector activity:** 8.35% (48 intrusions) from ApateWeb (47 intrusions) and related campaigns
- **Information Stealer alerts:** 5.04% (29 intrusions) from Collector Stealer (14), Redline (8), and StealC (5) variants
- **Skimmer activity:** 3.30% (19 intrusions) from web skimmer operations
- **Ransomware:** 3.30% (19 intrusions) from Shadow Syndicate (18) activity
- **Backdoor/Implant activity:** 0.87% (5 intrusions) - significantly lower than prior year
- **Initial Access Broker:** 5.57% (32 intrusions) from SocGholish (32) activity

CNI SOC/MDR Service Detection Analysis

Geographic Distribution

This section summarises the geographic distribution and threat-group mix observed in the MDR alerts dataset.



Region	Alert Count	Percentage
North America (US + Canada)	336	58.43%
Europe	190	33.04%
Middle East	10	1.74%
Russia	21	3.65%
Asia-Pacific	12	2.09%
South America	2	0.35%
Central America	4	0.70%
TOTAL	575	100.00%

Country	Top Threat Group	Alerts	% of Country Total
United States	Burp	50	25.77%
Canada	Burp	119	83.80%
United Kingdom	Xtreme-RAT	20	38.46%
Ireland	Burp	41	95.35%
France	BR-UNC-009	30	78.95%
Germany	Xtreme-RAT	11	50.00%
The Netherlands	Redline	8	47.06%
Russia	Web Skimmer	19	90.48%

Table 3. Total C2 Alerts Split by Country and Region

GEOGRAPHIC CONCENTRATION

- North America dominates with 58.43% of all alerts (336 of 575 total)
- The United States alone accounts for 33.74% (194 alerts) - highest single country
- Canada follows with 24.70% (142 alerts) - second highest
- Europe collectively represents 33.04% (190 alerts)
- Western-aligned nations (North America + Europe) account for 91.48% of infrastructure

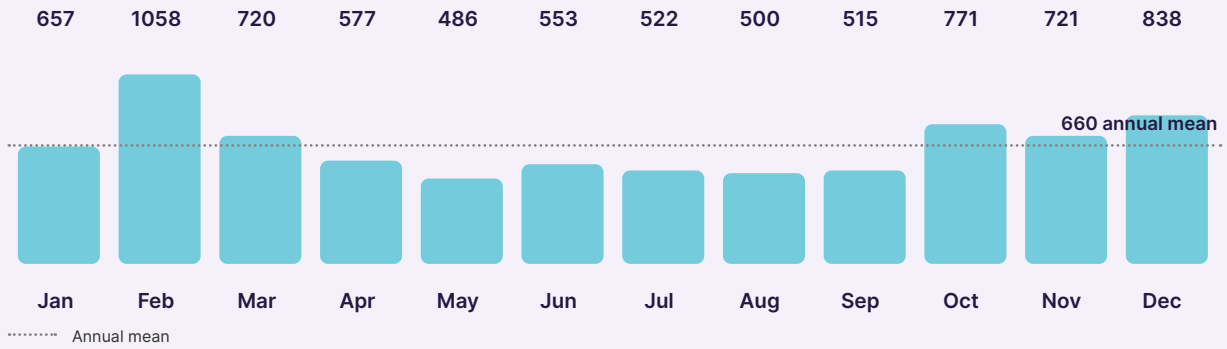
Ransomware in 2025

Ransomware Overview

Across 2025, Bridewell observed 7,918 victim postings on ransomware group data-leak sites (DLS) across 129 distinct threat actors sourced from ransomware. live. Victims were recorded across 144 countries and 30 industry sectors, reflecting the continued broad and opportunistic nature of the ransomware threat.

Of the 129 active groups observed in 2025, 43 published fewer than 10 victims. This represents 33% of all active actors and is consistent with ecosystem fragmentation, in which smaller operators are increasingly active alongside established RaaS programmes. The top 10 groups accounted for 54% of all victim postings.

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.



i Each bar represents the total number of victims publicly posted on ransomware group data-leak sites (DLS) during that month. This reflects confirmed public disclosures only – the true number of attacks is typically higher, as many victims pay quietly or are never listed. Victims without a recorded attack date are excluded from monthly totals but included in the overall quarter count.

Figure 23. Victims Postings Per Month in 2025

February was the most active month of the year with 1058 victim postings. Activity averaged 660 victims per month across 2025, with the lowest recorded month being May at 486 postings.

Ransomware in 2025

Month-over-Month: What Changed?

Figure 24 breaks down key metrics across each month, Q1 – Q4, showing how victim volumes, group activity, and geographic spread shifted over time. The delta-column shows the percentage change between consecutive quarterly periods.

Across the full 2025 calendar year, Ransomware.live recorded 7,918 victim postings. The Q1 period saw the most victims claimed, with the 'Active groups' count ranging from 81 to 87 throughout the year.

Metric	Q1	Q2	Q3	Q4	Q1 - Q4
Total victims	2,435	1,616	1,537	2,330	-4.3%
Active groups	86	87	81	83	-3.5%
Countries hit	109	92	91	93	-14.7%
Industries hit	25	17	16	16	-36.0%
Top group	16.5% (clop)	12.8% (qilin)	14.2% (qilin)	20.1% (qilin)	+21.9%

i *Each column shows key metrics for one month of the quarter, with the delta columns showing percentage change between consecutive months. Turquoise indicates growth, magenta a decline. "Active groups" counts distinct threat actors with at least one posting that month. "Top group's share" names the most prolific group that month and their share of that month's total – useful for spotting when one actor is disproportionately driving volume.*

Figure 24. Quarterly Breakdown of 2025 Ransomware Victims

Ransomware in 2025

Most Active Ransomware Groups

The ransomware landscape in 2025 was dominated by Qilin, which claimed 1009 victims - 12.7% of all activity observed this quarter. The group was followed by Akira (732) and CL0P (518), which together formed a concentrated upper tier of activity.

A total of 129 distinct groups were active this year, with 43 of them publishing fewer than 10 victims. This reflects the fragmentation of the RaaS ecosystem reported on previously, as smaller, independent operators also enter the landscape alongside established programmes.

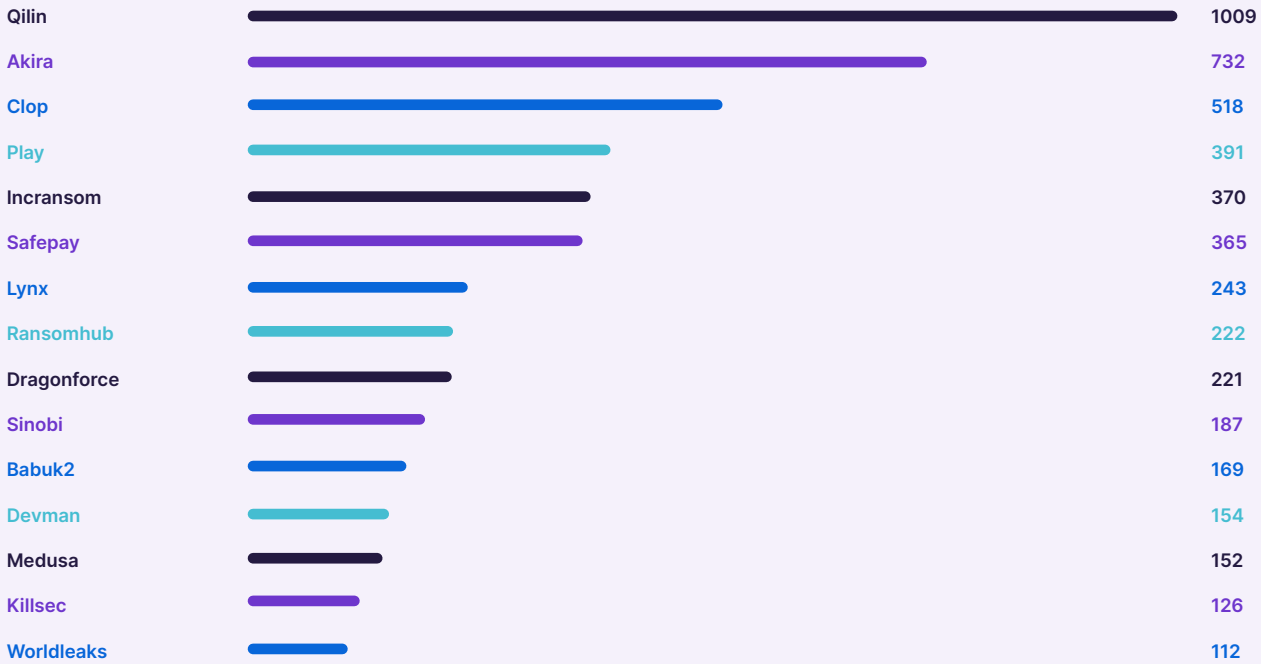
In 2024, activity was largely dominated by well-established operations, such as LockBit3, RansomHub, Play, Akira, and BlackBasta, but by 2025, a different set of actors had emerged. Groups such as Qilin, Safepay, Lynx, DragonForce, and Incransom started accounting for a growing proportion of observed victims, while previously dominant operators such as LockBit3 and AlphV were no longer among the most active. This change reflects the fluid nature of the ransomware ecosystem, where operational disruption, affiliate mobility, and the rapid emergence of new groups continually reshape the threat landscape.

A key driver behind this shift was the series of coordinated international law-enforcement actions conducted during 2024 against several high-profile ransomware operations. These interventions disrupted infrastructure, seized backend systems, and exposed operational details that undermined the credibility of affected groups within the cyber criminal community.

Under the RaaS model, affiliates who are responsible for conducting intrusions and deploying ransomware, operate with considerable autonomy from the 'service provider' and are not permanently tied to any single platform. When a RaaS operation becomes unstable, compromised, or perceived as a law-enforcement risk, affiliates will typically switch to alternative services that offer more reliable infrastructure or more attractive revenue-sharing arrangements. As a result, disruption of a major platform often leads to a redistribution of experienced affiliates across the wider ecosystem, enabling other groups to pivot and scale activity relatively quickly.

The data also reflects a broader trend toward fragmentation within the ransomware landscape. Where earlier periods were often dominated by a small number of highly active groups, the 2025 dataset observes a wider range of 'emerging' and 'mid-tier' actors competing for affiliates and victims. The rise of groups such as Safepay, Lynx, DragonForce, and Incransom highlights the relatively low barriers to entry associated with ransomware operations, particularly within the RaaS model where malware developers, initial access brokers, and affiliates collaborate through established criminal marketplaces. While law-enforcement actions continue to disrupt individual groups, the wider ecosystem has proven resilient, with actors frequently migrating between platforms, rebranding operations, or forming new groups. Consequently, these disruptions often produce displacement effects rather than sustained reductions in overall ransomware activity.

Ransomware in 2025



Bars represent victim count as publicly posted on each group's data-leak site. Groups are ranked by total victims claimed this period. Note that group names reflect operator branding only – some groups share infrastructure, tooling, or affiliates with others despite operating under distinct names. Victim counts may include organisations that paid a ransom and were subsequently delisted, causing slight undercounting for active negotiators.

Figure 25. Ransomware Groups by Victims Claimed in 2025

Ransomware in 2025

Regional Distribution of Victims

The geographic distribution of victims in 2025 reflects established patterns in the global ransomware ecosystem. The US remained the most targeted nation, accounting for 41.4% of all victims and consistent with historical trends driven by the concentration of high-value organisations and the perceived ability to pay significant ransoms.

Victims were recorded across 144 countries in total. The top five most affected nations, comprised of the US, Canada, Germany, the United Kingdom and France, collectively represented 55.4% of all activity. The United Kingdom ranked 4th, with 249 victims recorded.

Beyond the US, Canada and Germany ranked second and third respectively, accounting for a combined 8.6% of all victims.

		Country	Share	Victims	Total
1	US	United States		3281	41.4%
2	CA	Canada		349	4.4%
3	DE	Germany		328	4.1%
4	GB	United Kingdom		249	3.1%
5	FR	France		179	2.3%
6	IT	Italy		158	2.0%
7	ES	Spain		149	1.9%
8	BR	Brazil		140	1.8%
9	IN	India		137	1.7%
10	AU	Australia		122	1.5%
11	JP	Japan		111	1.4%
12	MX	Mexico		74	0.9%
13	TW	Taiwan		68	0.9%
14	CH	Switzerland		64	0.8%
15	SG	Singapore		63	0.8%

Country attribution is based on the victim organisation's listed location on the threat actor's data-leak site. This reflects where the victim operates, not necessarily where the attacker is based. Attribution should be treated as indicative – some victims may be misattributed, and multi-national organisations may appear under a single country. The mini-bar shows each country's share of total victims for the period.

Figure 26. Distribution of Ransomware Attacks by Country in 2025

Ransomware in 2025

Industries Under Pressure

The sector distribution of victims in 2025 reflects the broad and opportunistic nature of modern ransomware operations. Manufacturing was the most affected sector, accounting for 11.8% of all victims, followed by technology (11.5%) and then healthcare (6.9%).

Healthcare organisations accounted for 545 victims (6.9% of total), reflecting the continued targeting of the sector despite informal avoidance policies observed among some RaaS operators.

	Sector	Distribution	Victims	%Share
1	Manufacturing		933	11.8%
2	Technology		911	11.5%
3	Healthcare		545	6.9%
4	Business Services		392	5.0%
5	Financial Services		368	4.6%
6	Construction		335	4.2%
7	Consumer Services		331	4.2%
8	Education		289	3.6%
9	Transportation/Logistics		287	3.6%
10	Public Sector		258	3.3%
11	Agriculture and Food Production		203	2.6%
12	Hospitality and Tourism		161	2.0%

Sector data is sourced from Ransomware.live's activity classification tags. The distribution bar shows each sector's share of total victims visually. Some victims carry no sector tag ("Not Found") and are excluded from this table – this is noted in the source data and does not affect total victim counts shown elsewhere in the report. Organisations operating across multiple sectors may be classified under their primary industry.

Figure 27. Ransomware Victims by Industry Sector in 2025

Ransomware in 2025

Payment Trends & Resolution Rates

Ransom payment data sourced from Coveware's quarterly incident response case data provides important context on the financial impact of ransomware beyond victim counts. In 2025, the average ransom payment stood at $621,247 (a 34% increase compared to 2024), while the median payment was $253,750 (a 36% increase on 2024). The figures shown represent the mean of quarterly averages across all four quarters of the year. The divergence between average and median figures reflects the continued presence of large-payment outliers skewing mean values upward, while most organisations settle at significantly lower sums.

Overall, 2025 saw 24% of affected organisations make a ransom payment, continuing the multi-year downward trend from a peak of 85% in early 2019. This declining payment rate reflects improved organisational resilience through offline backup capability, as well as increased awareness of sanctions exposure and the reputational risk of payment.

AVG RANSOM PAYMENT (2025 ANNUAL MEAN)

$621,247

↑ +34% vs 2024

Prior period (mean across 2024): $465,000

MEDIAN RANSOM PAYMENT (2025 ANNUAL MEAN)

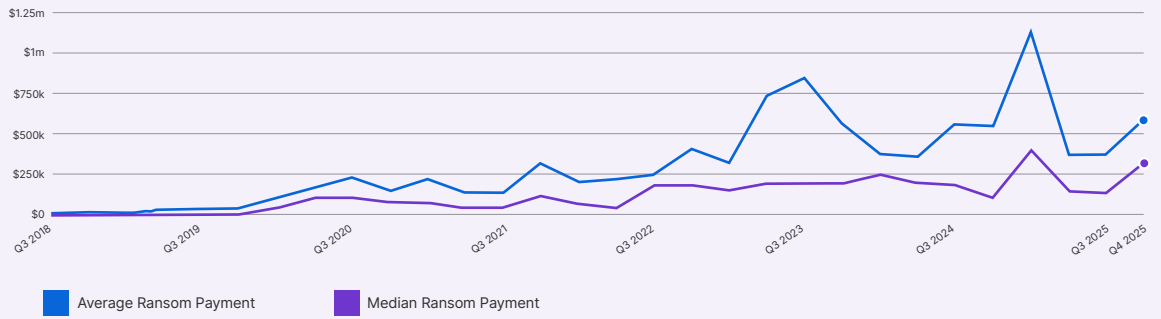
$253,750

↑ +36% vs 2024

Prior period (mean across 2024): $186,250

Figure 28. Average/Median Ransomware Payment

Source: coveware.com



Average and median figures represent payments made by organisations that chose to pay the ransom demand - non-paying cases are excluded from payment calculations. The average is sensitive to outliers: a small number of very large payments in a quarter can materially increase the mean while the median (middle value) remains stable. Where the average significantly exceeds the median, this indicates a small number of high-value outlier payments skewing the mean upwards.

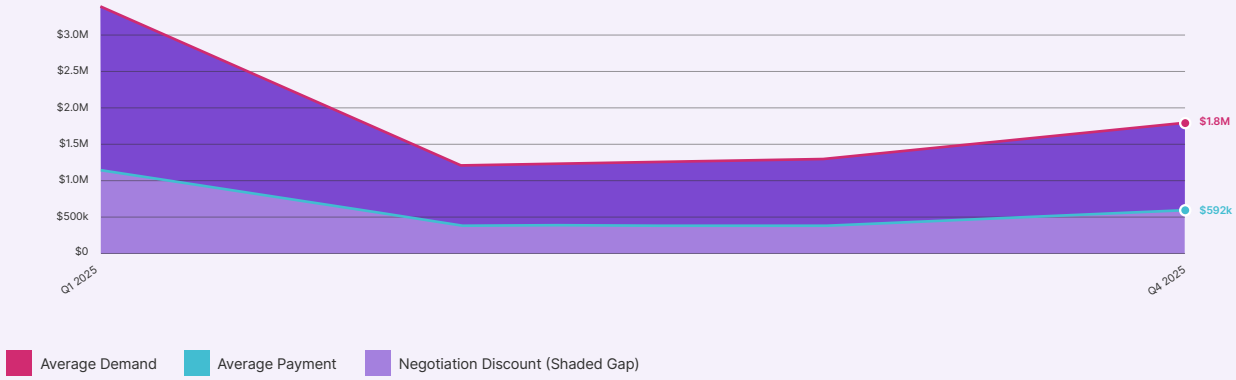
Figure 29. Ransom Payments by Quarter

Source: coveware.com

Ransomware in 2025

While Figure 30 shows what organisations paid, the chart below contextualises those payments against what ransomware operators initially demanded, revealing the negotiation discount that victims are achieving. Coveware's incident response data captures both the initial demand figure and the final settled payment, allowing the gap between the two to be tracked over time.

The negotiation discount is calculated as: (1 − paid ÷ demand) × 100. A discount of 60% means the victim paid 40 cents for every dollar initially demanded. The quarterly cards below show how this discount has changed. Rising discounts suggest victims are gaining leverage or becoming more willing to decline payment; a falling discount suggests operators are demanding closer to what victims will actually pay, or that victim negotiating position is weakening.



NEGOTIATION DISCOUNT BY QUARTER (RECENT 8 QUARTERS)

Q1 2025	Q2 2025	Q3 2025	Q4 2025
66% Discount	69% Discount	71% Discount	67% Discount

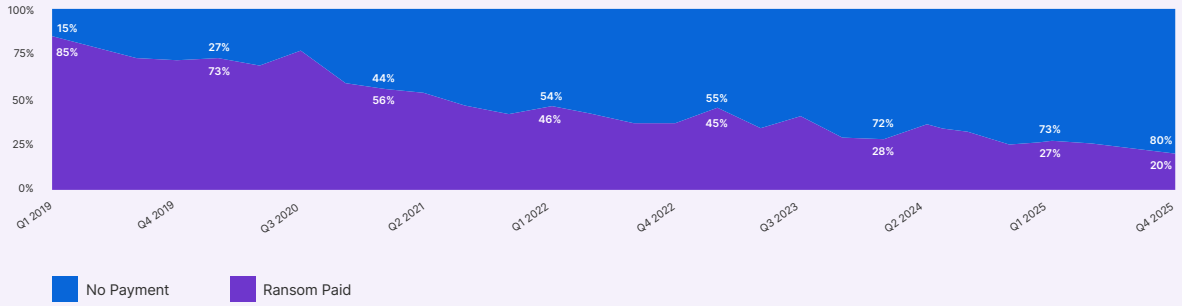
Period avg: **68% discount** Range: **66%-71%** Latest: **67% discount in Q4 2025**

i *The shaded area between the demand line (pink) and payment line (turquoise) represents the negotiation discount – the portion of the initial demand that victims successfully negotiated away or declined to pay. A widening gap indicates increasing leverage or unwillingness to pay; a narrowing gap suggests demands are closer to final payments.*

Figure 30. Ransom Demand vs Payment & Negotiation Discount in 2025

Source: coveware.com

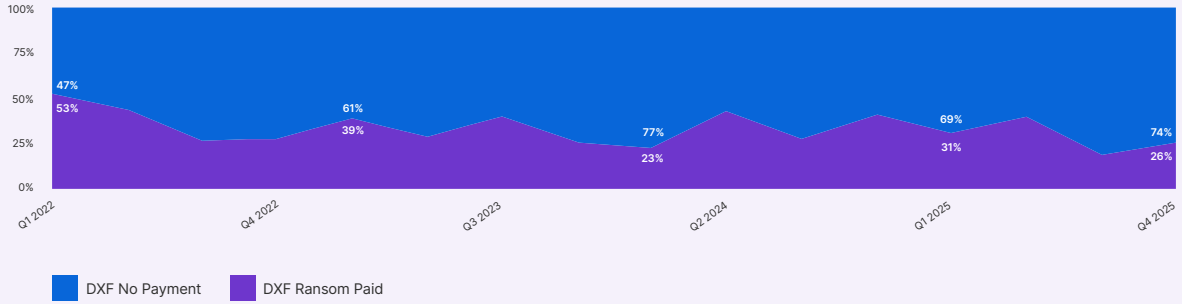
Ransomware in 2025



The "Ransom Paid" area shows the percentage of all ransomware cases (including encryption-based attacks) where the victim organisation made a ransom payment. The remainder chose not to pay – typically relying on backups, accepting data loss, or assessing payment as ineffective or legally risky. The long-term decline from 85% in 2019 to around 20-27% today reflects improved backup infrastructure, increased legal risk from sanctions exposure, and growing scepticism about whether payment guarantees decryption or data deletion.

Figure 31. Ransomware Payment Resolution Rates

Source: coveware.com



DXF (Data Exfiltration-only) cases involve threat actors who steal data without deploying ransomware encryption – leverage is purely reputational and regulatory (threatened publication of sensitive data). Payment rates in DXF cases are historically lower and more volatile than encryption cases because the operational disruption pressure is absent. Organisations increasingly decline to pay DXF demands as they assess that payment does not guarantee data deletion and may invite repeat targeting.

Figure 32. DXF-Only Payment Resolution Rates

Source: coveware.com

The Data Exfiltration-only (DXF) payment resolution rate continues to reveal the growing prominence and impact of data exfiltration attacks. Unlike traditional encryption-based ransomware, these attacks threaten the public exposure of sensitive information, which sustains pressure on organisations to pay, despite improved defences against encryption. The 2025 data shows that DXF-only ransom payments remain highly volatile, showing a payment rate of 29% on average across 2025, highlighting that while some organisations are refusing to pay, a significant proportion still feel compelled to meet attacker demands to prevent data disclosure.

This trend reinforces the view that data theft has become a more effective lever for ransomware actors than encryption alone, as organisations are increasingly resilient to file encryption attacks through backups and disaster recovery planning. However, the persistent willingness of some victims to pay underscores the continuing effectiveness of leak site extortion tactics, which threaten reputational damage, regulatory penalties, and operational disruption. Overall, these figures illustrate that while the broader ransomware landscape is maturing in its defences against encryption, the threat of data exposure remains a critical concern for many organisations, and threat actors have successfully adapted their tactics to exploit business risk appetite and reputational fragility.

Ransomware in 2025

Incidents of Significance

In 2025, the ransomware ecosystem fragmented heavily, seeing upwards of 19 new groups emerge, raising the total to 129 active extortion crews, driven by the collapse of major brands and rapid affiliate reshuffling.

One of the biggest drivers of the shift was international law-enforcement operations targeting dominant ransomware groups. The most significant example was ‘Operation Cronos’ (2024), which targeted LockBit infrastructure and saw the seizure of servers, exposed internal data and operator identities, resulting in a damaging effect upon the affiliate trust in the platform. Because most ransomware groups operate as RaaS platforms, affiliates are free to move to other platforms if one becomes risky or unreliable. As a result, affiliates previously working with LockBit and similar groups migrated to alternative RaaS platforms.

Despite increased law-enforcement operations, ransomware volumes surged with 5,524 incidents (Jan–Sept 2025) and 6,290 leak-site cases by October, marking a 34% and 47% year-on-year increase respectively, with projections indicating 11,000+ global incidents in 2026.

Research

Phishing Kits and Techniques

Introduction

Bridewell CTI continues to track various phishing kits leveraged by threat actors and has observed them in a number of customer environments. These kits continue to go through iterations of development and subsequent improvements and have consistently dominated the threat landscape. Phishing remains the most prevalent initial access vector used by adversaries. The PhaaS model provides threat actors a convenient method to leverage such frameworks to facilitate credential access in target environments.

The underlying themes used to lure the victims remained consistent and comprised scams related to financial and legal documents, voicemails, human resources (benefits, payroll, work-based processes), document signing and other generic payment and invoices. Additionally, threat actors were observed experimenting with generative AI to construct phishing lures that appeared to be more convincing and appealing to their victims.

Threat actors continue to improve their operational security (OPSEC) through the use of CAPTCHAs as a form of anti-analysis measure to circumvent automated scanners. The use of CAPTCHAs simultaneously obfuscates URLs and scripts to make analysis of phishing infrastructure more challenging for researchers which are tracking them. Some operators were also seen using malicious QR codes to evade detection by security tools. One of the key objectives for these PhaaS kits remains bypass of MFA through interception of session tokens.

Adversaries continue to use legitimate services to host their infrastructure such as cloud hosting and storage, file sharing and collaboration, identity and authentication, content delivery networks (CDNs) and other decentralised storages. The purpose of using this infrastructure to relay phishing attacks is to abuse the good reputation of these services, implement OPSEC and to make management of infrastructure easier for operators.

Frameworks

2025 witnessed nearly double the number of known phishing kits when compared with 2024, with a vast majority of kits being distributed under the PhaaS model. New and emerging phishing kits in 2025 built upon kits such as Tycoon2FA and Mamba 2FA in terms of sophistication, stealth and defence evasion. This section covers the prevalent phishing kits that are likely to continue dominating in the subsequent months. The two phishing frameworks mentioned below, EvilGinx and Tycoon 2FA, have been sighted in our own telemetry.

EvilGinx

EvilGinx was released in 2017 (specifically Evilginx2 and the commercial Evilginx Pro). It is a well-known and documented modular phishing kit with open-source documentation available on GitHub, and is heavily used in various phishing campaigns. It operates as a man-in-the-middle proxy, enabling operators to intercept and manipulate traffic between users and legitimate websites. EvilGinx is modular and customisable as it enables the configuration of phishlets, redirectors, and other components, which makes it extremely useful to threat actors. Since its public release, the kit has undergone a significant number of changes to improve functionality.

While the popularity of the phishing kit is greater among cyber criminals such as Storm-0485 and Scattered Spider, for example, there have been instances where nation state threat groups have also leveraged it. Examples of this are the Russian-attributed groups, Star Blizzard and Void Blizzard.

In October 2025, while researching a phishing campaign centred around Docusign, our CTI team observed connection to the unattributed threat cluster ‘BR-UNC-017’. The URL ‘dynamics.com’ was used, which serves as the central hub for Microsoft’s powerful suite of business management applications, ‘Microsoft Dynamics 365’. A previous campaign linked to BR-UNC-012 by the team, also observed the use of ‘dynamics.com’ in their infection chain which resulted in an EvilGinx phishing page.

Research

Tycoon2FA

Tycoon 2FA operates as an adversary-in-the-middle phishing kit. Since its emergence in August 2023, it's undergone several development iterations and became one of the most leveraged PhaaS platforms used by various threat actors in different campaigns. A number of organisations are tracking the usage of this kit by operators such as Storm-1747, who manage the network infrastructure and sell access to the kit via encrypted channels like Telegram.

Our team has observed the use of Tycoon2FA in several customer environments throughout 2025. One such instance saw the phishing kit used in an intrusion attributed to a known threat cluster that we are tracking internally, known as BR-UNC-019. The uniqueness of this cluster can be traced back to their use of custom CAPTCHA pages and targeting of senior stakeholders within financial services. Previously, BR-UNC-019 was observed using Sneaky2FA and Evilginx phishing kits in their campaigns.

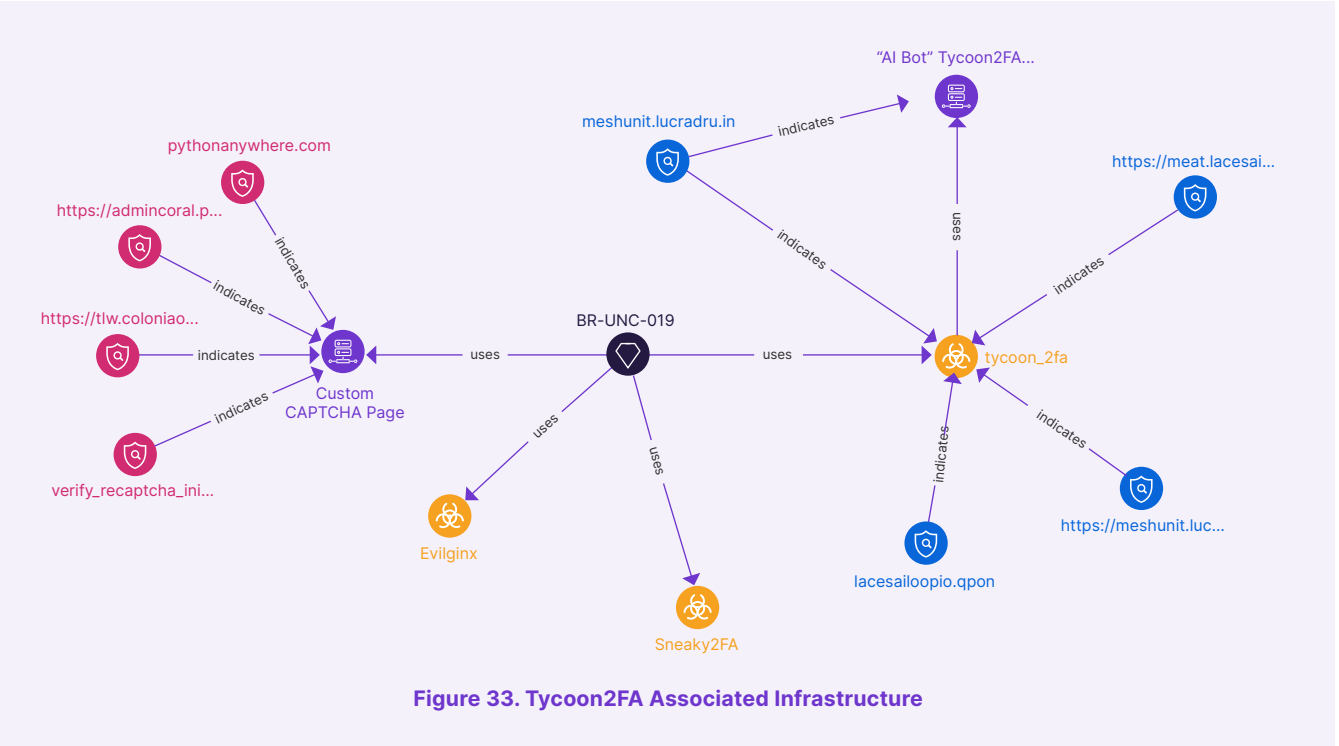


Figure 33. Tycoon2FA Associated Infrastructure

Research

In addition to BR-UNC-019 leveraging Tycoon2FA, we also track BR-UNC-025 which differs from BR-UNC-019 in observed tradecraft. More specifically, BR-UNC-025 has been seen to use QR codes embedded in PDF attachments, although the targeted victimology of both the threat clusters remains the same.

Recently, Bridewell CTI also released a blog documenting the rise and fall of Tycoon2FA phishing kit which detailed the core mechanics, advanced defence evasion techniques, similarities with Dadsec OTT phishing kit, different observed CAPTCHAs, and key elements of the kit itself.

We additionally analysed over 3000 email log records within our data sources to measure the email delivery success rate of Tycoon 2FA over the last six months prior to the takedown operation.

In March 2026, a global takedown operation coordinated by Europol's European Cybercrime Centre (EC3) was conducted by law enforcement partners and private sector stakeholders. As part of the disruption, 330 domains forming the core infrastructure of the criminal service, including phishing pages and control panels, were taken down.

The impact of this disruption was observed prominently within our own email telemetry and while the massive volume drops are highly encouraging, our investigation of the remaining March telemetry identified that a number of Tycoon 2FA phishing CAPTCHA pages are still live.

Key Takeaway

Historically, the emergence of newer phishing kits has been inspired by older ones. Source code is repurposed and readily available modules are leveraged from within the phishing framework. We assess with moderate confidence that this pattern is likely to persist and further accelerated through the usage of AI in 2026 where new phishing kits are developed through the reuse of source code from already known phishing kits.

Fix Style Attacks

Phishing remains one of the most prominent methods threat actors use to achieve initial access. However, as email security controls mature and increasingly thwart the delivery of malicious links and attachments, threat actors have pivoted toward new behavioural-driven tactics. This shift represents a foundational evolution in social engineering. Rather than relying on technical exploits, these attacks bypass technical defences and identity controls by weaponising human behaviour.

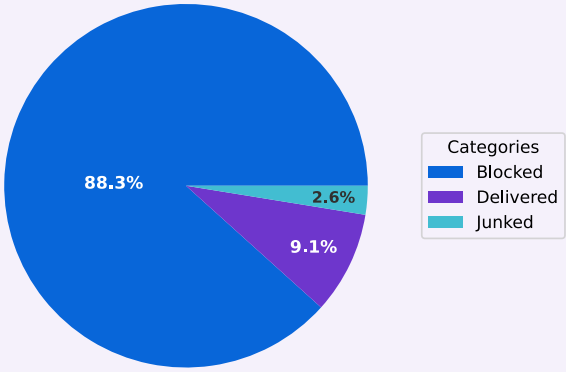


Figure 34. Email Actions for Tycoon2FA

Evolution of Phishing and "Fix Style" Attacks

A prominent example of this new methodology was the emergent ClickFix technique, first observed in late 2023 to early 2024. ClickFix attacks operate by presenting the user with a fake CAPTCHA verification prompt, often hosted on legitimate, compromised websites. These highly convincing lures are designed to entice users into manually copying and pasting malicious commands directly onto their own devices, frequently utilising the Windows Run prompt.

Microsoft's 2025 Digital Defence report identified ClickFix as the most prevalent initial access method of the year, accounting for 47% of observed attacks. Due to its high success rate, ClickFix has been heavily adopted across the threat landscape and state-sponsored APTs quickly integrated the technique into their espionage operations.

Notable examples include Russia-aligned actors such as APT28 (Fancy Bear) and Star Blizzard, Iran's MuddyWater, and North Korea's Kimsuky. Amongst cyber criminals, a high-volume of initial access brokers (IABs) were among the earliest adopters, including TA571, who utilised large spam campaigns spoofing Microsoft Word and OneDrive to deliver ClickFix payloads.

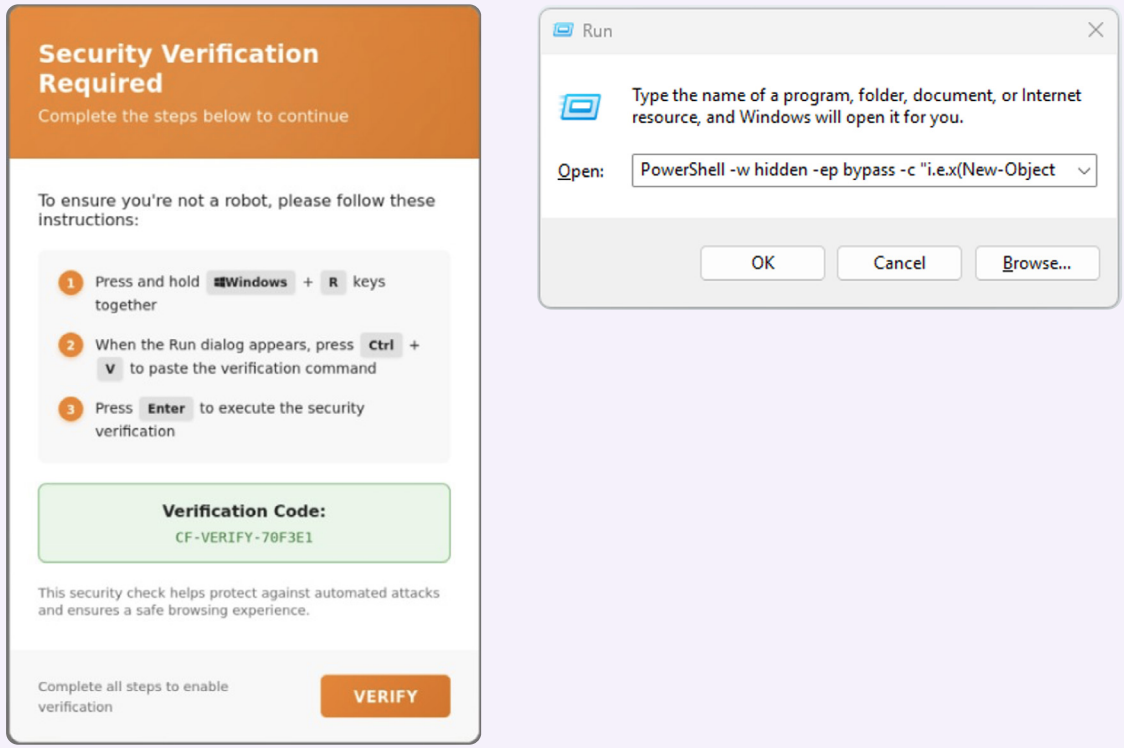


Figure 35. ClickFix Attacks Operate by Presenting the User With a Fake CAPTCHA

Widespread Adoption and Emerging Techniques: FileFix Attack

As user awareness and monitoring solutions adapted to detect the abuse of the Windows Run dialogue, threat actors sought stealthier execution methods. In June 2025, [Bridewell CTI identified a change in ClickFix methodology], now known as FileFix. In this unique variation, rather than relying on the Run prompt or terminal, FileFix shifts the attack surface entirely to the Windows File Explorer address bar.

The FileFix attack typically begins when a victim interacts with a benign-looking button on a web page, prompting the user to upload a file, which uses hidden HTML elements to open a legitimate File Explorer window on their system. Concurrently, malicious code is copied to the user's clipboard and the webpage then instructs the user to press a keyboard shortcut like 'CTRL-L' to navigate directly to the Explorer address bar, paste what they think to be a standard file path, and press 'Enter'.

The execution process of a FileFix attack differs from the original ClickFix technique as it originates directly from the web browser, which then is used to spawn additional processes. This unusual process hierarchy complicates analysis, leaving no obvious command window and more effectively bypasses traditional endpoint security and sandbox analysis processes.

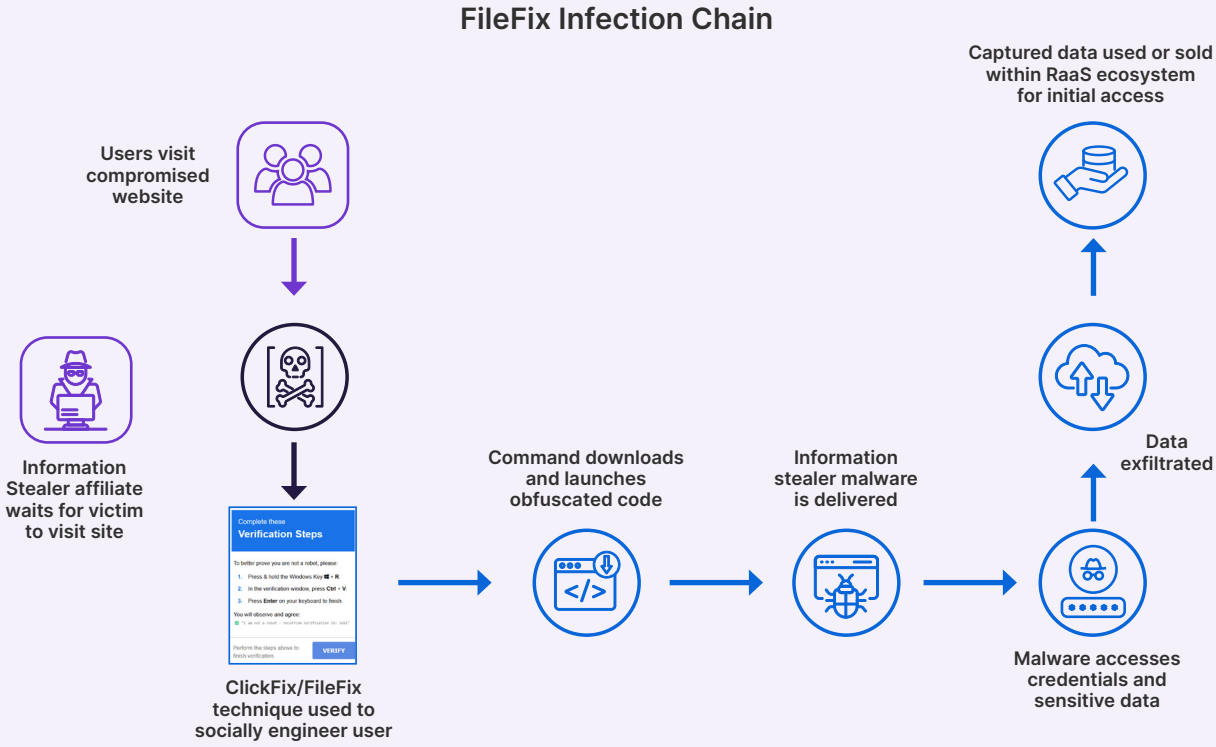


Figure 36. FileFix Infection Chain Analysed by Bridewell CTI

One notable FileFix campaign, tracked by Bridewell CTI under BR-UNC-011, used a modified execution chain for stealth and persistence. The campaign, identified in Q3 2025, involved the use of PowerShell scripts, legacy XHTML COM objects and Base64-encoded payloads to deliver malware disguised as legitimate browser software, Chrome. This instance highlights a prominent trend of legitimate software being used to evade detection.

Additionally, the KongTuke threat cluster, observed operating a large-scale Traffic Distribution System (TDS) since at least mid-2024, quickly adopted FileFix techniques alongside its traditional ClickFix lures. This IAB abused legitimate, public-facing web assets with a focus on outdated WordPress websites to host their malicious content. KongTuke is a well-known group in the cyber criminal ecosystem, selling their initial access to prominent ransomware operations such as 8Base, Akira, AlphV, Rhysida, Interlock and others.

"Fix Style" Attacks Continue to Change: ConsentFix

As security teams and platforms have grown more adept at identifying the unusual process hierarchy generated by ClickFix and FileFix techniques, threat actors have adapted by abandoning the endpoint.

The latest evolution of the "fix-style" methodology is known as ConsentFix, representing a pivot from device exploitation to browser-native identity theft.

By confining the attack entirely within the browser, threat actors eliminate the need to execute malicious payloads on the host machine, rendering traditional endpoint protections, automated sandboxing and operating system-level safeguards obsolete.

The first usage of ConsentFix was discovered by PushSecurity in a blog where they highlighted the attack in detail. The ConsentFix execution chain leverages the deceptive prompt characteristics of previous attacks, presenting victims with a CAPTCHA or verification page that eventually prompts them to "verify" their identity by following a legitimate sign-in process. Once the user authenticates, an OAuth authorisation code is generated, which is then copied and pasted back to the attacker, unwittingly handing over access to the victim's account. This technique continues to evolve rapidly. Researchers have observed variations that eliminate copy-paste requirements, instead manipulating users into simply dragging and dropping the authorisation code directly to the attacker.

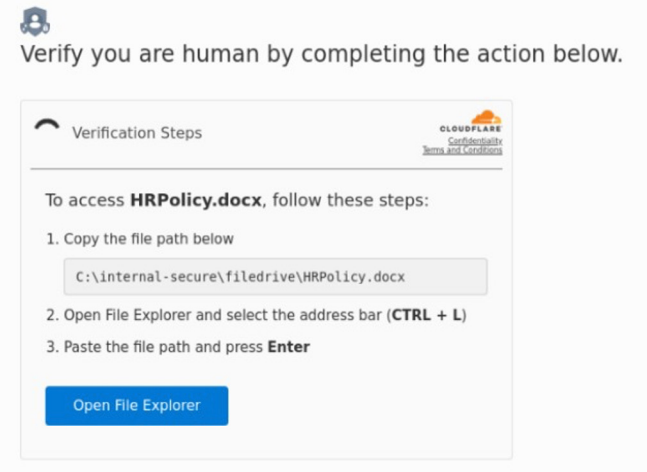


Figure 37. FileFix Abuses File Explorer in a Novel Way

Research

The overarching risk of ConsentFix lies in its abuse of implicitly trusted first-party applications, like Microsoft AzureCLI. These first-party apps are trusted by default, allowing adversaries to easily bypass default restrictions. Furthermore, these attacks leverage the victim's active browser session to generate the authorisation token which circumvents Entra Conditional Access policies and phishing-resistant authentication methods such as MFA.

In one of the defining campaigns that led to the discovery of ConsentFix, researchers identified threat actors targeting Microsoft accounts by weaponising first-party Microsoft applications. Rather than relying on conventional email-based phishing, the attackers predominantly used Google Search (via SEO poisoning and malvertising) to drive victims to compromised, high-reputation websites. Highlighting a broader shift in initial access delivery, telemetry indicates that over 80% (4 out of 5) of intercepted "fix-style" attacks are now delivered through SEO poisoning.

Bridewell CTI assesses with medium-high confidence that "fix-style" attacks will remain a prominent threat within the wider threat landscape, with both nation-state and cyber criminal threat actors adopting increasingly novel and sophisticated techniques in an attempt to avoid traditional security controls.

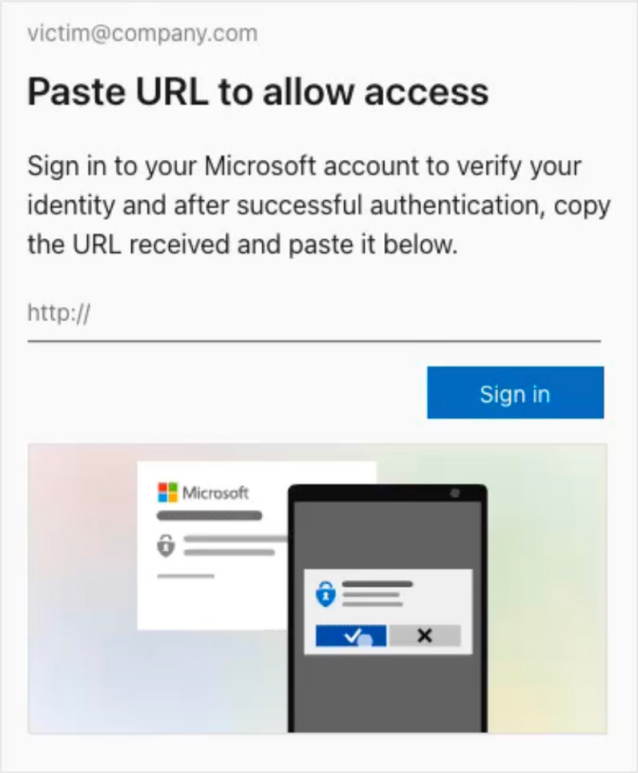


Figure 38. ConsentFix Evolves the 'Fix' Methodology

Bridewell Targeted Ransomware Research

DragonForce and RansomHub

During 2025, Bridewell CTI identified an uptick in ransomware activity driven by the emergence of new groups and the rapid adoption of tools, techniques and collaboration models across the cyber threat landscape. Threat actors continue to refine their tradecraft to achieve faster intrusion times, more effective defence evasion and greater operational impact. The threat landscape evolved not only in attack volume but also in the number and diversity of active ransomware groups. Throughout the year, multiple threat clusters demonstrated heightened cooperation, sharing tooling, infrastructure and tradecraft to accelerate their initial access and expand capabilities.

This growing interoperability between groups, paired with the widespread use of legitimate administrative tools for “smash and grab” style operations, helped solidify ransomware extortion and rapid data theft as dominant threats facing organisations in 2025 and beyond.

At the same time, intra-group conflict and competition intensified. Several groups engaged in direct conflict, conducting disruptive operations against rival threat actors. One notable example occurred in Q2 2025, when the DragonForce group carried out a “hostile takeover” and defacement of the RansomHub data leak site, an event that highlighted both the volatility of the threat landscape and the shifting power dynamics between prominent ransomware operations.

Figure 39. Defacement of the Dragonforce Data-Leak Site, Shared by Ransomhub Member, ‘Koley’

These events reflect a broader trend of convergence, where boundaries between ransomware groups continue to blur as they adopt each other’s tooling and increasingly operate across multiple groups simultaneously.

Research

Hellcat Ransomware Emerges

Hellcat, first identified in Q4 2024, became a highly visible and unignorable threat. Bridewell CTI published a report in February 2025, where we highlighted the group's growing reputation for high-profile attacks against telecommunications, critical national infrastructure and government entities.

Operating initially as a loose collective of individual operators, Hellcat later formalised into a coordinated ransomware group. The group's leadership, notably founders operating under the aliases 'Pryx' and 'Rey' are assessed to be deeply embedded in the wider ransomware ecosystem, even establishing their own forum, Dangerzone, to support recruitment, collaboration and operational coordination.

Hellcat's tradecraft is adaptable. The group typically achieves initial access through phishing campaigns and the exploitation of public facing assets, including exploitation of vulnerabilities and misconfiguration. Once inside the network, operators heavily employ Living-off-the-Land (LotL) techniques, relying on low-profile tools and custom scripts to maintain access in target environments.

Illustrating a broader trend of collaborative ransomware tradecraft, Hellcat's encryption payload and ransomware notes shared a strong resemblance to two other groups, Morpheus and Underground Team. This overlap highlights how modern extortion groups are increasingly relying on shared tooling, infrastructure and knowledge to accelerate operations and expand their capabilities.

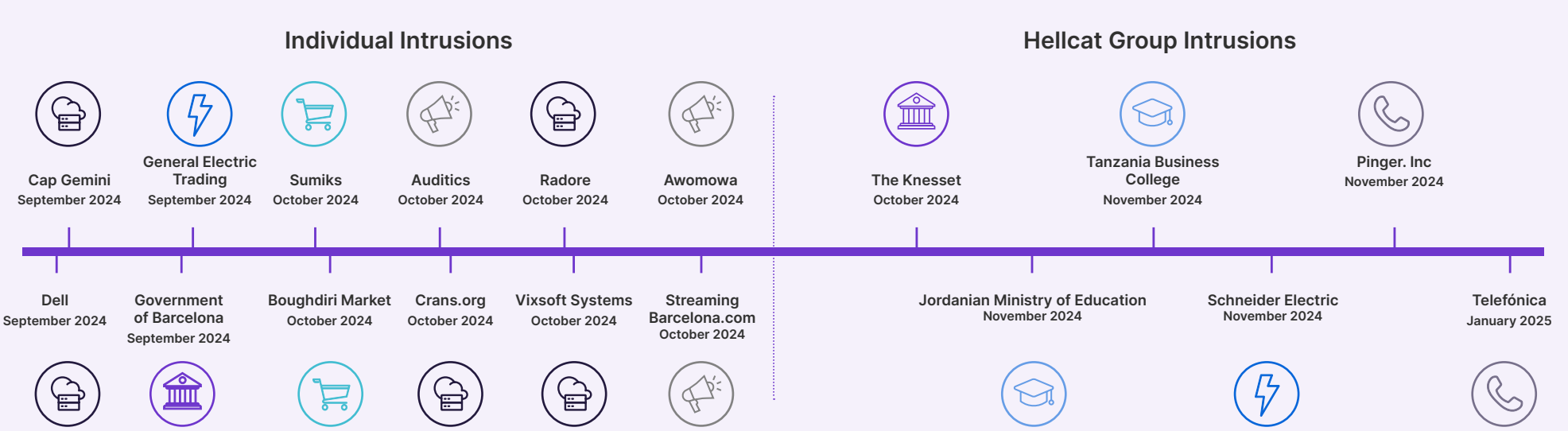


Figure 40. Hellcat Operators Began as Individual Threat Actors, Consolidating Into Hellcat

Research

Converging Ransomware Tradecraft

In December 2025, Bridewell CTI published a report outlining the dissolving barriers between distinct Ransomware-as-a-Service operations. This convergence has created a far more fluid threat landscape, where threat actors routinely share tooling, infrastructure and operational expertise, enabling them to operate across multiple groups simultaneously. As a result, ransomware risk must now be assessed through a broader lens, as a single intrusion may carry the combined sophistication and capabilities of several major groups.

As part of this research, Bridewell CTI analysed a multi-phase intrusion in which activity from a single affiliate was directly linked to several prominent ransomware operations, including PLAY, DragonForce, RansomHub, with additional ties to Shadow Syndicate, an initial access broker supporting ransomware campaigns. This intrusion also highlighted a shift in operational objectives. In the campaign, the adversary successfully achieved collection and exfiltration of sensitive data without deploying the final ransomware encryptor payload in the infection chain.

Increasingly, threat actors are prioritising speed and efficiency, relying on widely available administrative tools, such as WMI, RDP, WinSCP, alongside leveraging custom malware for defence evasion. This behaviour reinforces the “smash-and-grab” extortion, where rapid data theft either precedes encryption or replaces it entirely. With the line between early reconnaissance and active data theft becoming increasingly difficult to distinguish, defenders must treat the earliest phases of an intrusion with full severity.

Nation-State Collaboration with Ransomware Groups

North Korea’s Lazarus group provides a clear example of the growing convergence between traditionally distinct threat clusters. The group has recently been observed leveraging off the shelf RaaS payloads, operating as an affiliate for both PLAY and Medusa. These payloads were deployed against healthcare and non-profit organisations across the USA and the Middle East. By adopting already established RaaS tooling, nation-state actors can minimise malware development overheads while blending their espionage and revenue driven activities into the wider noise of criminal operations. Bridewell CTI released a report during May 2025, highlighting Medusa’s operations in more detail.

Active since late 2021, Medusa has sustained a high operational tempo, functioning as a double-extortion RaaS group. While healthcare remains a primary target, Medusa payloads have also affected critical national infrastructure (CNI), education, legal services, manufacturing and other sensitive sectors.

Medusa is characterised by its multi-layered extortion model. In addition to operating a dark web data leak site (DLS), its operators are known to escalate pressure through direct harassment of victims via phone calls and email, thereby attempting to increase the likelihood of payment.

Medusa commonly gains initial access through targeted phishing campaigns, using malicious attachments or embedded links to harvest credentials. The group has also been observed exploiting known vulnerabilities in public facing and edge infrastructure. Once inside the network, the group relies heavily on LotL techniques. Rather than deploying custom malware, they use legitimate commercial tools, such as network scanners, to map the environment, identify high-value assets and accelerate data collection. This approach reflects the broader trend of “smash-and-grab” extortion, in which rapid data theft is prioritised ahead of, or sometimes instead of, deploying an encryption payload.

Beyond Medusa and Lazarus, ransomware operators continue to adopt novel techniques like ClickFix, FileFix and ConsentFix to achieve initial access while circumventing traditional security controls such as email gateways and phishing-prevention tooling. These evolving methods highlight the continued innovation within the ransomware threat landscape as actors seek more reliable and less detectable paths into victim environments.

Research

Akira: SEO Poisoning and VPN Software Abuse

Akira targeted organisations globally, with a particular focus on manufacturing, education, professional services and critical national infrastructure. Analysis of Akira's victim postings throughout the year reveals a consistent operational tempo, punctuated by several notable surges that reflect strategic shifts in their targeting and campaign cadence.

Critical sectors such as financial services, agriculture, healthcare, energy, and telecommunications also appear within Akira's victim pool, emphasising the group's willingness to target essential services when operational pressure can accelerate ransom payment.

Akira's operations demonstrated highly adaptable tradecraft and increasingly aggressive extortion tactics. While the group routinely deployed ransomware to lock down Windows and ESXi environments, Akira affiliates also exemplified the broader shift toward "extortion only" intrusions, where operators bypass encryption entirely and move directly to data theft and extortion. These intrusions are often completed in under 24 hours, reflecting a streamlined and well rehearsed operational model.

To support these rapid campaigns, Akira operators increasingly weaponised SEO poisoning to distribute fake enterprise software installers. By manipulating search engine rankings, the group elevated malicious websites that closely mimicked legitimate download pages.

These fraudulent sites impersonated well known security and VPN products, including solutions from vendors such as Fortinet, Cisco, and Ivanti, redirecting users to malware laden executables hosted on attacker controlled infrastructure.

By exploiting the trust placed in search engines and familiar product names, Akira affiliates were frequently able to bypass traditional perimeter defences. This includes email gateways and phishing filters, tools that would normally block malicious payload delivery. In several cases, attackers also circumvented MFA by obtaining valid credentials during the initial compromise, aided by the fact that victims voluntarily executed the malware under the assumption that it originated from a trusted vendor.

This technique provided Akira operators with immediate, privileged access that could be leveraged to rapidly deploy ransomware payloads or facilitate extortion only operations on behalf of the wider Akira ecosystem. As security controls continue to mature around email borne threats, SEO poisoning offers threat actors a highly effective, scalable, and user driven initial access vector, one that is likely to see continued adoption across the ransomware landscape.

CL0P's 2025 Enterprise Software Exploitation Campaigns

Throughout 2025, CL0P (TA505) reinforced its position as one of the most prolific ransomware and extortion operations by continuing its long standing strategy of mass exploitation of internet facing enterprise applications. Rather than relying on phishing or other conventional intrusion routes, the group focused heavily on exploiting zero day and high severity vulnerabilities, enabling large scale, high impact attacks against global organisations.

CL0P, also known as TA505 or Graceful Spider, is a financially motivated, Russian speaking threat actor active since at least 2014. Having transitioned to widespread zero day exploitation in 2023, the group first drew global attention through its attacks on MOVEit Transfer, a widely deployed file transfer platform. This shift toward industrialised exploitation continued into 2025.

CL0P's 2025 operations followed a consistent pattern: identify a widely deployed enterprise platform, exploit a critical vulnerability at scale, extract sensitive data, and extort victims via its DLS. Prior operations targeting Accellion FTA, GoAnywhere MFT, MOVEit Transfer, and PaperCut demonstrated this methodology. In 2025, the group aggressively expanded this playbook to new technologies, focusing particularly on Oracle products.

Across the year, CL0P exploited 34 vulnerabilities spanning vendors such as Microsoft, Citrix, Gladinet, and Cleo, but Oracle systems were targeted most heavily.

Key high severity CVEs included:

- CVE 2025 62481 – Critical unauthenticated vulnerability in Oracle Marketing enabling full system compromise over HTTP.
- CVE 2025 61882 – Unauthenticated remote code execution in Oracle E Business Suite.
- CVE 2025 61757 – High severity authentication bypass in Oracle Identity Manager allowing full takeover.
- CVE 2025 53072 – Critical flaw in Oracle Marketing Administration enabling remote compromise.

One of the most impactful campaigns centred on the exploitation of CVE 2025 61882, an unauthenticated RCE in Oracle EBS. CL0P abused this flaw to conduct widespread data theft and extortion, with victim organisations gradually appearing on their DLS as the campaign progressed. Bridewell attributed this activity to CL0P/TA505 with high confidence based on infrastructure reuse, CL0P branded extortion communications, and alignment with historic tactics, techniques and procedures (TTPs).

Notably, the infrastructure used in the campaign included re used SSH fingerprints previously associated with Netwrix Auditor exploitation activity from 2022–2023.

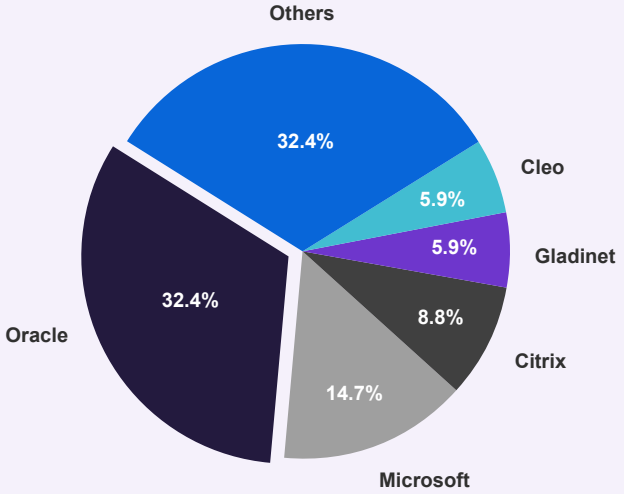


Figure 41. Oracle CVEs Were the Most Targeted by CL0P During 2025

By 2025, large scale exploitation of enterprise software had become central to CL0P's operational identity, marking a clear transition away from opportunistic access routes toward system wide, industrial level exploitation.

The group's 2025 campaigns demonstrated a mature, repeatable model targeting high value enterprise technologies and executing rapid, wide reaching attacks.

Their sustained reuse of infrastructure improved attribution confidence but simultaneously hindered takedown efforts. Additionally, overlaps with the infrastructure patterns of other RaaS operators reflect CL0P's role within a broader, interconnected extortion ecosystem.

Cyber Crime Operations

Bridewell CTI have been tracking both internal and publicly reported campaigns pertaining to cyber crime operations that span across organised groups, IABs and supply chain compromises. This section shares insights into research that we have conducted through collection of all source intelligence.

Initial Access Brokers: Development in Threat Clusters – STAC5777, STAC5143

IABs can be pivotal in cyber crime operations. Their role to breach corporate networks, establish a persistent foothold, and then sell that access to other cyber crime groups or ransomware operators presents a focused intent in terms of evidenced technical behaviours, resulting in a minimised attack footprint.

In early 2025, Sophos reported on threat clusters: STAC5143 and STAC5777 and their involvement in different ransomware campaigns. Based on the open-source reporting on this activity, as part of standard actions taken, Bridewell CTI authored and curated detection content, YARA rules and identified new campaign infrastructure to continue tracking the development activity of these clusters.

Historically, we have seen sightings of a threat cluster with similar characteristics to Storm-1811 within our UK CNI customer environments, which has been the primary motivator to track these threat clusters and adapt our detection strategies accordingly. STAC5777 shows overlapping characteristics with Storm-1811. Storm-1811 is a financially motivated cyber criminal group known to deploy Black Basta ransomware. While STAC5143 is associated with FIN7 threat group. FIN7 is a financially motivated threat group with ties to Russia. This complex cluster of threat actors has been linked to ransomware operations related to REvil, DarkSide, BlackMatter, ALPHV, Black Basta, Maze and Ryuk.

Campaign Overview

Industry reporting highlights the continued adaptation of techniques, adoption of new malware, and notable threat actors FIN7 adopting a mirrored approach to attacking organisations. These activities and trends are likely to continue and, therefore, updated awareness of associated activities linked to Storm-1811 (STAC5777) and STAC5143 (FIN7) is encouraged.

Common tradecraft between STAC5143 and STAC5777

- Email Bombing: Overwhelming target individuals with a flood of spam emails (up to 3,000 within an hour) to create urgency and disrupt their work.
- Social Engineering via Teams: Sending messages, making calls, or initiating video conferences through compromised Office 365 accounts, impersonating legitimate tech support.
- Remote Access Exploitation: Gaining unauthorised control of target devices using tools like Quick Assist or Teams screen sharing to install malicious software.

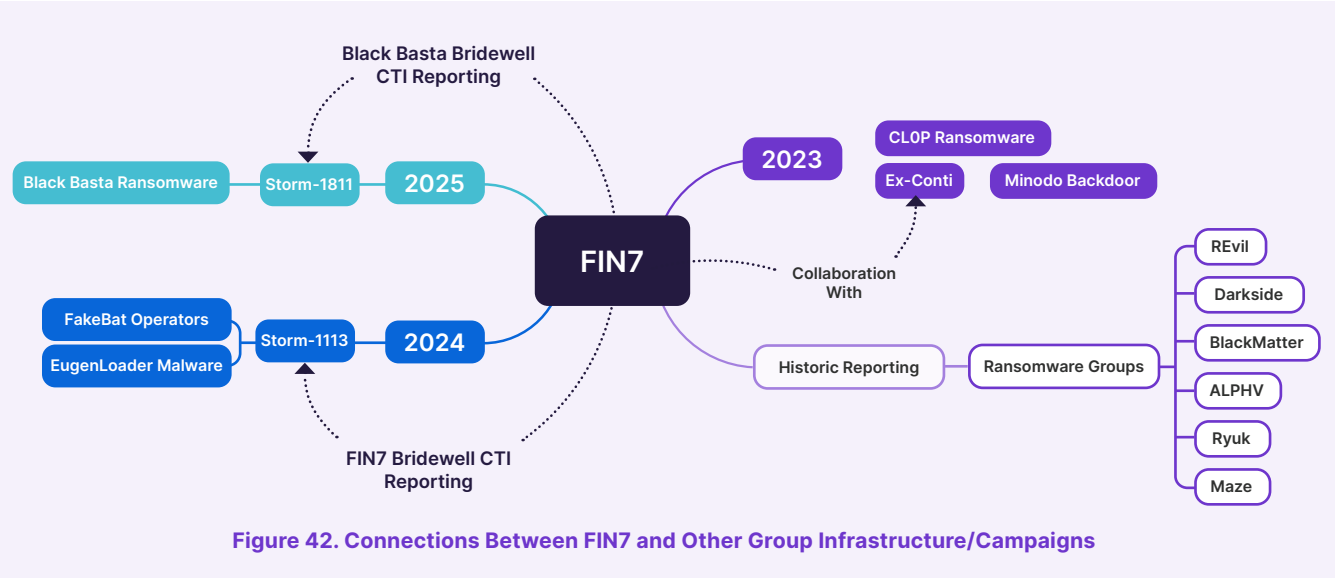


Figure 42. Connections Between FIN7 and Other Group Infrastructure/Campaigns

Research

Operation Deceptive Prospect: RomCom Campaign Targeting UK Orgs

In March 2025, we identified a campaign, that we termed Operation Deceptive Prospect, which was attributed to an intrusion set that was assessed with high confidence to have significant technical overlap with the RomCom threat actor. The campaign was derived from our own customer telemetry through collaboration with our SOC and Incident Response team.

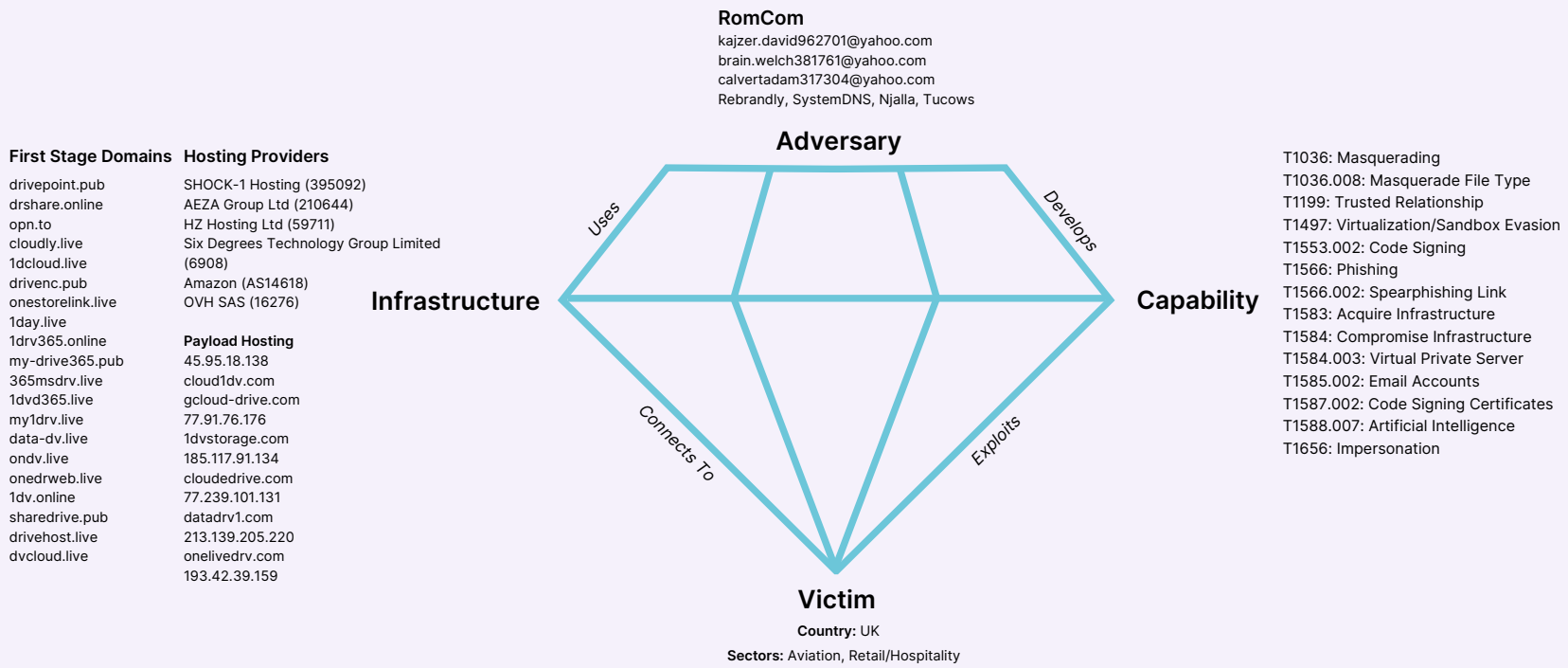


Figure 43. Diamond Model of RomCom

Research

RomCom

RomCom (a.k.a. Storm-0978, Tropical Scorpius, UNC2596, Void Rabisu & UAC-0180) is a Russian-based threat group focused on espionage and financially motivated operations. They have been active since at least 2022 and were observed to primarily target governmental and military entities, with a notable focus on organisations associated with Ukrainian affairs and bodies like NATO. Their primary operational methods include spear-phishing campaigns and the distribution of malware, which is often disguised with trojanised installers for popular legitimate software applications, ultimately aimed at intelligence collection.

Campaign Overview

The “Deceptive Prospect” campaign targeted customer feedback portals on company websites as a mechanism to deliver phishing emails containing malicious links directing customer service representatives to supporting evidence in the form of files (e.g., police statements). Of the intrusion attempts delivered to Bridewell customers, we observed emails reporting stolen luggage at a hotel, recruitment enquiries, and unsatisfactory levels of facilities at a major UK transport hub.

During this campaign, the threat actor leveraged externally facing customer feedback portals to submit phishing emails directed at customer service representatives of two Bridewell customers operating within the UK retail and hospitality, and CNI sectors.

Contained within the feedback forms were user complaints pertaining to events facilities operated by the target or recruitment enquiries, including links to further information supporting the complaints stored on Google Drive and Microsoft OneDrive impersonation domains hosted threat actor-controlled VPS infrastructure.

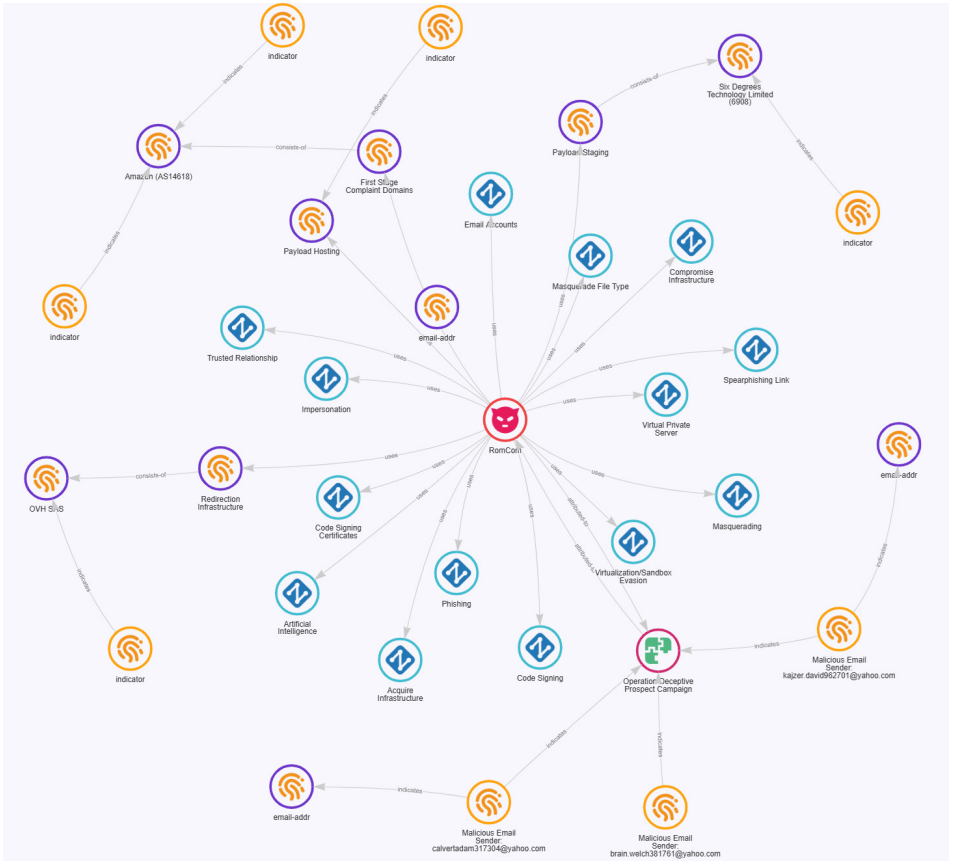


Figure 44. Indicator and Infrastructure Relationship Management for RomCom

Research

Supply Chain Compromise: Scattered Spider Coordinated Attacks on UK Retail Orgs

Supply chain compromises continue to be an effective method for threat actors to gain an initial foothold in target environments by abusing the trust relationships between entities. One of the most prominent breaches of 2025 was the coordinated attacks on M&S, the Co-op and Harrods which were attributed to Scattered Spider. The M&S incident was linked back to DragonForce ransomware group which also was the first instance linking the two groups together. The attacks on M&S and the Co-op involved social engineering, where the threat group impersonated IT staff to deceive help desk personnel into resetting passwords, granting them access to internal systems and allowing ransomware to be deployed.

Scattered Spider

Scattered Spider (a.k.a Starfraud, UNC3944, Scatter Swine & Muddled Libra) is a cyber criminal group that targets large companies and their contracted IT help desks. Scattered Spider threat actors, per trusted third parties, have typically engaged in data theft for extortion and have also been known to utilise BlackCat/ALPHV ransomware alongside their usual TTPs.

Emergence of SLSH

The emergence of SLSH (Scattered LAPSUS$ Hunters) marks a significant evolution in the cyber crime landscape, transitioning from a single-group operation to a supergroup alliance. This federation primarily consists of members from Scattered Spider (UNC3944), Lapsus$ and ShinyHunters. The SLSH brand surfaced prominently in August 2025 via a Telegram channel called “Scattered LAPSUS$ Hunters - The Com HQ” effectively formalising a partnership between the three threat groups.

“Supply chain compromises continue to be an effective method for threat actors to gain an initial foothold in target environments by abusing the trust relationships between entities.”

Research

Timeline of Attacks

Cyber Attacks Against British Retail Organisations

21/04/2025

Initial Report: Source 'Mail Online' - M&S; contactless payments services disrupted/offline.

22/04/2025

Initial Action: Source 'London Stock Exchange (LSE)' - Statement shared with LSE with the following confirmations:

- Communication - Acknowledged 'cyber incident'
- Response Action - Informed National Cyber Security Center (NCSC)
- Response Action - Involvement of external cyber security experts
- Response Action - Reduction in services, no customer actions required
- Communication - Customer

23/04/2025

Press Release: Source 'M&S' - Company posted official press release on website

25/04/2025

Press Release: Source 'M&S' - Second official press release posted on their website.

Industry Reporting: Source 'Bleeping Computer' - The cybersecurity news outlet shares information they claim to have been provided, highlighting the following detail:

- Attack Description - Ransomware
- Threat Actor - Scattered Spider
- Source - Undisclosed

Industry Reporting: Source 'Retail Gazette' - The sector news outlet reports the following:

- Response Action - M&S reduce access to internal systems for WFH staff

Industry Reporting: Source 'Daily Mail' - The news outlet reports the following:

- Response Action - Agency staff at Castle Donington logistics site are informed not to come into work

29/04/2025

Industry Reporting: Source 'HelpNetSecurity' - The cybersecurity news outlet shares findings provided by security research Kevin Beaumont:

- Containment Action - M&S took internet-exposed VPN endpoints and other external services offline since 20/04/2025
- Malicious Indicators - M&S observed inbound traffic from IPs with a known history of use by crimeware groups
- Malicious Indicators - M&S VMware ESXi infrastructure encrypted by DragonForce (Ransomware-as-a-Service)

30/04/2025

Industry Reporting: Source 'Bleeping Computer' - The cybersecurity news outlet reports the following:

- Cyber Attack - The Co-op (British supermarket chain) shuts down parts of its IT systems due to potential intrusion attempts
- Communication - Details surrounding the attack are confirmed by a Co-op spokesperson to Bleeping Computer, however, success/ failure of the attempt IS NOT confirmed
- Impact Description - Malicious activity observed targeting network, back office & call center sevices

01/05/2025

Industry Reporting: Source 'Bleeping Computer' - The cybersecurity news outlet reports the following:

- Communication - Harrods confirm all stores and websites remain open to the public, and that no customer action is required
- Response Action - Partial access restriction to some platforms
- Impact Description - A Harrods spokesperson confirms threat actors were observed gaining unauthorised entry to it's network
- Impact Description - Malicious activity observed targeting network, back office & call center services prompting Response Action

Figure 45. Timeline of Cyber Attacks in Summer 2025

Conclusion

Bridewell has conducted extensive research on the Scattered Spider group and has been studying their evolving tradecraft over the past few years to build detection content and enable analytics in customer environments through collaboration with our detection engineering team. Additionally, we have been tracking C2 and phishing infrastructure used by the group.

Nation State Spotlight: DPRK

This section shares key insights from our research and analysis on Democratic People's Republic of Korea (DPRK) attributed offensive cyber operations. Our research is derived from infrastructure tracking, intrusion analysis and malware to provide a more comprehensive view.

In terms of hosted infrastructure, the DPRK assets identified in 2025 were overwhelmingly concentrated in the US and South Korea. Bridewell tracks clusters such as Contagious Interview, Kimsuky, Dream Job, Lazarus, BeaverTail and various DPRK UNC clusters. Across this dataset the US was the leading live hosting geography every month, while South Korea remained the second-largest monthly host. On a full-year unique IP basis, South Korea slightly led the footprint, but together the US and South Korea accounted for nearly three quarters of all unique DPRK-linked infrastructure observed across the year.

This concentration likely reflects more than simple hosting availability. The weighting toward US and South Korean infrastructure suggests these clusters may be seeking proximity, plausibility, and better operational blending into the geographies, platforms, and traffic patterns most relevant to their targets, meaning the hosting pattern appears to support the deception layer as much as the technical delivery layer.

The preference for hosting their infrastructure directly coincides with known geopolitical factors, thereby driving the requirement for DPRK operators to host their infrastructure in the same region as their intended targets. For example, they may host infrastructure in the US and South Korea for the purpose of eliminating any network geo-blocks while conducting offensive operations.

Infrastructure Hosting Insights

	Jan 2025	Feb 2025	March 2025	April 2025	May 2025	Jun 2025	Jul 2025	Aug 2025	Sep 2025	Oct 2025	Nov 2025	Dec 2025	Total
Korea, Republic of	27.50%	29.55%	26.67%	36.76%	35.76%	26.72%	28.46%	30.99%	31.85%	22.70%	25.53%	20.90%	**40.67%**
United States	52.50%	47.73%	54.44%	46.32%	45.70%	57.25%	55.38%	52.82%	54.07%	60.99%	60.28%	58.96%	**36.39%**
Italy			2.21%	3.31%	3.05%	3.08%	5.63%	2.96%	2.84%	2.84%	4.48%		**8.26%**
Netherlands	7.50%	7.95%	6.67%	4.41%	4.64%	3.05%	3.08%	3.52%	3.70%	2.84%	4.26%	4.48%	**3.36%**
United Kingdom	1.25%	1.14%	1.11%	0.74%	1.32%	1.53%	1.54%	1.41%	1.48%	2.84%	2.13%	3.73%	**1.83%**
Taiwan	5.00%	4.55%	1.11%	0.74%	0.66%	0.76%	1.54%	0.70%	0.74%	0.74%	0.71%	0.75%	**1.53%**
Germany		2.22%	2.21%	1.99%	0.76%					0.71%	0.71%	0.75%	**1.22%**
Japan	1.25%	2.27%	1.11%	0.74%	1.32%	1.53%	2.31%	1.41%	0.74%	0.71%			**1.22%**
India	1.25%								0.74%	0.71%		0.75%	**0.92%**
China											0.71%	0.71%	**1.49%**
Singapore								0.70%	0.74%	1.42%	0.71%	0.75%	**0.61%**
Spain		1.14%	1.11%	0.74%	1.32%	0.76%	0.77%	0.70%	0.74%	0.74%	0.71%		**0.61%**
Viet Nam			0.74%	0.66%	1.53%	1.54%	0.70%	0.74%	0.71%	0.71%	0.75%		**0.61%**
Australia			0.74%	0.66%	0.76%								**0.31%**
Hong Kong												0.75%	**0.31%**
Mexico	1.25%	1.14%	1.11%	0.74%	0.66%	0.76%	0.77%		0.74%	0.71%	0.71%	0.75%	**0.31%**
Portugal	1.25%	1.14%	1.11%	0.74%	0.66%	0.76%	0.77%						**0.31%**
Romania		1.14%	1.11%	0.74%									**0.31%**
Slovakia	1.25%	1.14%	1.11%	0.74%	0.66%	0.76%	0.77%	0.70%	0.74%	0.71%	0.71%	0.75%	**0.31%**
Turkey		1.14%	1.11%	0.74%	0.66%								**0.31%**

Table 4. DPRK Infrastructure Distribution

Research

Insights from a DPRK Attributed Campaign

Bridewell conducted collaborative research with Ransom-ISAC to share analysis of a DPRK-attributed campaign involving the usage of novel C2 mechanisms, custom OPSEC techniques and a selection of lesser known ASNs for hosting their infrastructure.

These traits combined place their inherent threat on par with other nation-state threat groups. Several findings from the analysis of this campaign are similar to those shared by other organisations. However, one of the unique observations from the campaign findings was the connection between DPRK and Russian operators.

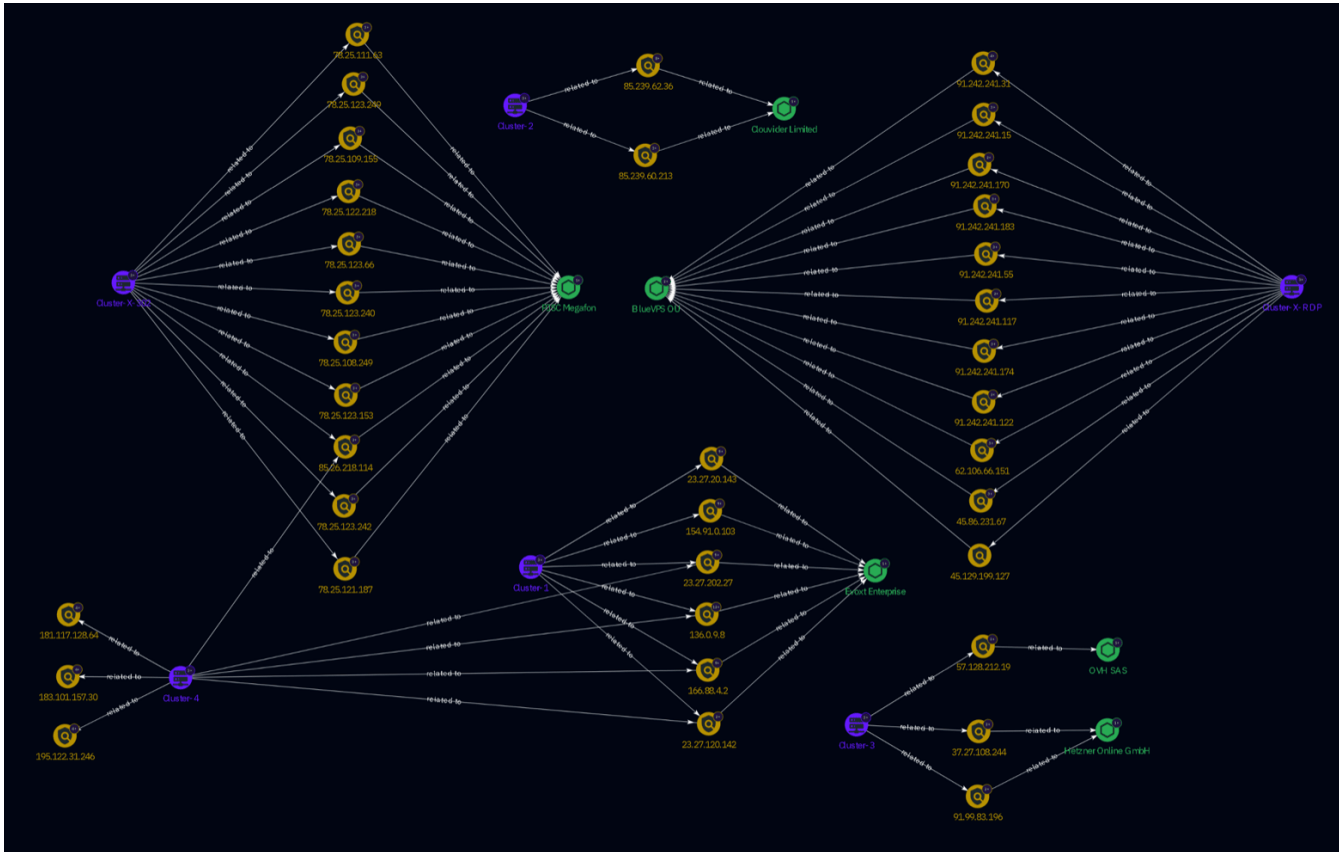


Figure 46. Different Infrastructure Clusters and Associated ASNs

Research

Initial Payload Hosted on GitHub

2025 recorded a number of malicious NPM repositories hosted on GitHub by various threat actors including the DPRK operators contributing to them. These repositories were targeted towards developers through fake job recruitments.

Novel Block Chain-based C2 Mechanism

Historically, the DPRK is known to experiment with initial access techniques and break ground for other adversaries who later adopt their tactics within their own campaigns. One of the most significant tactical shifts in 2025 was the adoption of public blockchain infrastructure as a C2 mechanism using a technique derived from 'Etherhiding' known as 'Cross-Chain TxDataHiding'. Outside of this campaign, several DPRK operators have been using Etherhiding to embed malicious payloads directly into smart contracts on Ethereum and BNB Smart Chain. This technique on the other hand employs an arbitrary blockchain as a decentralised pointer system to reference (formerly known as 'Binance Smart Contract') transaction hashes containing encoded and obfuscated payloads. The architecture is blockchain-agnostic—any chain supporting custom data fields in transactions can serve as the pointer layer.

Some of the advantages of using this type of C2 channel include:

- **Takedown-Proof Infrastructure:** Traditional C2 servers can be seized by law enforcement or shut down by hosting providers within hours, but blockchain-stored data is replicated across thousands of decentralised nodes worldwide, making removal effectively impossible.
- **Dynamic Payload Updates:** The attacker can modify payloads at any time by posting new blockchain transactions while the malware's hardcoded addresses never change, meaning infected machines automatically fetch updated payloads without code modifications.
- **Traffic Obfuscation:** Connections to blockchain APIs (api.trongrid.io, aptoslabs.com, binance.org) appear identical to legitimate cryptocurrency wallet traffic, blending seamlessly into millions of daily crypto transactions. Organisations cannot block these APIs without preventing all legitimate cryptocurrency usage by employees, creating an impossible choice between allowing malware or breaking business operations.
- **Attribution Obfuscation:** Traditional C2 infrastructure leaves clear trails through domain registrars, hosting providers, and payment records that can be traced back to threat actors. Blockchain transactions use pseudonymous addresses funded through mixers and exchanges, breaking attribution chains.

Cross-chain transaction hiding provides a takedown-proof, self-updating C2 infrastructure that costs less than a dollar, evades analysis by appearing legitimate, cannot be blocked without business disruption, and leaves minimal forensic traces, fundamentally changing the malware C2 from a chokepoint to an advantage.

Infrastructure Clusters and ASNs Selection

During our analysis of the campaign, three different clusters were identified based on the underlying infrastructure. One cluster particularly stood out as we had the highest confidence in assessing it as being hosted on an (ASN AS149440) belonging to Evoxt Enterprise. We assessed this to be an intentional choice for the campaign by the DPRK operators for the purpose of hosting dedicated Virtual Private Servers (VPS). Threat actors often use such dedicated VPS to host their C2s giving them more granular control over the infrastructure which can also be treated as better investment when it comes to resource development.

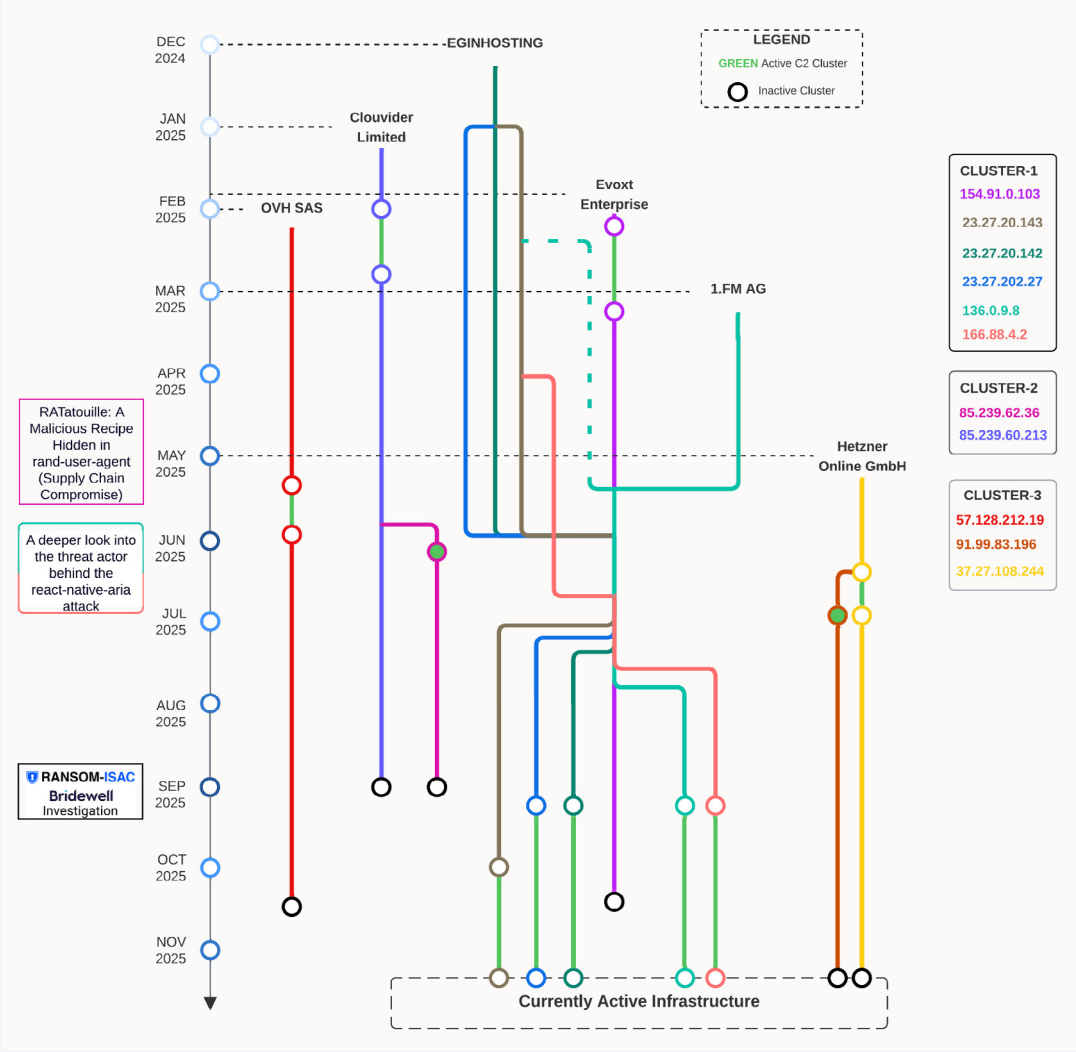


Figure 47. DPRK Campaign Hosting Across Different ASNs

Research

DPRK Collaboration with Russia

One of the most interesting findings from the campaign analysis was that there were certain Russian nodes used for remote access to set up the infrastructure prior to the campaign's active timeline. All these nodes were hosted on the same ASN (AS31213) belonging to 'PJSC Megafon' which is a leading Russian telecommunications operator headquartered in Moscow, providing mobile, internet, and fixed-line services.

At a later point, conventional OSINT also revealed other Russian infrastructure accessing one of the crypto wallets connected to the campaign. The presence of a DPRK-linked IP address geolocating to Vladivostok is consistent with North Korea's known internet infrastructure arrangements with Russia. TransTeleCom, one of Russia's largest telecommunications companies, began providing internet service to North Korea in October 2017 via a fibre-optic cable linking Vladivostok to the North Korean border.

This connection between the DPRK and Russia provided us with a rare sighting where more than one nation state is involved in a single campaign. We are likely to see more of such collaboration in 2026 where threat actors share their resources with those from other nations. This is likely to further blur the lines of attribution. It is worth noting that this partnership between DPRK and Russian operators might not be exclusive and whilst we have not seen other countries that have facilitated remote access for DPRK, others might exist and may be uncovered during future iterations of the campaign.

"This connection between the DPRK and Russia provided us with a rare sighting where more than one nation state is involved in a single campaign."

Outlook and Closing Remarks

The following sections cover key cyber threat intelligence observations as we move into 2026.

Edge Devices and the AI-Accelerated Threat Landscape

We assess with high confidence that edge device exploitation is here to stay and remains a primary entry point for threat actors. Because traditional endpoint detection and response tools typically cannot be installed on edge devices such as routers, firewalls, and VPN appliances, these assets continue to provide attackers with a critical visibility blind spot. Furthermore, we assess with high confidence that attackers are disproportionately targeting end-of-life or unsupported infrastructure, taking advantage of devices that no longer receive security updates.

The most profound shift in the 2025 threat landscape has been the industrialisation of exploit development using generative AI and Large Language Models (LLMs). We assess with high confidence that the traditional time-to-exploit window has collapsed from days to hours or minutes. Threat actors are now leveraging AI to autonomously reverse-engineer security patches the moment they are released, identifying the underlying vulnerability and generating weaponised exploits almost instantly. Consequently, the release of a security patch now effectively serves as an exploit blueprint for AI agents, allowing attacks to propagate before human defenders can realistically test and deploy fixes.

We also assess with moderate to high confidence that AI agents are also automating broader attack chains, taking over reconnaissance, vulnerability discovery, and post-exploitation lateral movement with minimal human intervention.

To combat this rapidly accelerating threat, organisations must urgently adapt their defensive posture. Building on previous principles, the following steps are critical to protect edge devices against AI-enabled threats:

- **Decommission End-of-Life Infrastructure:** Know your asset inventory and ruthlessly phase out EOL and end-of-sale edge devices. Attackers actively seek out these unpatched appliances as permanent footholds.
- **Implement Automated and Virtual Patching:** The era of month-long patch testing cycles is obsolete. Organisations should aim for automated, continuous repair mechanisms and leverage virtual patching (such as web application firewalls) to neutralise exploits at the network edge within hours of disclosure.
- **Centralise and Automate Monitoring (SIEM/UEBA):** Because edge devices lack EDR, it is vital to stream all device audit logs, configuration changes, and authentication logs to a centralised SIEM. Implement User and Entity Behaviour Analytics (UEBA) to instantly flag anomalous logins, suspicious configuration downloads, or the creation of rogue local administrator accounts. These are all common tactics used by attackers to maintain persistence on devices.
- **Strictly Isolate Management Interfaces:** Network management interfaces (NMIs) must never be directly exposed to the public internet. Ensure that administrative access is restricted to dedicated, isolated Privileged Access Workstations (PAWs).
- **Enforce Phishing-Resistant MFA:** Implement hardware-backed, phishing-resistant Multi-Factor Authentication (MFA) (e.g., FIDO2) for all administrative and remote access to edge devices, effectively neutralising AI-generated social engineering and MFA fatigue attacks.

Outlook and Closing Remarks

Cyber Crime and Ransomware Ecosystem

As modern ransomware operations propagate in 2026, we are likely to observe threat actors shifting to double extortion attacks or solely focusing on the exfiltration of data rather than the encryption of target systems. The shift is likely due to the better success rate and ease of operation of these types of attack. This is further exacerbated with more operators leveraging AI and more specifically autonomous agents capable of scanning networks, developing zero-day exploits, and deploying data exfiltration mechanisms across thousands of endpoints in under a minute.

One of the key drivers in ransomware operations within the UK, specifically for the public sector and CNI, is the ban of ransomware payments. This may deter some threat actors as impacted organisations are legally unable to pay ransoms. Instead, they may divert their efforts towards other regions and sectors that are not impacted by the ban in order to maximise their profits. On the contrary, ransomware operators might increase attacks on banned entities to test the government's resolve. The ban of ransomware payments may also be yet another driver for operators to shift to pure data extortion by threatening GDPR fines or loss of reputation.

Supply chain compromises will continue to increase as they provide threat actors the foothold they require within various organisations. 2025 witnessed the compromise of several high value organisations through their dependencies on SaaS applications such as Salesforce and Salesloft. Additionally, popular packages used by developers were also compromised by threat actors where the code was modified within the public repositories to deploy malware.

Additionally, as AI capabilities grow and organisations continue using it without the right guardrails in place, the deployment of unvetted, cloud-based AI tools will allow threat actors to bypass organisational security controls. This shadow AI is likely to create vulnerabilities through undocumented AI environments which will eventually prove costly to remediate.

Gen AI

Assessment of Generative AI Threat Capabilities

We assess with moderate confidence that generative AI (GenAI) has transitioned from an emerging threat to a proven force multiplier. Validating our prediction from last year, both public reporting and our own intelligence confirm that GenAI is actively empowering lower-tier actors to accelerate their operational velocity. Rather than deploying autonomous super-malware, adversaries leverage AI to automate reconnaissance, lateral movement, and administrative tasks. North Korean actors, for example, utilise these capabilities to bypass technical and linguistic barriers, securing remote IT roles for illicit revenue generation.

Furthermore, confirming our assessment regarding the escalation of personalised social engineering, AI has effectively neutralised traditional linguistic barriers. We observe Iranian actors translating complex Farsi idioms into flawless English and Hebrew to craft high-fidelity lures and synthetic personas for fraud.

Evolution of Obfuscation and Exploit Generation

Consistent with our previous prediction on advanced evasion tactics, we assess with moderate to high confidence that adversaries are transitioning towards no-code malware generation. Threat actors utilise AI for rapid language conversion and debugging, enabling the creation of obfuscated tools specifically designed to evade standard security controls.

Additionally, AI drastically accelerates the exploitation of known vulnerabilities (N-day attacks). By instantly analysing vendor security patches, AI allows adversaries to rapidly reverse-engineer fixes and expedites the development of working exploits, potentially compressing the defender mitigation window from months to days.

Outlook and Closing Remarks

The Emergence of Agentic AI and Critical Sector Impact

As anticipated in our prior threat modelling, automated AI campaigns are now successfully executing disruptive operations across critical sectors, including healthcare and finance. The threat landscape is experiencing a critical shift from AI as an advisory tool to AI as an active operator. Recent intelligence demonstrates single actors deploying automated AI agents to replicate the workload of an entire cyber criminal syndicate.

Furthermore, adversaries are weaponising AI interfaces for stealthy command and control, concealing malicious traffic within legitimate API communications. In extortion scenarios, actors now employ AI models to calculate the optimal ransom demand against black-market valuations of exfiltrated data.

Divergent State-Sponsored AI Doctrines

State actor integration of AI is highly fragmented and aligned with specific strategic objectives:

- **Iran:** Prolific application of Western AI models for regional espionage, influence operations, and deep reconnaissance on defence personnel.
- **China:** Focused on the industrialisation of hacking processes and the deployment of AI-generated propaganda across global media to advance strategic narratives.
- **North Korea (DPRK):** Concentrated on financial exploitation, leveraging AI to sustain clandestine IT worker networks within major global corporations to fund state weapons programmes.
- **Russia:** Exhibiting strategic restraint. We assess with lower confidence that Russian actors deliberately limit engagement with Western language models to prevent telemetry leakage, likely prioritising self-hosted infrastructure.

Defence Imperatives

The democratisation of advanced offensive capabilities requires an immediate evolution in defensive posturing. It is critical for organisations to integrate automated, AI-driven security frameworks and continuous red-teaming. Human operators are no longer adequately equipped to counter machine-scale attacks without AI-augmented defences.

The AI Threat Evolution Matrix

The following AI threat evolution matrix outlines the trajectory of adversary capabilities from the pre-GenAI baseline through to our projected outlook for 2026 and beyond. It highlights a paradigm shift: the rapid transition from manual, resource-intensive cyber operations to highly automated, AI-driven campaigns.

As detailed in the matrix on page 77, the integration of generative AI is fundamentally altering the threat landscape across three core areas:

- Lower barriers to entry
- Accelerated operational velocity
- Advanced threat actor capabilities

Outlook and Closing Remarks

Threat Metric	Pre-GenAI (Baseline)	Current State (2024–2025)	Future State (Projected 2026+)
Research and Resource Development	Manual code comparison. Slow exploit development requiring deep reverse-engineering expertise (weeks to months).	**Accelerated.** AI rapidly analyses patch changes, identifying root vulnerabilities and speeding up exploit creation (days to hours).	**Automated.** AI instantly generates working exploits the moment a vendor publishes a security patch (minutes).
Velocity & Scale	Linear. Constrained by human work hours and manual scripting.	**High.** AI accelerates existing workflows (e.g., rapid reconnaissance and debugging).	**Extreme.** Autonomous, agentic AI systems executing end-to-end multi-stage campaigns.
Barriers to Entry	High. Requires deep programming and networking expertise.	**Lowered.** "No-Code" exploitation; low-skilled actors use AI to bridge technical gaps.	**Near-Zero.** Intent-based execution (operators simply provide high-level goals to an AI agent).
Social Engineering	Generic, mass-spray phishing with obvious linguistic errors.	**High-Fidelity.** Perfect, culturally accurate localisation and convincing synthetic personas.	**Interactive.** Real-time, multi-modal synthetic engagement (deepfake voice/video live interaction).
Payload Novelty	Static variants; reliance on known, patched vulnerabilities.	**Adaptive.** Rapid porting of malware between languages (e.g., Python to Node.js) to avoid signature detection.	**Dynamic.** AI-optimised, real-time polymorphism; malware that rewrites itself upon deployment.
Command & Control	Hardcoded domains and identifiable traffic patterns.	**Obfuscated.** API abuse; hiding C2 traffic within legitimate HTTPS requests to public AI services. New methods such as leveraging blockchain for C2.	**Ephemeral**. AI-negotiated routing; self-healing, dynamic infrastructure that evades blocking.

Table 5. Evolution of AI Threat

Outlook and Closing Remarks

Geopolitical Events

Iran

Outlook on Geopolitical and Cyber Events for 2026: The "Epic Fury" Escalation.

We assess with moderate to high confidence that the geopolitical and cyber threat landscape in 2026 will be radically defined by the severe escalation following the late-February pre-emptive US and Israeli military strikes on Iran, codenamed Operation 'Epic Fury' and 'Shield of Judah', respectively. The resulting regional conflict, including the death of Ayatollah Ali Khamenei and Iran's multi-vector "Truthful Promise IV" retaliation, has triggered widespread kinetic and cyber operations targeting Israel, the US, neighbouring Middle Eastern states, as well as European/UK assets sited in the nearby regions.

Evolution of State-Sponsored Cyber Tactics.

While a near-total internet blackout in Iran initially hindered the domestic coordination of state-aligned threat actors, we assess with moderate confidence that Iranian cyber units will adapt and seek to execute targeted destructive operations. We have already observed Iranian state-aligned cyber tactics toward "Identity Weaponisation." Groups associated to the Islamic Revolutionary Guard Corps, like Void Manticore (Handala), are observed compromising privileged cloud identities before abusing mobile device management (MDM) platforms, such as Microsoft Intune, to issue mass remote-wipe commands across hundreds of thousands of corporate devices globally.

Groups linked to Iranian intelligence (MOIS) are increasingly converging with the cyber crime ecosystem to obscure attribution and enhance operational reach. State-sponsored actors are leveraging commercial infostealers like Rhadamanthys and participating in RaaS affiliate programmes (i.e., Qilin), to conduct disruptive attacks and leak data under the guise of financial extortion.

Surge in Hacktivism and Proxy Cyber Warfare.

We observed Hacktivist groups operating under umbrellas like the 'Holy League' and 'Cyber Islamic Resistance' and more recently under the newly established banner of the 'Electronic Operations Room'. The target map for these proxies is rapidly broadening:

- **Israel & US:** Hacktivist groups (e.g., Handala Hack, FAD Team) actively target Israeli healthcare, energy, defence, and SCADA/PLC systems, alongside direct death threats to perceived critics of Iran.
- **Middle Eastern Entities:** Cyber proxies attack critical infrastructure across the Gulf, claiming responsibility for sabotaging fuel systems in Jordan, attacking airports in Bahrain and Saudi Arabia, and disrupting government systems in Kuwait and the UAE.
- **UK/EU & Broader Allies:** The cyber threat to UK and EU assets globally is expanding asymmetrically with kinetic attacks, such as the drone strike on the UK's RAF Akrotiri base in Cyprus.

Notably, pro-Russian hacktivist groups (such as Server Killers and NoName057(16)) have officially entered the conflict to support the pro-Iran coalition, claiming infiltrations of Israeli defence systems and municipal entities.

Physical-Cyber Overlap and Collateral Risk.

We assess with moderate confidence there will be collateral impact on global logistics, communications, and energy sectors. The conflict has already triggered an energy war with kinetic strikes shutting down numerous major gas and oil hubs in Qatar, the UAE, Kuwait, and Saudi Arabia, pushing oil prices past $100 a barrel and having an immediate disruptive effect on the regional airspace.

Defence Imperatives.

It is critical for organisations, especially those in the defence industrial base, critical infrastructure, and those with supply chains in the Middle East, to urgently strengthen their defences. Organisations must eliminate standing administrative privileges, mandate phishing-resistant multi-factor authentication (MFA), isolate operational technology (OT) from the public internet, and prepare robust offline backups to survive destructive attacks.

Outlook and Closing Remarks

Russia

Outlook on Geopolitical and Cyber Events for 2026 Regarding Iran and Ukraine

The situation in Ukraine through 2025 and 2026 continues to present a point of uncertainty and disruption, with arranged peace talks stalled, a new conflict to divert important political attention, and an increasingly emboldened upsurge of hacktivism activity that seeks to undermine any supporting narratives that allied countries may seek to foster on behalf of Ukraine.

The resulting landscape leaves both independent and proxy groups from both sides conducting continuous campaigns of disruption that have in several ways spilled out into wider states' environments, whether inadvertently or intentionally. The situation in Iran adds greater fuel to this particular fire, where boundaries grow increasingly blurred as more external states are drawn in, either politically or militarily, which again creates even more narratives for both sides to exploit as motivation for their respective cause.

Evolution of State-Sponsored Cyber Tactics

Reporting from across the security industry has collectively, over time, highlighted the role that state-sponsored APTs are playing in the Russian invasion of Ukraine. Many cite the involvement of the intelligence apparatus of the state in directing cyber capabilities toward both adjacent, regional disruption, as well as direct support for kinetic operations on the ground. With regards to cyber capabilities, several call out the use of proxy groups, so-called 'hacktivist' elements steered into action and fed the appropriate propaganda language and content to sow discord among foreign nationals during mainstream events such as elections, as well as using the guise of cyber activism as a form of 'burner' account when conducting targeted activities.

This is observed across several key events throughout 2025 such as low and high-sophistication attacks on foreign critical infrastructure and a supply chain attack that impacted UK Ministry of Defence sites. The broad theme indicates continuation of hybrid tactics with mixed tiers of strategic levers being used. This is in contrast to what came before, which looked more like singular points of access via sophisticated infection chains designed to go undetected and execute without means of attribution or tangible investigation. The objective is to damage trust in the security environment as much as it is to exfiltrate and encrypt.

Hacktivism and the Ransomware Service

Reporting of hacktivism throughout the Russia-Ukraine conflict consistently highlights both the increasing volume of attacks but also threat actors involved in the attacks. The targeting scope is broad and often reactive in nature, coordinated and directed at states that publish announcements or key developments in support of Ukraine. Another interesting development from this swell of activity was the observed shift in some hacktivist groups toward establishing their own RaaS operations. Similar to our observations within Iranian groups, this shift is reportedly in service of wider objectives, likely influenced by state-backed operators. By asserting themselves as a RaaS provider, their activity shifts from ideologically and/or politically motivated to financially motivated. This change redefines how they are perceived by the wider industry and clouds the role attribution has to play in any assessments. Financially motivated attacks are often investigated via the lens of the extortion mechanism, with lesser emphasis applied to group origin, which is typically reserved for commentary on expectations of legal consequence as opposed to any foreign state involvement. Additionally, acting through the shape of a ransomware actor, these groups also add the possibility of causing added impacts through extortion as well as being able to extract funds to support their respective backers. Examples of groups who have made this transition include Dragon RaaS (a.k.a. Dragon Team / DragonRansom), Stormous, CyberVolk and AzzaSec.

Outlook and Closing Remarks

DPRK

Key Foreign Policy Objectives

The cyber operations of the DPRK are influenced by their foreign policy objectives listed below:

Recognition as an Established 'Nuclear State'

The DPRK has made it clear that denuclearisation is no longer an option. Their narrative is of a wealthy country with a strong military arm. Kim Jong Un has pledged to increase the country's nuclear capabilities which, evidenced by recent actions and objectives, include the refinement of tactical nuclear weapons and the deployment of advanced military systems.

Management of Relations with South Korea

The DPRK has abandoned the concept of South Korea (the Republic of Korea) as a partner for unification. Instead, they are officially defined as a principal enemy and hostile state, with the objective of maintaining a state of managed hostility through which direct dialogue is currently suspended. The focus is solely on crisis management to avoid all-out war, while ignoring Seoul's offer for cooperation.

The Russia-DPRK Quasi-Alliance

A core objective is the mutual exchange of resources, which has resulted in a symbiotic relationship with Russia where North Korea provides shells, missiles, and manpower (for the Ukraine war and beyond) in exchange for Russian energy, food, and advanced military technology. Pyongyang aims to remain a useful partner for Russia, even after the Ukraine conflict ends, specifically through labour and resources for post-war reconstruction.

Evasion of International Sanctions

The international sanctions against the DPRK are among the most extensive and complex in history. Primarily established to pressure the regime into abandoning its nuclear and ballistic missile programs. The DPRK has engaged in trade with Russia and China to circumvent UN Security Council restrictions. Russia effectively renders UN panel monitoring sanctions against North Korea as ineffective through use of veto power, while China backs the DPRK through economic and diplomatic support. The most significant shift in recent years is the move towards digital revenue generation. The DPRK treats the cyber domain as an asymmetric equaliser where efforts have shifted from traditional smuggling to socially engineered cyber operations and strategic geopolitical partnerships.

Objectives for Offensive Cyber Operations

Revenue Generation

Since the regime cannot trade freely under the imposed international sanctions, the government apparatus is linked to using state-sponsored proxy groups, such as Lazarus, to conduct offensive cyber operations with the motive of generating revenue on their behalf. Global cryptocurrency theft and espionage are now state-sponsored initiatives, from which millions in revenue are reportedly generated annually, thereby accounting for over 13% of the DPRK's gross domestic product.

Additionally, thousands of DPRK IT workers operate in foreign countries where they secure remote contracts with Western companies, often earning six-figure salaries that are funnelled directly back to the state. DPRK IT workers not only earn money during their employment period but also have insider access to sensitive business systems which can further be used for data extortion.

Targeted Areas and Sectors of Interest

The DPRK's reach is global with respect to targeting organisations for financial theft, which tends to be opportunistic in nature. Such broad targeting spans across financial and cryptocurrency entities in different regions. However, certain regions and sectors can be more specifically targeted to accomplish their R&D related objectives that support advanced warfare.

The DPRK likely targets US and South Korea due to the hostile Two-State Doctrine between the DPRK and South Korea (ROK), which is further exacerbated by the solidified US-ROK alliance. The focus is on intelligence collection, intellectual property (IP) theft and espionage-based operations. Two sectors in particular stand out and, from a conventional intelligence perspective, are likely to be targeted based on the aligned key foreign policy objectives stated above.

Outlook and Closing Remarks

Maritime and Submarine Warfare

Following the late 2025 inspection of North Korea's latest 8,700-ton nuclear-powered submarine, the maritime sector is likely to become a high priority for the DPRK in 2026. It is possible we will see increased targeting of Naval defence contractors and maritime logistics/ shipping firms to gain expertise in underwater-launch nuclear capabilities.

Additionally, maritime and logistics also enable the DPRK to effect the movement of goods, providing both financial opportunities and a means to facilitate sanctions-evading trade. This trade is crucial for North Korea to bypass limits on oil imports and coal exports through deceptive shipping practices (e.g., ship-to-ship transfers for under-the-radar operations).

Aerospace and Satellite Technologies

With the successful deployment of the Malligyong-1 reconnaissance satellite in early 2024, there is likely to be a further push for more frequent launches as the DPRK aggressively seeks to bridge its reconnaissance gap. As a result, satellite manufacturers, space agencies in the EU and North America, and other South Korean aerospace R&D centres may be targeted with the objective of acquiring high-resolution imaging technology and advanced AI for autonomous drones.

Forward Looking Assessment

One of the key events to note in 2026 is the 9th Congress of the Workers' Party of Korea which will be held in April in Pyongyang. The event will solidify the perceived key policy objectives and potentially provide more in-depth insights into the underlying strategic drivers behind those objectives.

Outlook and Closing Remarks

Identity Attacks

Identity remains one of the most reliable routes to access because it allows attackers to operate as legitimate users and blend into normal activity. We assess with moderate to high confidence that identity compromise will remain a primary access method in 2026, based on the continued operational advantage of using valid credentials compared with exploiting software flaws. This is evidenced by recurring credential-led intrusions that we have observed across MDR and incident response engagements, and consistent themes in industry reporting.

This activity typically combines three elements: obtaining initial credentials, expanding access to higher privilege or wider systems, and maintaining access by reusing tokens, keys, or trusted relationships. The following themes reflect how attackers are expected to continue using identity to achieve these goals.

The dominance of identity compromise

We assess with high confidence that identity-driven activity will continue to account for a significant share of incidents, based on the scale and repeatability of password attacks and credential phishing, and evidenced by year-on-year reporting of high volumes of credential abuse and token theft across the security industry.

AI-enhanced social engineering

We assess with moderate confidence that threat actors will use AI to improve the realism and scale of social engineering, based on the lower cost of generating convincing content and the ease of targeting at volume, and evidenced by the growing use of high-quality written lures and synthetic audio or video in fraud and account takeover attempts, as described in numerous public reports throughout 2025 and continuing into 2026.

Once initial access is achieved, attackers often seek methods that are less dependent on a single user account and harder to spot in day-to-day activity.

Targeting of non-human identities

We assess with moderate confidence that attackers will continue to target non-human identities, such as application credentials, API keys, and service accounts. These will continue to be targeted based on the access these accounts can provide without user interaction and the tendency for them to be over-permissioned. This is evidenced by repeated incidents involving leaked keys and compromised service accounts reported across the security industry and seen in investigations.

As organisations increase the use of automation and connected services, the number of identities with meaningful access increases, including those that are not tied to a single person.

AI agents and privileged access

We assess with moderate confidence that wider use of autonomous agentic AI tools will introduce new identity and access risks, based on these tools being granted permissions to act across systems, and evidenced by early cases and vendor guidance highlighting risks from excessive permissions, weak approval controls, and poor secrets handling.

Even where multi-factor authentication is in place, attackers are likely to focus on stealing what is needed to impersonate a trusted session rather than repeatedly attempting to log in.

MFA bypass and session token theft

We assess with moderate confidence that session hijacking will remain a common method to bypass basic multi-factor authentication. This is based on the effectiveness of stealing session tokens or using social engineering to abuse legitimate authentication mechanisms compared with breaking authentication directly. This is evidenced by frequent incidents involving infostealer malware, real-time phishing, device code authentication abuse, and MFA prompt bombing which have been reported by numerous security vendors and through MDR incidents and incident response engagements.

Bridewell

Cyber Security. Where it Matters.

About Bridewell Threat Intelligence

Committed to our clients' security, Bridewell Threat Intelligence Team is a multi-disciplined threat research team comprised of Bridewell managed security professionals.

The team's mission is to produce high signal low noise threat intelligence and insights focused on disrupting attacks and delivering robust protection against advanced threats to both critical national infrastructure (CNI) and the organisations that we manage and protect.

To learn more about our CTI services, please visit:
https://www.bridewell.com/cyber-threat-intelligence

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