

CYBER
THREAT
ANALYSIS

Recorded Future®

By Insikt Group®

August 28, 2025



H1 2025 Malware and Vulnerability Trends

Vulnerabilities in Microsoft products and edge security appliances were the most exploited in H1 2025, with state-sponsored actors driving over half of observed exploitation campaigns.

RATs such as XWorm and Remcos overtook infostealers as primary tools for persistent access and data theft compared to H1 2024, while ransomware groups adopted new affiliate models and evasion tactics.

Android banking trojans adopted overlays and NFC relay attacks for real-world fraud, while Magecart operators expanded beyond Magento to WooCommerce and used modular e-skimmers to evade detection.

Executive Summary

The first half of 2025 (H1 2025) reflected a rapidly evolving threat landscape defined by the convergence of persistent legacy threats and advanced new tactics.

The total disclosed CVEs¹ increased by 16% from H1 2024, and threat actors exploited 161 vulnerabilities with assigned CVEs, with nearly half linked to malware or ransomware campaigns. Microsoft remained the most targeted vendor, while edge security and gateway devices continued to be high-value targets for initial access. Malware activity was similarly dynamic: while law enforcement takedowns disrupted major players like LummaC2, a resurgence of legacy malware such as Sality indicated that old tools still offer utility for modern actors. Remote access trojans (RATs) like AsyncRAT, XWorm, and Remcos also gained prominence, marking a tactical shift away from the previous dominance of dedicated information stealers (infostealers) in [H1 2024](#) toward more versatile tools that combine data theft capabilities with persistent, hands-on access.

Mobile malware threats continued to grow in H1 2025, with Android banking trojans adopting virtualization-based overlays and near-field communication (NFC) relay attacks to bypass user defenses and enable real-world financial fraud. These innovations reflect a growing trend in financial fraud toward mobile-first exploitation targeting both app and payment ecosystems. Ransomware groups, meanwhile, leaned further into affiliate-driven models, offering ready-made payloads and infrastructure to lower barriers for new entrants. Some ransomware families introduced stealth features such as protected payloads or novel loaders designed to evade endpoint detection. Meanwhile, Magecart skimming campaigns adopted multi-stage, modular infection chains and innovative obfuscation techniques to evade content security policies and inject malicious scripts only during critical moments like checkout.

Taken together, H1 2025 underscores that the threat landscape is not only expanding but fragmenting, with threat actors exploiting both novel and legacy tools across diverse attack surfaces. To respond effectively, organizations should prioritize patching of internet-facing systems, particularly gateway and edge security products, which are frequently targeted for initial access. Detection capabilities must extend beyond endpoint telemetry to include behavioral monitoring, command-and-control (C2) traffic analysis, and script obfuscation detection in web environments. Investment in threat intelligence is essential for staying ahead of rapidly changing tactics, such as malware repackaging. Organizations should also revisit mobile device policies and strengthen application vetting and user awareness to counter increasingly sophisticated mobile malware campaigns.

¹ [Common Vulnerabilities and Exposures](#)

Key Findings

- CVE disclosures increased 16% compared to H1 2024, with 161 of those vulnerabilities actively exploited in H1 2025. Of those, 42% had a public proof-of-concept (PoC) exploit, nearly 69% required no authentication, and 30% enabled remote code execution (RCE), underscoring attackers' preference for low-friction, high-impact exploits. Microsoft and edge-gateway appliances each made up 17% of exploits, and more than half of the attributed exploitations were state-sponsored, highlighting state-sponsored threat actors' high capabilities to weaponize flaws quickly.
- Based on Recorded Future Triage submissions and Insikt Group reporting, Command and Control (TA0011) was the most frequently observed malware tactic, with over 194,000 detections. Top techniques (according to the [MITRE ATT&CK matrix](#)) included data encrypted for impact (T1486), valid accounts (T1078), and data from local systems (T1005), emphasizing the prevalence of ransomware deployment and the importance of persistent access to obtain and exploit sensitive data.
- The mobile threat landscape continued to evolve during the first half of 2025, marked by the discovery of eleven new mobile malware strains and the resurgence or continued operation of nine others. This included banking trojans, infostealers, spyware, and RATs. Long-standing tactics, techniques, and procedures (TTPs) like overlay attacks remained common, though with some innovation.
- Threats to contactless payments increased, as evidenced by the discovery of SuperCard X, a Chinese MaaS platform that enables NFC relay fraud by capturing and transmitting contactless card data to attacker-controlled devices.
- Ransomware threat actors adopted new TTPs across the attack chain during the first half of 2025. This included ClickFix-based social engineering for initial access, endpoint detection and response (EDR) evasion via bring-your-own-installer (BYOI) techniques, and custom payloads using just-in-time (JIT) hooking and memory injection to bypass detection. Ransomware threat actors also continued to use legitimate tools for persistence, data theft, and stealthy C2, including AnyDesk to maintain access, Syteca for keylogging, and GC2 for cloud-based C2.

Table of Contents

Vulnerability Exploitation Trends	4
Key Takeaways	4
Microsoft Leads Actively Exploited Vulnerabilities as Total Disclosed Vulnerabilities Rise Compared to 2024	4
UNC5221 Focuses on Ivanti Products as Cobalt Strike Is Most Frequently Associated with Post-Exploitation Activity	7
Insikt Group Detection Rules Maintain Alignment with Known Exploited Vulnerabilities	11
Malware Trends	13
Key Takeaways	13
Botnets and the Return of Legacy Malware in C2 Detections	13
Malware TTP Trends and Insights	15
Mobile Malware	19
An Ever-Expanding Landscape	19
Threat Actors Favor Fake Downloads, Abuse Official Stores, and Exploit Supply Chains	20
Accessibility Service Abuse With a Twist	20
Threats to Contactless Payments Continue to Rise	21
Ransomware	22
Ransomware Groups Innovate to Attract Affiliates Amid a Reshaped Landscape	22
New Initial Access, Defense Evasion, and Malware Deployment Techniques	24
Magecart Infections Remained High in H1 2025	25
Mitigations	27
Vulnerability Exploitation	27
Malware Intrusions	27
Magecart Attacks	28
Outlook	29

Vulnerability Exploitation Trends

Key Takeaways

- 23,667 CVEs were published in H1 2025, a 16% increase compared to H1 2024. Attackers actively exploited 161 vulnerabilities, and 42% of those exploited flaws had public PoC exploits. 21 out of the 27 Nuclei templates published by Insikt Group corresponded to vulnerabilities that appear in the US Cybersecurity and Infrastructure Security Agency (CISA) Known Exploited Vulnerabilities (KEV) catalog.
- Microsoft products accounted for 17% of such exploitations, but attackers also concentrated on edge-security and gateway appliances such as SSL-VPNs and next-gen firewalls (similarly 17%), whose position at the network perimeter makes them attractive entry points for attacks that can later propagate through downstream supply chains.
- 69% of exploited vulnerabilities did not require authentication, and nearly one-third enabled RCE. 151 exploited vulnerabilities were used to deploy malware and 73 to launch ransomware, with backdoors the most common payload. State-sponsored actors drove more than half of the attributed exploitation, highlighting the significant strategic drivers of such attacks, as well as such actors' capabilities to weaponize flaws shortly after disclosure.

Microsoft Leads Actively Exploited Vulnerabilities as Total Disclosed Vulnerabilities Rise Compared to 2024

In the first half of 2025, the volume of disclosed vulnerabilities continued to climb. The total number of CVEs increased by 16% compared to H1 2024, rising from 20,385 in H1 2024 to 23,667 in H1 2025. This growth suggests an expanding attack surface and more opportunities for threat actors to find exploitable flaws. Notably, the most common vulnerability types by weakness were web application issues: [Cross-Site Scripting \(CWE-79\)](#) and [SQL Injection \(CWE-89\)](#) represented the highest share of weaknesses, followed by [Cross-Site Request Forgery \(CWE-352\)](#), generic [Injection flaws \(CWE-74\)](#), and [Missing Authorization \(CWE-862\)](#). This highlights that fundamental security gaps in web applications remain widespread, and organizations should heed these trends; the persistence of injection and scripting weaknesses means attackers will continue to find easy targets in poorly secured web interfaces.

When looking at actively exploited vulnerabilities in H1 2025, Microsoft products dominated the field. Microsoft accounted for the highest number of actively exploited CVEs with 28 (see **Figure 1**), of which twenty targeted Windows specifically. This tally was more than triple that of the next most targeted vendors: Apple (eight), Ivanti (seven), and Linux (six). The outsized targeting of Microsoft likely reflects the ubiquity of Windows across enterprises; attackers naturally prioritize vulnerabilities in widely deployed systems to maximize potential victims. In total, Insikt Group identified exploited vulnerabilities

affecting 81 distinct vendors. This breadth indicates that exploitation in the wild is not concentrated on just a few big-name software suites; instead, attackers are casting a wide net.

Attackers continue to opportunistically probe less common software and environments, likely perceiving that organizations may delay patches or have limited monitoring on those systems, making them softer targets. For defenders, this means a robust patch management program cannot ignore the long tail of software assets: a vulnerability in a lesser-known product can still be the entry point for a major breach if left unpatched.

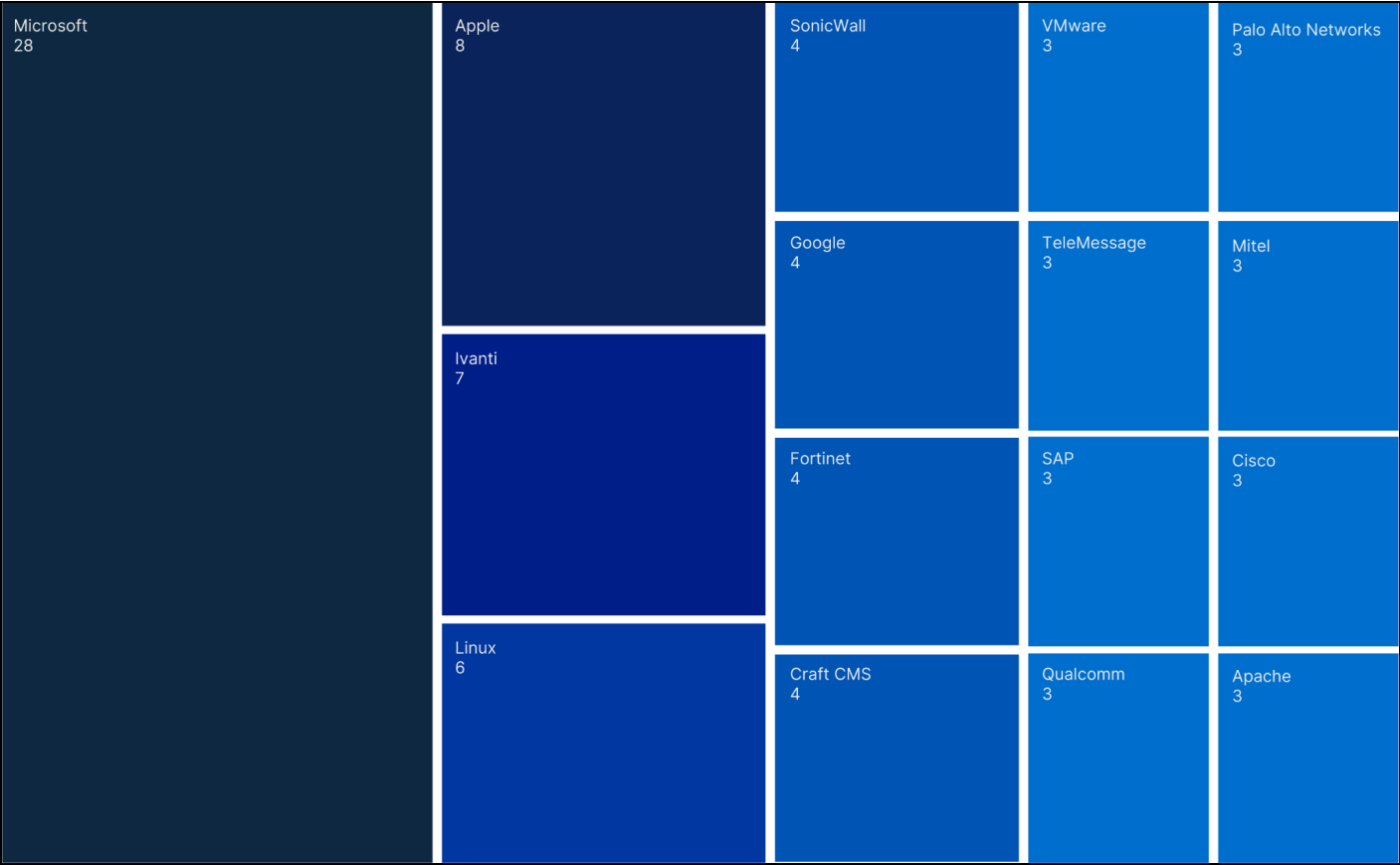


Figure 1: Top ten vendors (including ties) by number of actively exploited CVEs in H1 2025 (Source: Recorded Future)

Another notable trend is the focus on vulnerabilities in the tools designed to keep networks safe. 17% of the actively exploited CVEs affected edge-security and gateway products. This included SSL-VPNs, next-gen firewalls, secure gateways, and remote access portals from vendors such as Ivanti, SonicWall, Fortinet, Palo Alto, Cisco, Citrix, Juniper, and Sophos, as well as virtualization underlays like VMware.

Because these appliances terminate VPNs, decrypt traffic, and broker trust between networks, a single exploit instantly grants attackers a privileged, authenticated pathway into an organization’s environment for initial access and lateral movement. For instance, CVE-2025-0282 (Ivanti Connect Secure and Policy Secure) allowed remote, unauthenticated attackers to execute arbitrary code on the appliance and steal credentials for further lateral movement inside the network. This trend underscores that threat

actors — including well-resourced state-sponsored groups — are increasingly targeting these security infrastructure platforms to operate with minimal detection. Organizations must harden and promptly patch their network edge devices and monitor them closely, as these systems have become high-value targets that attackers use to bypass traditional defenses and pivot deep into corporate networks.

Attackers were observed exploiting 161 distinct vulnerabilities in the first half of 2025, according to Recorded Future data. This exceeds the 136 vulnerabilities listed in CISA's [KEV catalog](#) for the same timeframe. In other words, Recorded Future telemetry identified 25 additional exploited CVEs beyond what was publicly recognized by CISA during that period.

Of those 161 exploited flaws, 68 (42%) had a publicly available PoC exploit (see **Figure 2**). The availability of a PoC lowers the bar for exploitation, effectively allowing a larger pool of attackers (including less-skilled threat actors) to weaponize the vulnerability. In multiple cases, Insikt Group has observed exploitation activity surge within days or hours of a PoC release. Organizations should therefore implement rapid patching or interim mitigations to limit the window of exposure.

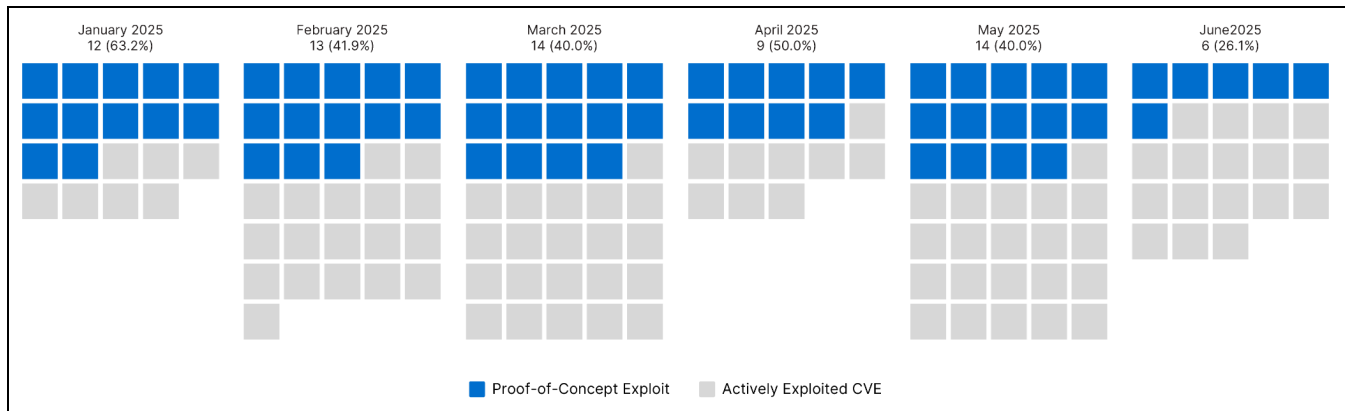


Figure 2: Actively exploited vulnerabilities with a public PoC exploit, by month (Source: Recorded Future)

In terms of access requirements and impact, **Figure 3** shows that 111 (69%) of the 161 vulnerabilities required no authentication to exploit, and 78 (48%) could be exploited remotely over a network (as opposed to requiring local access or user interaction). In other words, this heavy tilt toward unauthenticated, remote exploits means that attacks can be launched directly from the internet against vulnerable hosts, with no credentials or insider access needed.

48 (30%) of the exploited CVEs enabled RCE, which often grants an attacker full control over the target system, while another 11 (7%) enabled privilege escalation, which is typically used to gain higher system access. None of the exploited vulnerabilities facilitated lateral movement (exploits that facilitate jumping from one system to another). Given that so many exploited flaws are both remotely exploitable and require no valid user account, organizations must proactively scan and prioritize patching for internet-facing applications and services.

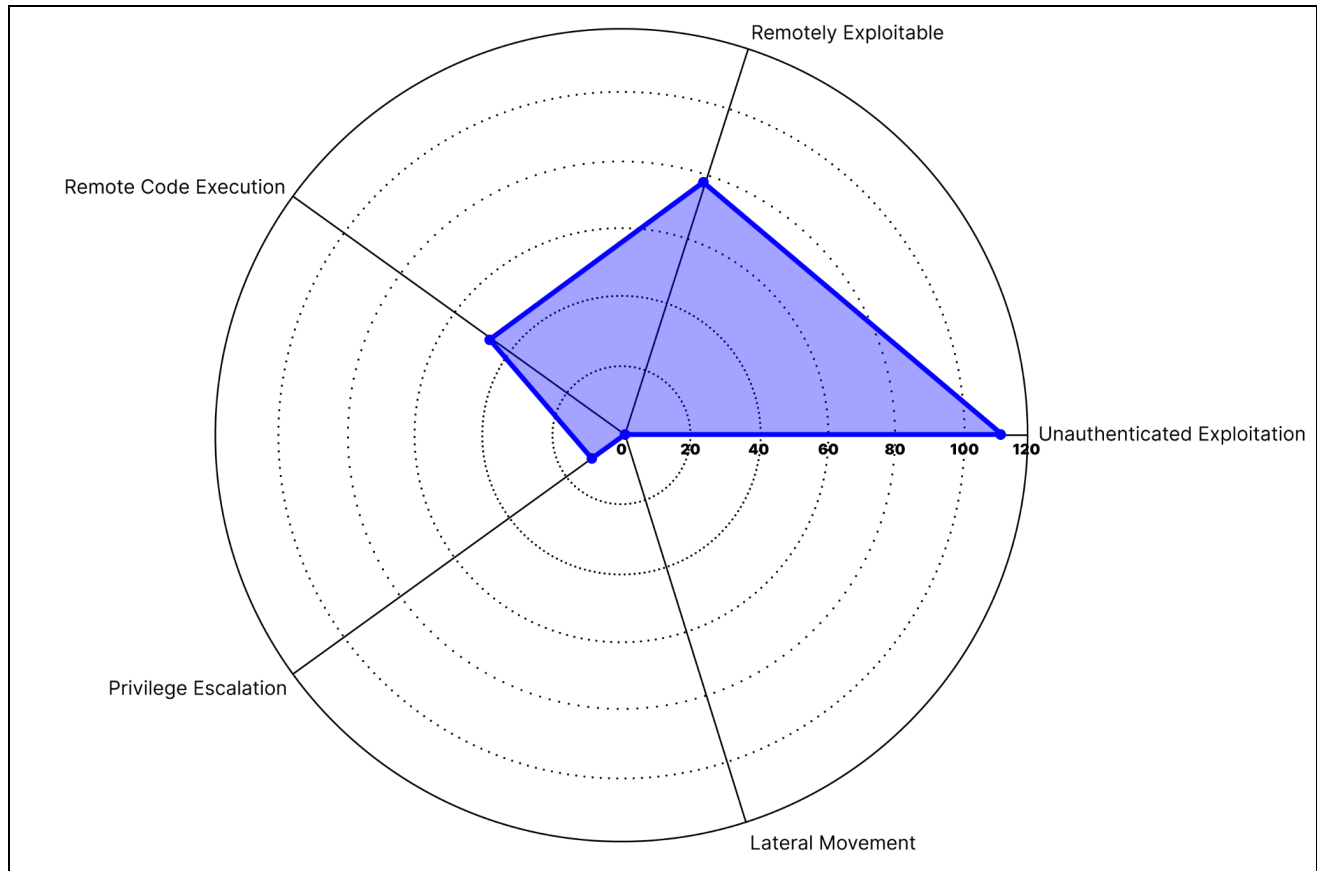


Figure 3: Actively exploited vulnerabilities by impact factors (Source: Recorded Future)

UNC5221 Focuses on Ivanti Products as Cobalt Strike Is Most Frequently Associated with Post-Exploitation Activity

The threat actors exploiting these vulnerabilities range from sophisticated state-sponsored groups to profit-driven cybercriminals, and the data from H1 2025 highlights the significant role of state-sponsored campaigns. In cases where Insikt Group could determine attribution, nearly 53% of the observed exploitation activity was driven by state-sponsored and suspected state-sponsored actors. This illustrates that more than half of the attributed exploitations were strategic in nature and conducted for espionage, surveillance, or other geopolitical objectives.

Financially motivated groups (those involved in, for example, theft and fraud and not necessarily linked to ransomware) accounted for 27% of exploitations. Another 20% of exploitation was attributed to ransomware and extortion groups, reinforcing how common it has become for ransomware operators to leverage exploits as an initial access vector to then conduct file-encrypting attacks at scale.

This breakdown highlights that both strategic and criminal motivations are driving vulnerability exploitation, with a notable absence of any known hacktivist campaigns; hacktivist collectives are typically motivated by disruption and likely lack the intent and capability to conduct such exploitations.

By contrast, the presence of state-sponsored actors at the top underlines that many governments' cyber units have the resources to weaponize new flaws quickly, often within days of a disclosure. The significant state-sponsored involvement also implies that these threats are not just random or opportunistic but often targeted and persistent campaigns aiming at specific sectors or high-value systems.

Geographically, the majority of state-sponsored campaigns were conducted by Chinese state-sponsored actors or suspected China-linked actors. Such groups are known to exploit edge infrastructure and enterprise solutions to establish footholds in target networks, and Insikt Group's observations in the first half of 2025 reaffirm that. The suspected China-linked group UNC5221 exploited the highest number of vulnerabilities and demonstrated a preference for Ivanti products, targeting Ivanti Endpoint Manager Mobile (EPMM; CVE-2025-4428) and Ivanti Connect Secure and Policy Secure (CVE-2025-22457 and CVE-2025-0282).

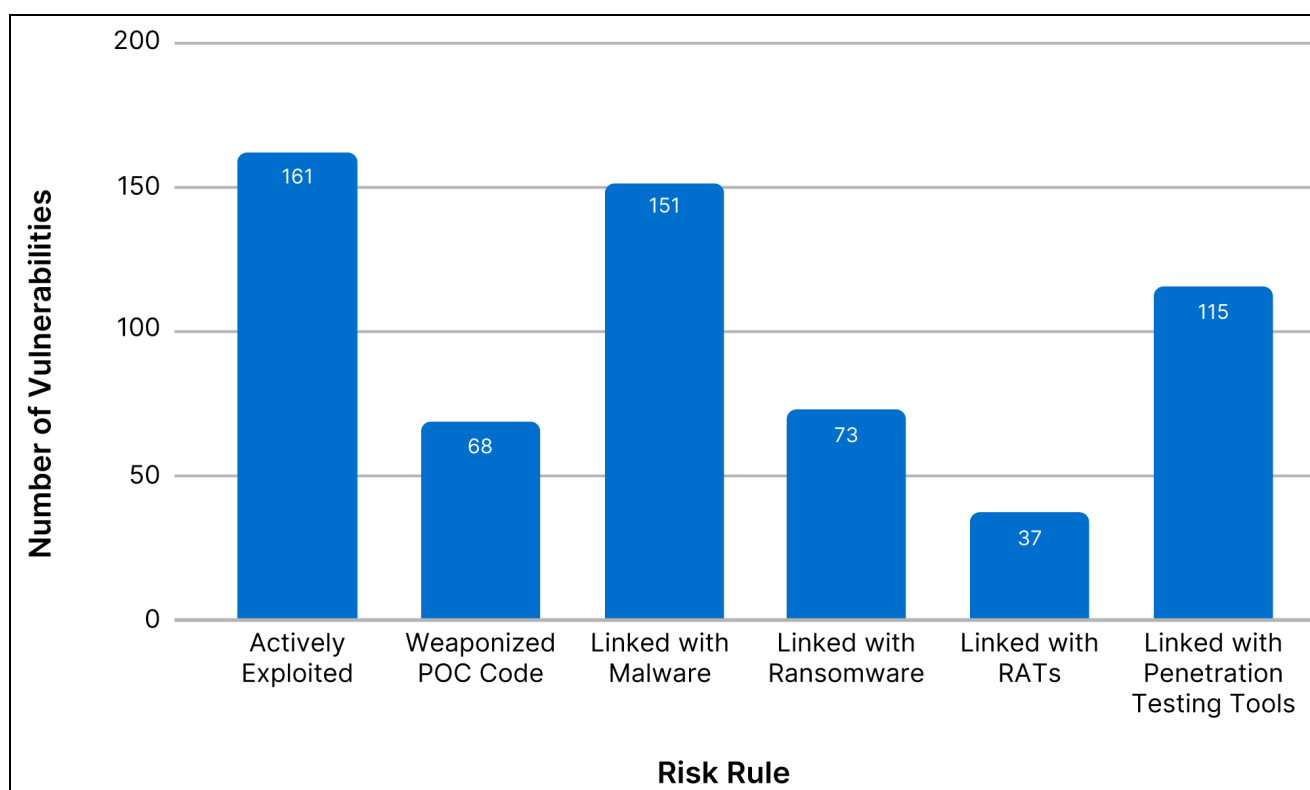


Figure 4: Vulnerabilities by triggered risk rule, based on Recorded Future data (Source: Recorded Future)

Of the 161 exploited vulnerabilities, Recorded Future data shows that 151 were leveraged in some form of malware deployment (see **Figure 4**). Within those, 73 vulnerabilities were specifically tied to ransomware deployments — they were either the initial access point for a ransomware attack or used at some stage in the ransomware kill chain. In practical terms, unpatched vulnerabilities are a common entry point for attackers to introduce malware into a victim's environment; whether the ultimate payload is a remote access trojan (RAT) or ransomware, the initial step of exploiting a weakness is the same.

Insikt Group found that the most commonly observed malware used post-compromise was the offensive security tool Cobalt Strike. Tools such as Cobalt Strike are ideal for gaining a reliable foothold for attackers as they provide a full-featured toolkit to run commands, escalate privileges, and move laterally, while blending in with normal network traffic. After Cobalt Strike, the Vshell RAT was the malware most frequently observed alongside exploitation.

Overall, as shown in **Figure 5**, backdoor malware accounted for nearly 23% of all post-exploitation activity. The frequent appearance of backdoors and various trojans means that a single exploit often leads to multi-payload efficiency for attackers: with one vulnerability, they may deploy a backdoor, which then allows them to stage additional tools or eventually deliver ransomware, all from that same initial entry point and without needing to develop custom malware.

For defenders, this trend is a reminder to monitor for known post-exploitation tools and behaviors. The presence of Cobalt Strike beacons, for example, should be treated as an immediate high-priority incident, while an unusual use of legitimate admin tools or new services could indicate that a RAT or backdoor is running.

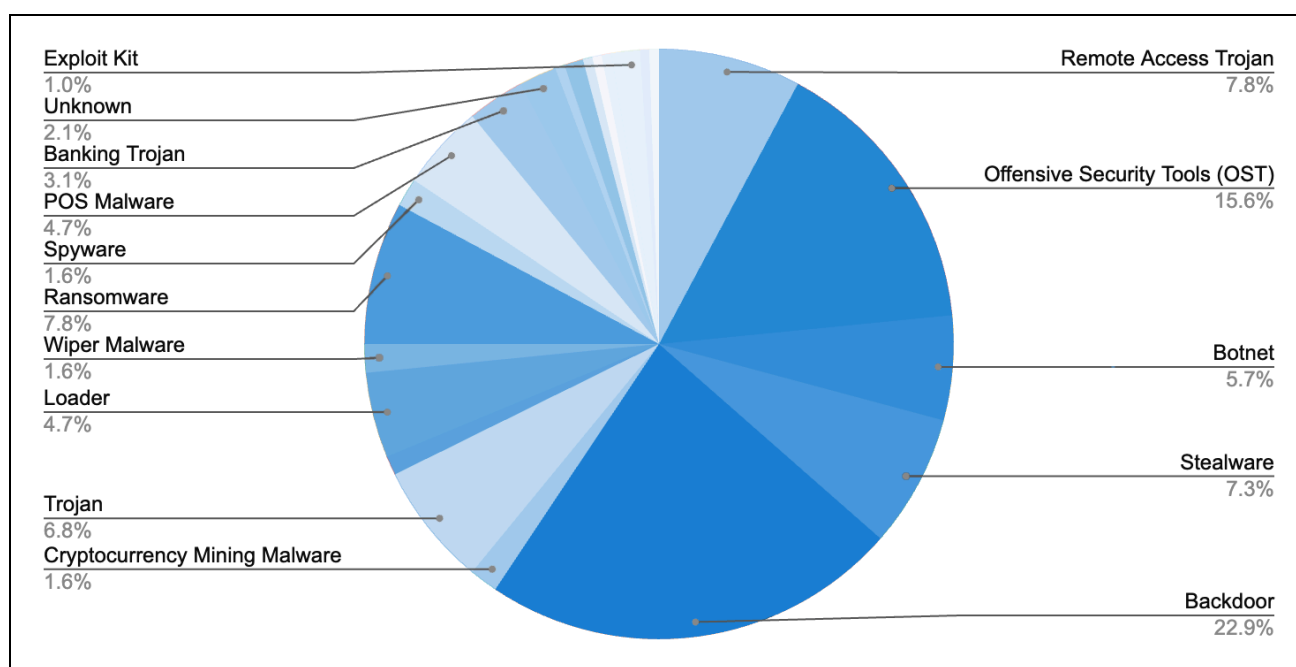


Figure 5: Actively exploited vulnerabilities by malware category (Source: Recorded Future)

From a tactics and techniques perspective, the patterns of exploitation in the first half of 2025 align with known adversary behaviors in the MITRE ATT&CK framework. The most frequent ATT&CK technique was Exploit Public-Facing Application (T1190), observed in 73% of actively exploited vulnerabilities. This was followed by Exploitation for Client Execution (T1203) and Exploitation for Privilege Escalation (T1068). These three techniques demonstrate a clear picture of attacker preferences and playbooks. T1190 indicates that attackers are heavily targeting servers and services

exposed to the internet (for example, web servers or VPN gateways), which is a direct route into a network.

The prevalence of T1203 shows that attackers are also investing in exploits that require user interaction (for example, a malicious email attachment or drive-by download that triggers an exploit on the victim's end). In these scenarios, the vulnerability may be in a client-side application such as a browser or office document software, and the attacker socially engineers the victim into running the exploit. T1068 underscores that once attackers get a foothold, they often elevate their privileges (for example, going from a normal user to SYSTEM or root). This pattern shows how attackers frequently leverage initial access, execution, and privilege escalation into a single exploit chain, and illustrates how an attacker can go from having no access to domain admin privileges if the right combination of unpatched flaws exists.

Internet-facing systems and unpatched client software will remain prime targets, and failing to patch those creates an avenue for attackers to get in and escalate their privileges. Defenders should ensure both their perimeter systems and endpoint applications are up to date, and have monitoring in place for exploit attempts.

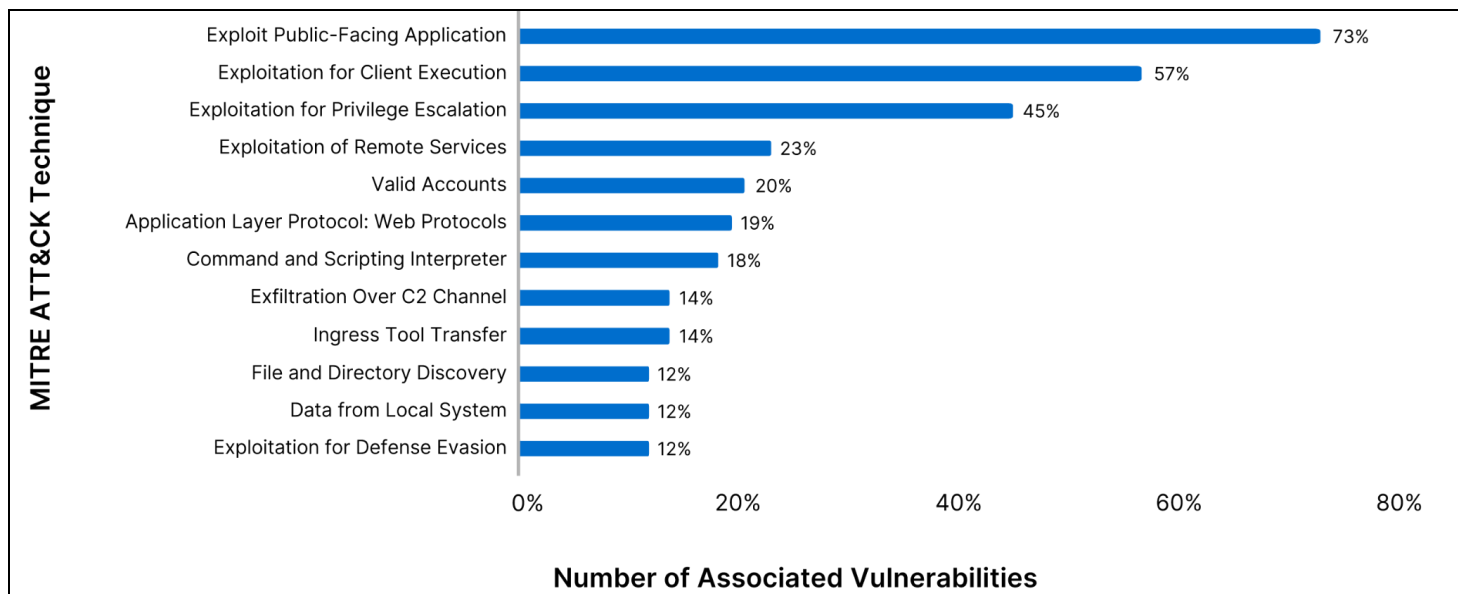


Figure 6: Share of actively exploited vulnerabilities by the most common MITRE ATT&CK techniques (Source: Recorded Future)

Insikt Group Detection Rules Maintain Alignment with Known Exploited Vulnerabilities

In the first half of 2025, Insikt Group's own detection efforts kept pace with the evolving threat landscape by continuously creating new Nuclei templates (automated vulnerability detection signatures). Insikt Group created 27 new Nuclei templates designed to identify vulnerable systems, focusing on the most dangerous flaws. 21 out of the 27 templates corresponded to vulnerabilities that appear in CISA's KEV catalog. In other words, the majority of Insikt Group's detection rules were directly aligned to vulnerabilities that were known to be actively exploited in the wild.

The vendors that showed up most frequently in Insikt Group's Nuclei templates were Fortinet, Apache, and Ivanti, which is consistent with the threat trends observed. By developing Nuclei templates for these vendors' vulnerabilities, Insikt Group helped equip organizations to rapidly scan their infrastructure and find any unpatched instances before attackers do.

Notably, Insikt Group published 13 unique Nuclei templates that do not have an existing public template available from Project Discovery (see **Figure 7**). In those cases, Insikt Group authored and shared the detection logic for vulnerabilities that were not yet covered by the open-source community for Nuclei signatures, filling critical detection gaps for Recorded Future customers.

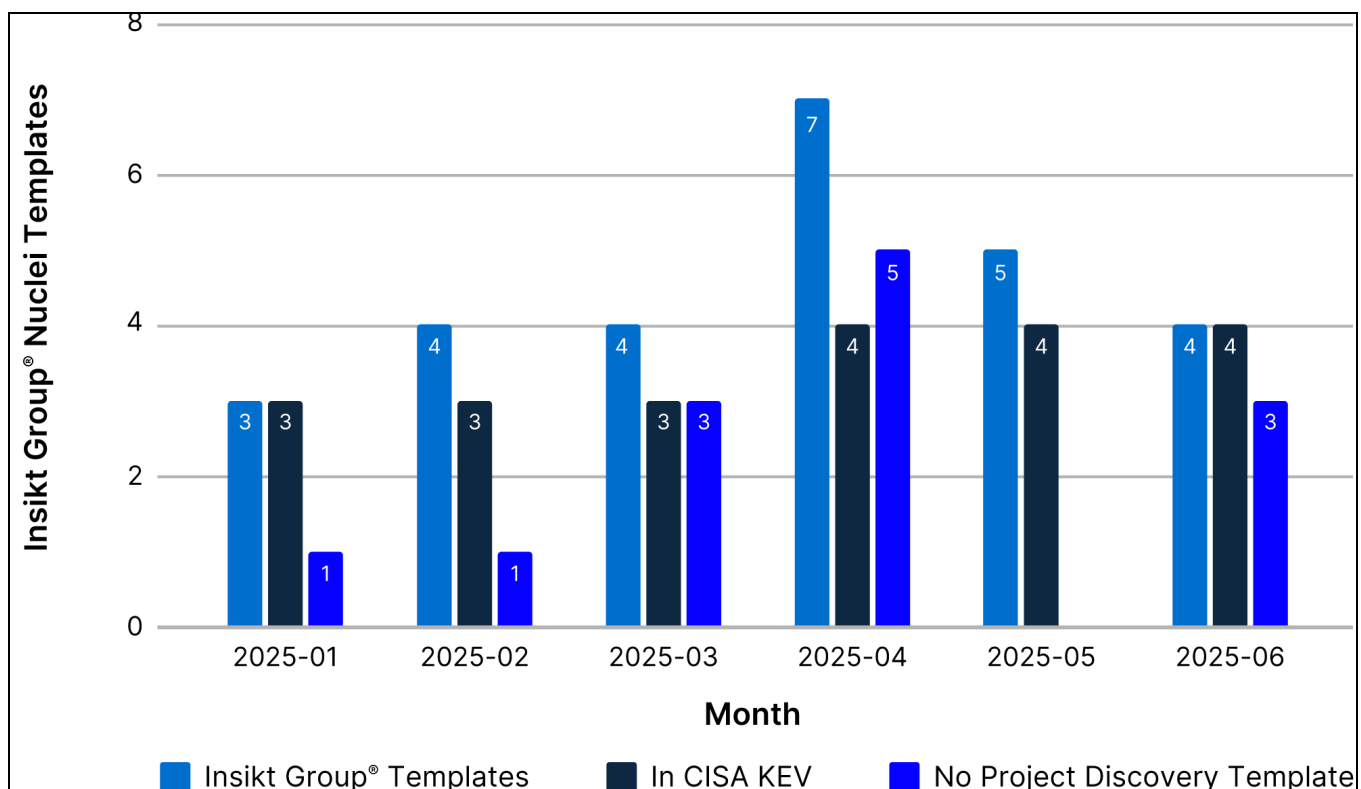


Figure 7: Overlap of Insikt Group Nuclei templates with CISA KEV and Project Discovery
(Source: Recorded Future, CISA, Project Discovery)

Additionally, **Figure 8** shows the time between Insikt Group's publication of a Nuclei template and the targeted vulnerability's addition to CISA's KEV catalog (the below chart only lists CVEs that both had a template and were added to KEV). Five vulnerabilities that were added to KEV in H1 2025 — CVE-2025-32433 (Erlang SSH), CVE-2025-24813 (Apache Tomcat), CVE-2024-41713 and CVE-2024-55550 (Mitel MiCollab), and CVE-2024-56145 (Craft CMS) — had an existing Insikt Group Nuclei template available. This means organizations leveraging Insikt Group's detections could scan for those issues as soon as (or even before) they were formally recognized as actively exploited by CISA.

For vulnerabilities added to KEV in 2025 for which Insikt Group did not already have a Nuclei template, the average turnaround time to publish a new template was 8 days after the KEV listing.

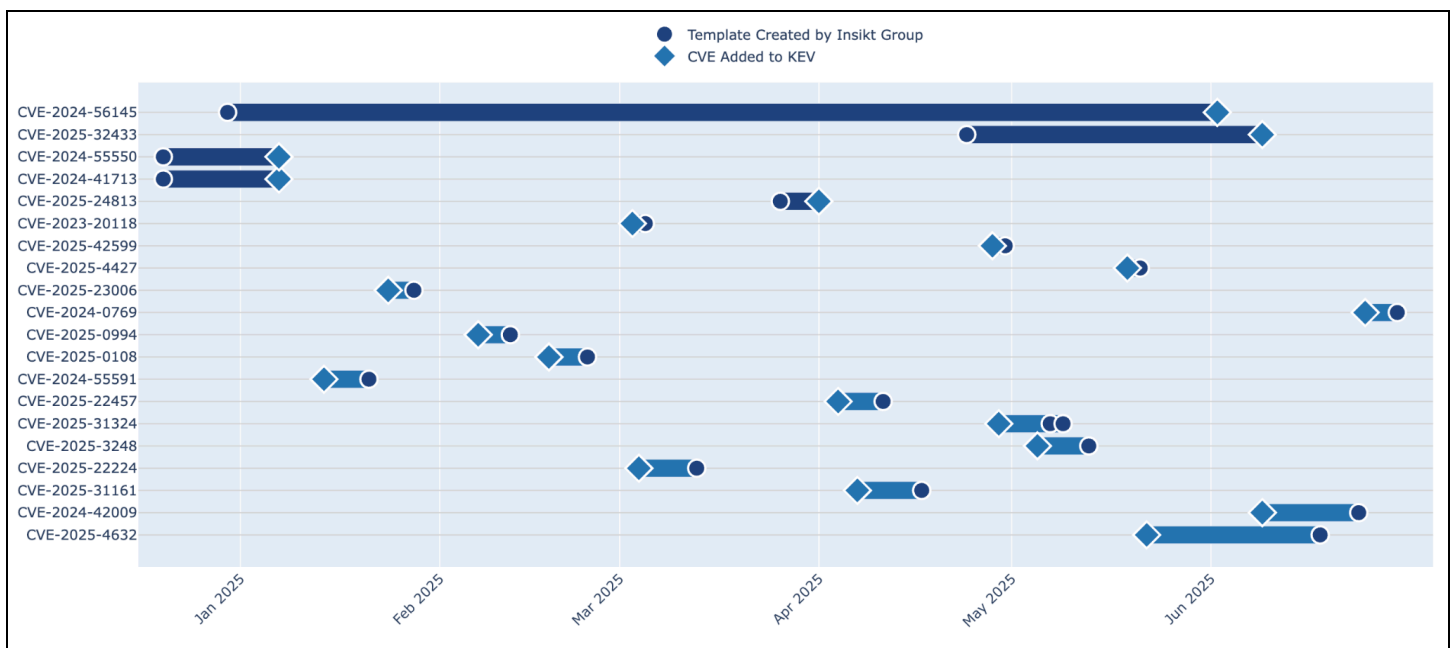


Figure 8: Timeline comparison of Insikt Group's Nuclei template releases and CISA KEV's CVE inclusions in H1 2025
(Source: Recorded Future)

Furthermore, during vulnerability testing and validation, Insikt Group discovered that Apache Tomcat 8.5.x versions (specifically 8.5.0 to 8.5.98 and 8.5.100, with the exception of 8.5.99) were also vulnerable to CVE-2025-24813, even though they were not included in Apache's initial list of affected product versions. In practice, this meant that many organizations running slightly older Tomcat 8.5 releases could have been unknowingly at risk if they only followed the vendor's advisory. By identifying those versions and providing a Nuclei template, Insikt Group provided a detection rule and an early warning and remediation guidance beyond what the vendor had first communicated.

Malware Trends

Key Takeaways

- Legacy malware families such as Sality and Tofsee reemerged as top threats, with Sality ranking first in configuration-based C2 detections — a notable shift from recent infostealer-dominated trends and a sign that threat actors are repackaging older codebases for modern use.
- Commodity remote access trojans (RATs) like AsyncRAT, XWorm, and Remcos were prominent in Recorded Future Triage data, including malware C2 extractions, reflecting a continued preference among threat actors for tools that support persistent access and data theft across varied intrusion campaigns.
- MITRE ATT&CK Tactic TA0011 (Command and Control) was the most frequently observed TTP across Recorded Future Triage submissions and Insikt Group reporting, with over 194,000 events recorded in H1 2025. Other commonly used techniques included data encryption, local data theft, and credential abuse, highlighting the emphasis on monetization and lateral movement.
- Ransomware threat actors adopted new TTPs across the attack chain, including ClickFix-based social engineering for initial access, EDR evasion via BYOI techniques, and custom payloads using JIT hooking and memory injection to bypass detection. Ransomware threat actors also used legitimate tools for persistence, data theft, and stealthy C2.
- Magecart infections remained elevated, with threat actors continuing to abuse Google Tag Manager (GTM), obscure HTML tags, and even CSS `::before` content properties to deploy modular e-skimmers on e-commerce platforms while evading content security policies.

Botnets and the Return of Legacy Malware in C2 Detections

Recorded Future identifies command-and-control (C2) servers based on malware configurations extracted from samples submitted to Recorded Future Triage. References to malware families in C2 detections in H1 2025 show major changes compared to H1 2024 in terms of prevalent malware families. Infostealers remain a cornerstone of the threat landscape, consistent with most threat actors' financial motivations, as stolen credentials, payment data, and crypto wallets can be [monetized](#) directly or sold on dark web markets. However, the specific malware driving these C2 detections has shifted. Several of H1 2024's top ten malware (Vidar, RedLine Stealer, and LokiBot, for example) have largely fallen off in 2025, owing in part to disruptive operations and law enforcement actions, while other malware families surged or emerged to take their place.

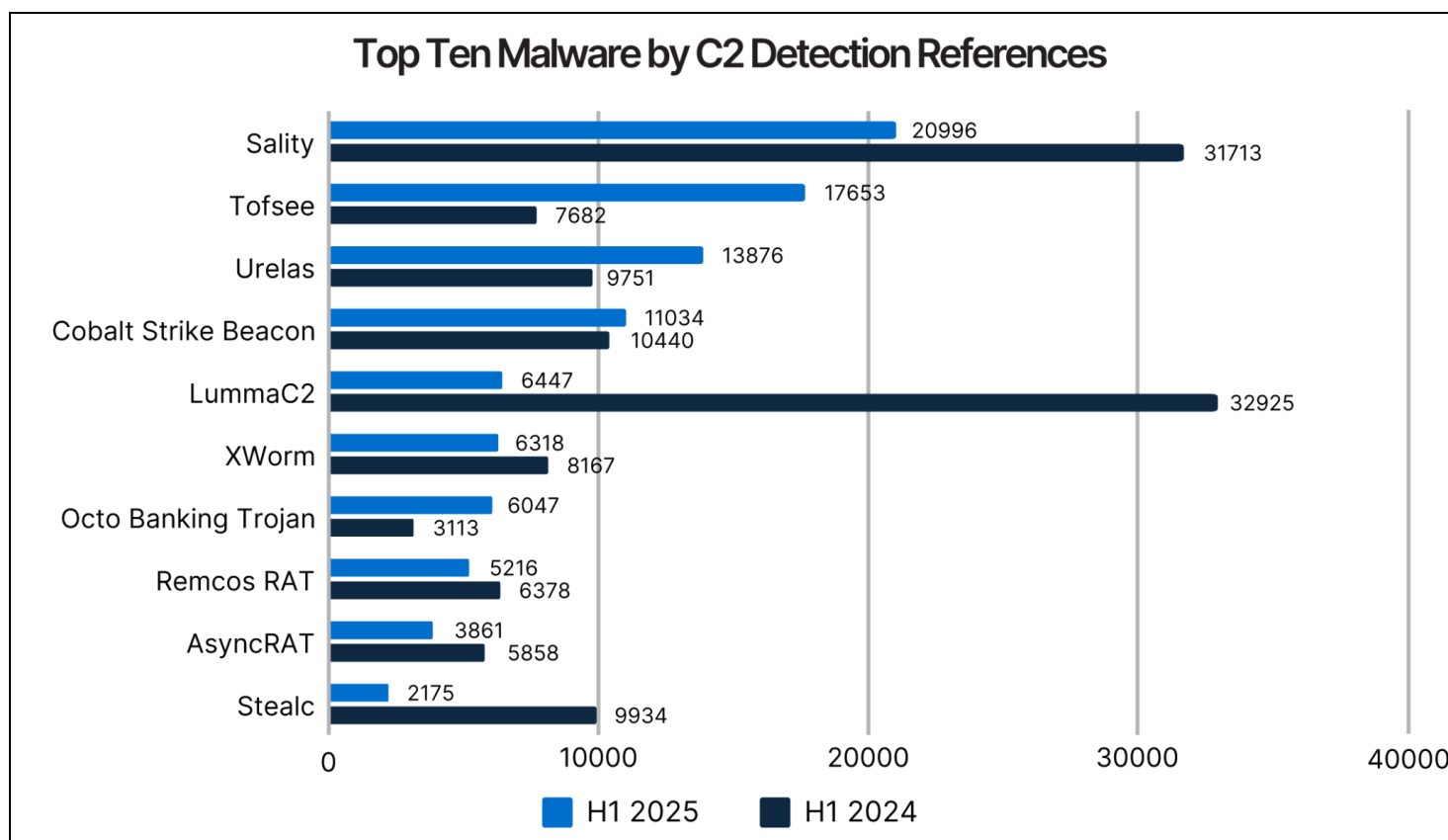


Figure 9: The top ten malware families by number of references to C2 detections in H1 2025 and H1 2024
(Source: Recorded Future)

H1 2025's C2 detections also highlight the enduring presence of long-lived malware. Sality, a polymorphic botnet first seen in 2003, remains in the top tier after a major [resurgence](#) in 2024, demonstrating the resilience of legacy threats. Likewise, the Tofsee trojan (active for over a decade) appears among the top families. Tofsee is a modular backdoor [capable](#) of spamming, DDoS attacks, cryptomining, and more, and its continued activity further demonstrates how older malware can persist as a steady backbone of criminal operations. The presence of these botnets, even as their absolute reference counts are far below last year's peak levels, indicates that threat actors still find value in exploiting well-established malware infrastructure that has stood the test of time. Notably, Sality's and Tofsee's ongoing use suggests that some attackers favor legacy tools either for their reliability or simply to target less-protected systems, even amid a constant influx of new malware. This mirrors the trend [observed](#) in H1 2024 with Sality's reappearance, reinforcing that "outdated" malware can remain unexpectedly prevalent.

Meanwhile, last year's infostealer frontrunner LummaC2 has seen a precipitous decline, likely a consequence of coordinated [takedowns](#) by law enforcement agencies. In late May 2025, an international operation [seized](#) LummaC2's infrastructure — over 2,300 domains — and wiped its main server, severely disrupting this malware-as-a-service. As a result, LummaC2 all but vanished from the top ranks for H1 2025, echoing RedLine Stealer's massive drop-off following the April 2023 GitHub repository [takedown](#) that broke RedLine's C2 panels. However, Insikt Group recently discovered that

LummaC2 operators have begun to reestablish infrastructure using Cloudflare-based C2 domains, signaling at least a partial operational recovery. Multiple new domains tied to LummaC2, observed as recently as mid-July 2025, resolve to Cloudflare IP addresses — a shift back to previous tactics following an initial pivot away from the provider after the takedown. This rapid pivot highlights the underlying resilience and [adaptability](#) of LummaC2's operators, who appear capable of reconstituting infrastructure and tactics even in the wake of extensive disruption.

Another development in H1 2025 is the increased prominence of remote access trojans (RATs) in C2 detections. Several commodity RAT families, including Remcos, AsyncRAT, and XWorm, climbed into the top ten this period. These RATs are freely or cheaply available and grant attackers hands-on control over compromised systems, making them versatile for espionage and data theft and as launchpads for ransomware. The ascent of these RATs suggests that many threat actors are leveraging RATs to maintain persistent, interactive access in victim environments, an approach favored by financially motivated groups and advanced actors alike. Their growing share in C2 detections may also imply that, as some infostealing services were disrupted, adversaries pivoted to using RATs, which often include info-stealing capabilities, as an alternative means to achieve similar goals.

Overall, the C2 detection trends of H1 2025 reflect an evolving threat landscape that is both dynamic and cyclical. While Insikt Group observes constant churn at the top, some long-standing threats and tools never truly disappear but persist or resurge in cycles, contributing steadily to the baseline of malicious activity. Financially motivated actors remain dominant, favoring infostealers and RATs that directly feed their profit motives. H1 2025's C2 detections were defined by a revival of credential-stealing trojans amid a backdrop of resilient legacy botnets and increased reliance on RATs for interactive control. These trends underscore that defenders must be prepared for both cutting-edge malware and the enduring tactics of established threats moving into the latter half of 2025 and beyond.

Malware TTP Trends and Insights

Between January and June 2025, Recorded Future's Insikt Group analyzed and aggregated thousands of malware-related observations to identify the top tactics, techniques, and procedures (TTPs) employed by threat actors mapped to the MITRE ATT&CK® framework. This data is sourced from Recorded Future Triage public sandbox submissions and Insikt Group reporting. Leading the list by a significant margin is the Command and Control (TA0011) tactic, with over 194,000 observations, highlighting its central role in enabling adversary communication with compromised systems.

Frequently observed TTPs include Data Encrypted for Impact (T1486), indicative of widespread ransomware activity, and Data from Local System (T1005), pointing to persistent data theft operations. Initial Access (TA0001) techniques such as Valid Accounts (T1078) and External Remote Services (T1133) were also highly represented, indicating adversary focus on stealing credentials and then using them to gain access via external-facing remote services. External Remote Services is also a persistence technique, discussed later in this section.

Top Ten TTPs Observed in H1 2025

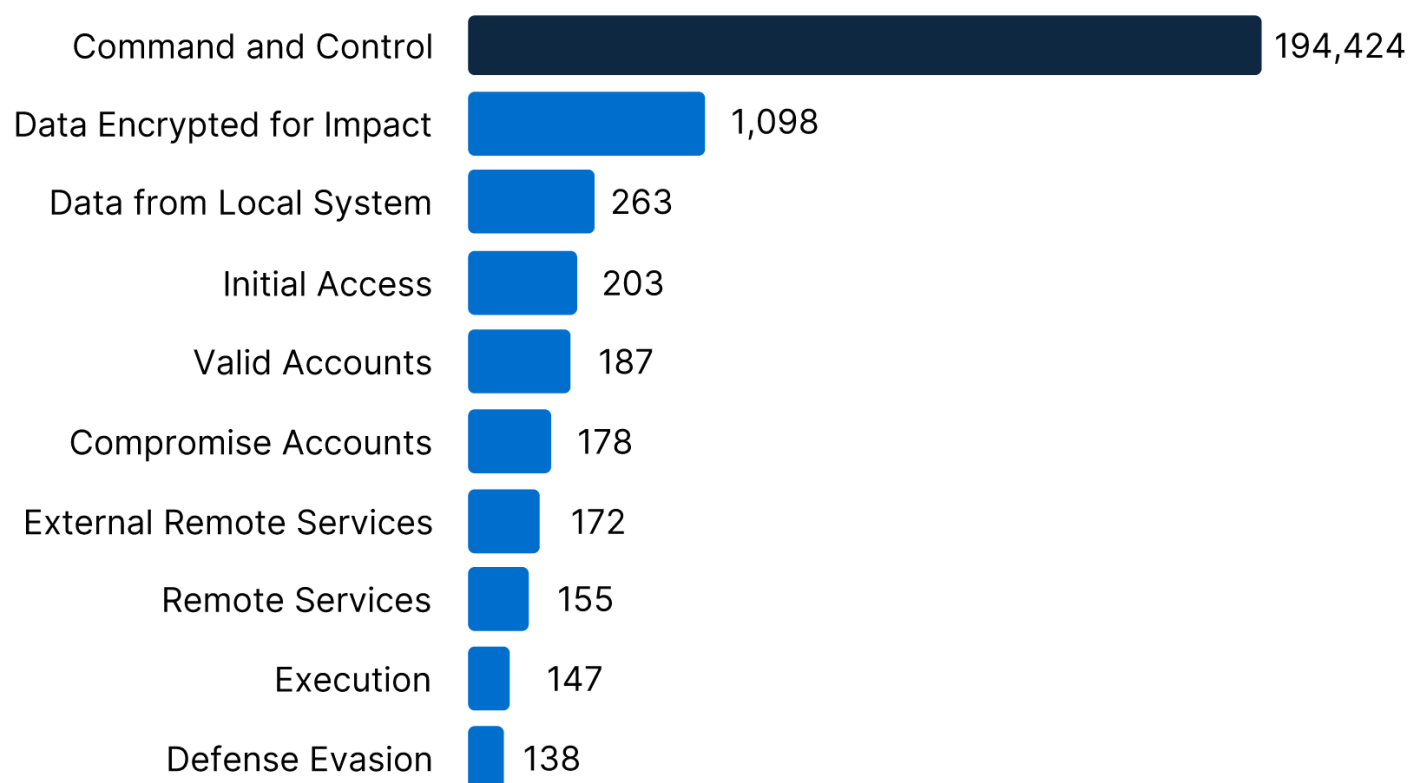


Figure 10: The top ten TTPs in H1 2025 based on Recorded Future Triage and Insikt Group reporting
(Source: Recorded Future)

Insikt Group observed ClickFix as a prominent, emerging initial access technique in H1 2025. ClickFix is a social engineering technique that tricks users into running malicious scripts by presenting deceptive error messages or verification instructions, either prompting them to paste and execute commands manually or by using clipboard hijacking to automate the process. First [identified](#) in October 2023, the technique gained significant traction in the latter half of 2024, with its use [surging](#) by 517% year-over-year during the first half of 2025, according to ESET.

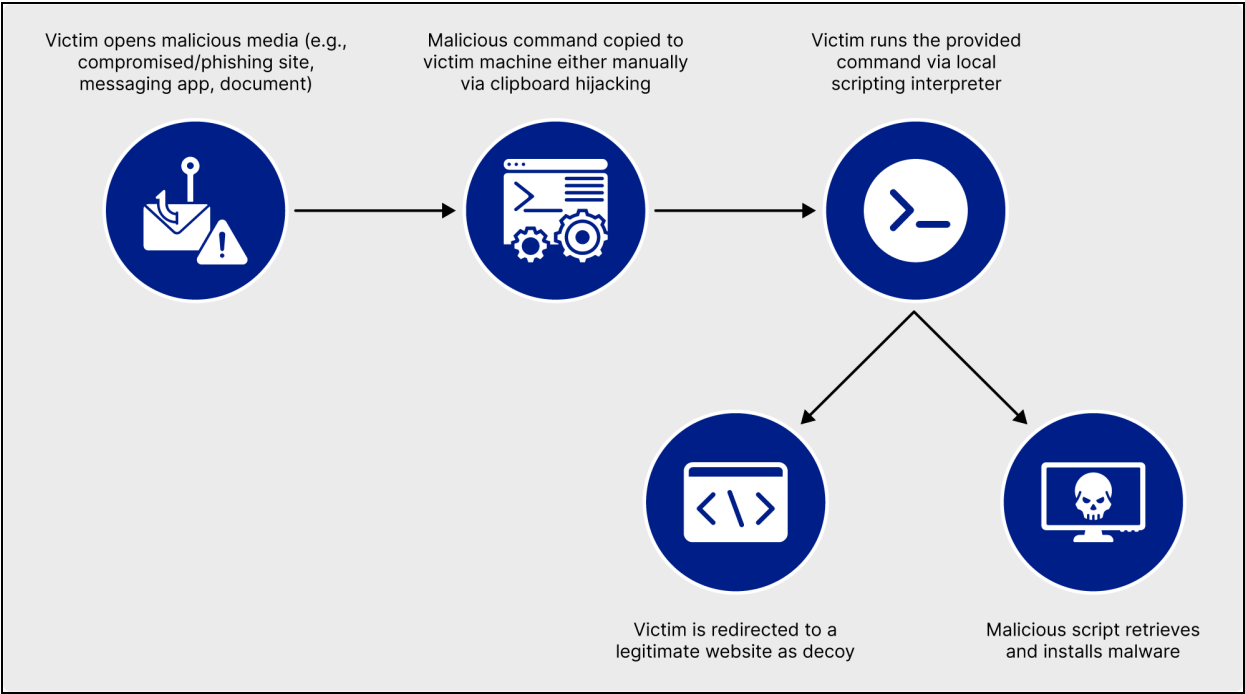


Figure 11: Illustration of ClickFix social engineering attack chain (Source: Recorded Future)

Further, the presence of Compromise Accounts (T1586) and External Remote Services (T1133) suggests adversaries are focusing on persistence and remote access. The technique Remote Services (T1021) supports lateral movement, while the tactics Execution (TA0002) and Defense Evasion (TA0005) round out the top ten, showcasing the breadth of tactics malware operators employ to infiltrate, persist, and evade detection across networks.

Cryptominer	RAT	Stealware	Offensive Security Tool	Botnet
XMRig	njRAT DCRat XWorm AsyncRAT	RedLine LummaC2 Stealc	Cobalt Strike	Mirai

Table 1: The top ten malware families in H1 2025 based on Recorded Future Triage public sandbox data² (Source: Recorded Future)

² In order to minimize false positives from historical or resubmitted samples and accurately represent in-the-wild observations, this data excludes certain malware families known to be defunct or polymorphic.

Based on Recorded Future Triage public sandbox data, from January to June 2025, XMRig Miner was the most-submitted malware family. XMRig Miner is a multi-stage cryptojacking tool, typically delivered via [malicious loaders](#) or [exploits](#), that covertly hijacks CPU resources to mine Monero (XMR), and [employs](#) evasion and persistence mechanisms to avoid detection and maximize uptime. Throughout H1 2025, Cobalt Strike, njRAT, DCRat, and XWorm rounded out the top five for public submissions to Recorded Future Triage.

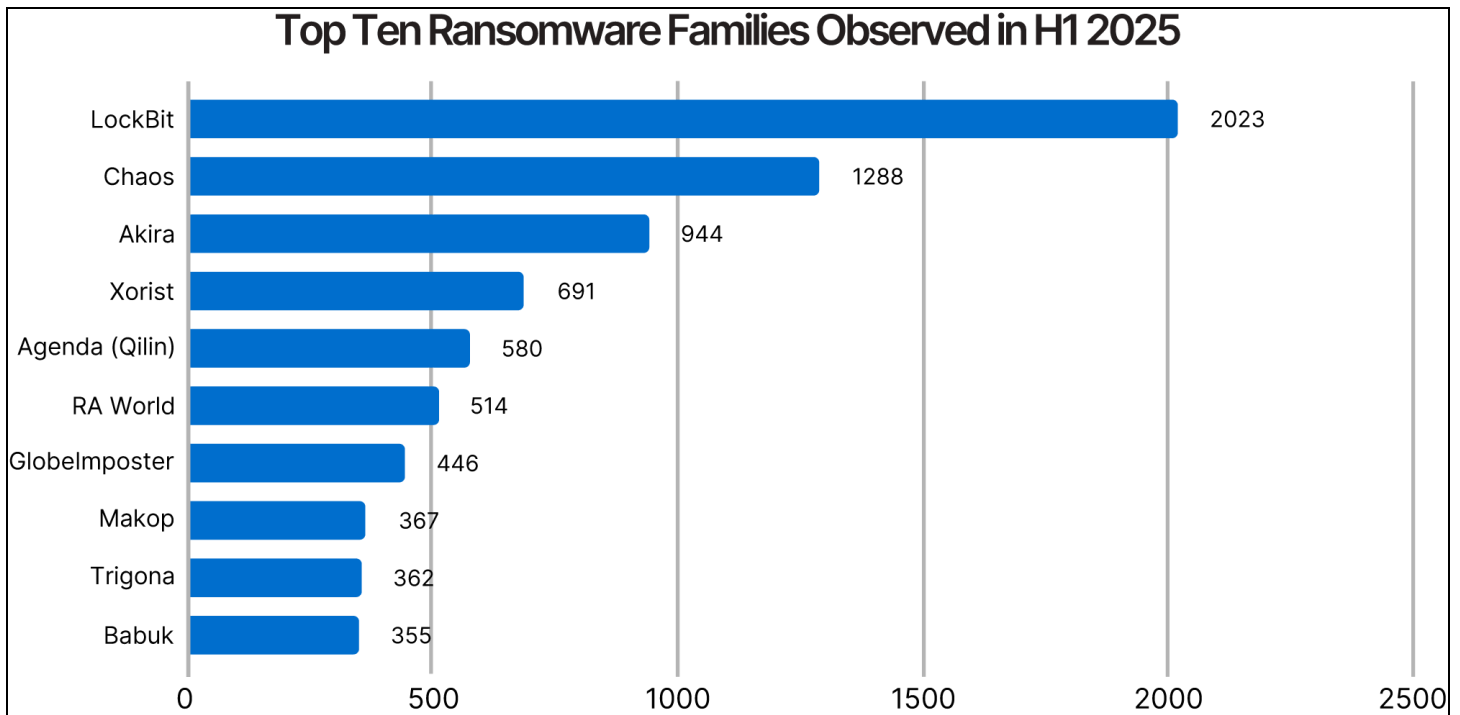


Figure 12: The top ten ransomware families in H1 2025 based on Recorded Future Triage public sandbox data³
(Source: Recorded Future)

Based on Recorded Future Triage public sandbox data, from January to June 2025, LockBit was the most-submitted ransomware family, followed by Chaos, Akira, Xorist, and Agenda (Qilin). LockBit is a notorious ransomware family that has remained operational despite significant law enforcement efforts to dismantle it, notably through "Operation Cronos" in early 2024, which aimed to disrupt its infrastructure. Babuk and Chaos had source code leaked in [June 2021](#) and [April 2022](#), respectively. This makes them more widely accessible for reuse, leading to the development of numerous variants, which likely contribute to their prevalence in Recorded Future Triage data.

³ In order to minimize false positives from historical or resubmitted samples and accurately represent in-the-wild observations, this data excludes certain malware families known to be defunct or polymorphic.

Mobile Malware

An Ever-Expanding Landscape

The mobile threat landscape continued to expand during the first half of 2025. Insikt Group identified at least eleven new malware strains, including RATs, infostealers, and spyware, and ongoing use or resurgence of nine others, including the multi-platform spyware Graphite, LightSpy, and Predator.





Banking Trojan	RAT	Spyware	Stealware
			
NEW	NEW	NEW	NEW
Crocodilus SuperCard X TsarBot	BTMOB Gorilla	Android.Spy.1292.origin SpyLend	Dcpro Salvador Stealer SparkKitty Tria Stealer
RESURGENT / ONGOING	RESURGENT / ONGOING	RESURGENT / ONGOING	RESURGENT / ONGOING
GodFather Marcher TgToxic	PJobRAT Triada	Graphite LightSpy Predator	SparkCat

Table 2: Overview of newly identified and previously known mobile malware in H1 2025 (Source: Recorded Future)

Several interrelated factors likely explain the continued expansion of the mobile threat landscape. The [increased adoption](#) of [mobile devices](#) for mobile banking and in corporate environments offers financially motivated threat actors an even larger attack surface. Particularly attractive is the [prevalence](#) of vulnerable mobile devices powered by outdated operating systems that lack the latest security patches.

The return of Predator was likely [sustained](#) by continued commercial demand despite international scrutiny. Similarly, Graphite was [detected](#) on devices belonging to European journalists, [indicating](#) ongoing misuse in targeted surveillance. Lastly, new [detections](#) of LightSpy, a spyware [linked](#) to

Chinese state-sponsored surveillance in Hong Kong, almost certainly indicate sustained regional espionage efforts against mobile users.

Threat Actors Favor Fake Downloads, Abuse Official Stores, and Exploit Supply Chains

Threat actors consistently relied on long-established TTPs to deliver mobile malware, primarily combining social engineering tactics like smishing and vishing, with fake downloads and brand impersonation to lure victims into installing malicious APKs. Campaigns often featured phishing pages and malware payloads mimicking [popular browsers](#), [cryptocurrency platforms](#), [financial apps](#), [streaming services](#), and [official app stores](#). In more targeted cases, attackers tailored lures to specific victims, as exemplified by Android.Spy.1292.origin, which [targeted](#) Russian military personnel by impersonating Alpine Quest Pro, a GPS and topographic mapping app reportedly used by both civilians and Russian military personnel.

Threat actors also employed less common but effective distribution methods, including abusing Google Play to deliver malware. While increasingly [robust](#) security measures have made delivering malware through official app stores more difficult, adversaries continued to find workarounds. SpyLend, for example, [posed](#) as “Finance Simplified” and evaded detection by offloading the malicious payload via external download links. Additionally, in a rare supply-chain compromise, a new variant of the Triada RAT was [discovered](#) pre-installed on counterfeit Android devices sold via unauthorized retailers.

Accessibility Service Abuse With a Twist

Once installed, Android-targeting malware frequently abused the brand’s Accessibility services, a [long-standing](#) TTP that grants broad control over infected devices. Android malware [abused](#) the functionality to [steal sensitive information](#) through overlay attacks, intercept text messages and push notifications, perform keylogging, screen and audio recording, and OCR-based image scanning, and ultimately take over the device to facilitate so-called “on-device fraud.”

The Android trojan GodFather stood out during the reporting timeframe for introducing a new overlay technique. While still abusing Android’s Accessibility services, a new iteration of GodFather [identified](#) in June 2025 was observed employing a virtualization-based overlay technique that combined open-source hooking frameworks such as Xposed with sandboxed app environments. This approach differs from traditional overlay attacks by using VirtualApp to create a virtualized environment that runs cloned banking apps without installing or modifying them on the device, effectively bypassing standard overlay detection mechanisms.

Threats to Contactless Payments Continue to Rise

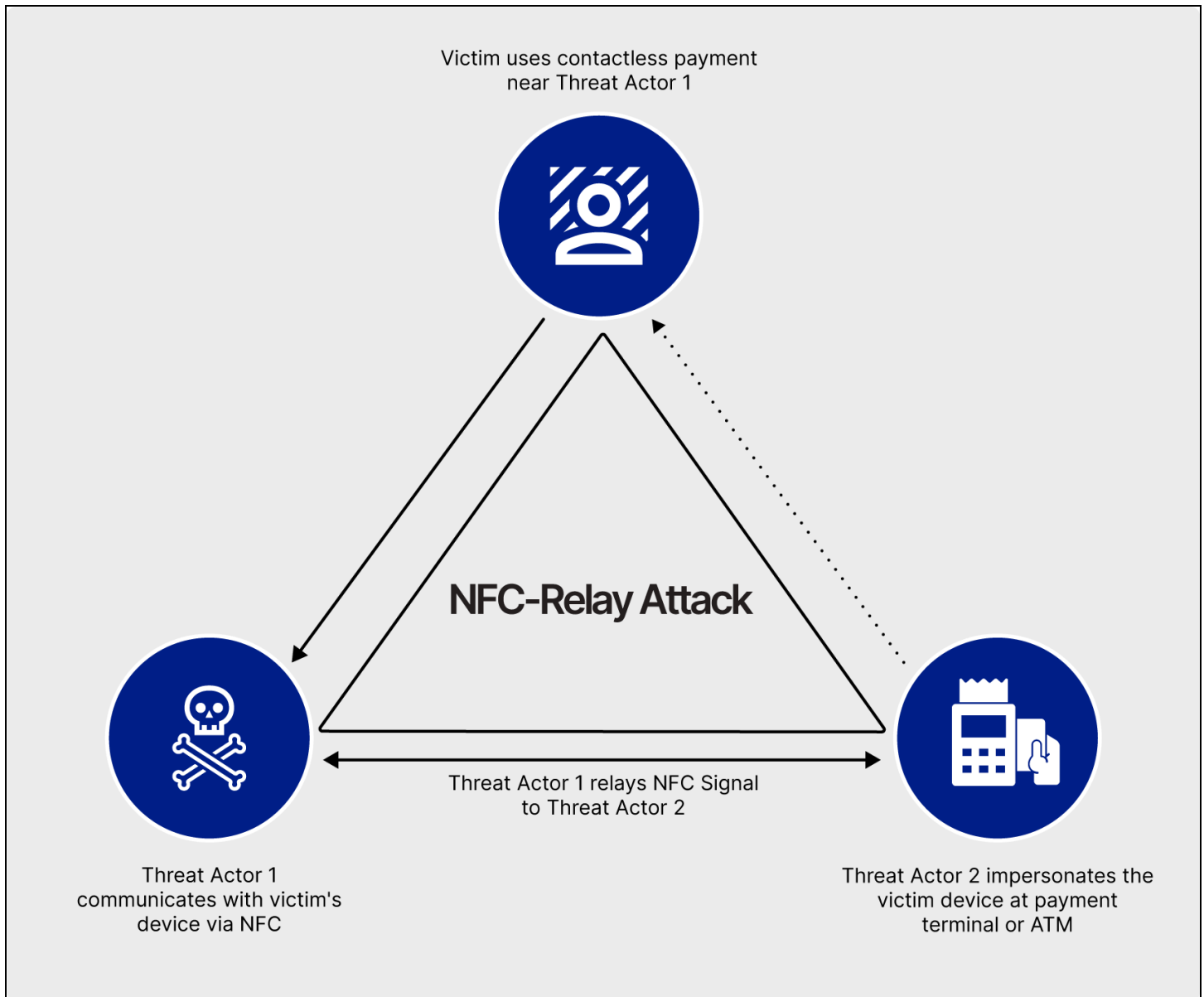


Figure 13: Illustration of NFC-relay attack flow (Source: Recorded Future)

In the first half of 2025, mobile malware posed a growing threat to contactless payment systems, exemplified by the [emergence](#) of SuperCard X, a Chinese-language MaaS platform targeting Android devices. The malware enables threat actors to conduct NFC relay fraud by tricking victims into tapping their contactless cards against compromised phones. Once a card is tapped, SuperCard X captures the NFC signal and relays it to a remote device controlled by the attacker, facilitating fraudulent transactions or ATM withdrawals. Its functionality closely mirrors that of NFCGate, an open-source tool [developed](#) in 2020, and shares similarities with NGate, an Android malware [linked](#) to NFC-based attacks in the Czech Republic during 2024, indicating likely code reuse or conceptual overlap.

Notably, the use of NFCGate-style techniques in real-world attacks has grown steadily. In January 2025, Russian cybersecurity firm F6 [reported](#) more than 100 such NFC relay attacks during 2024, with estimated losses of approximately \$400,000. In a follow-up report from April 2025, F6 [documented](#) an additional 40 successful NFCGate-based attacks, with an average loss of approximately \$1,500.

Ransomware

Ransomware Groups Innovate to Attract Affiliates Amid a Reshaped Landscape

In the first half of 2025, the ransomware landscape continued to evolve, [witnessing](#) the return of CL0P after a relatively quiet 2024, with its Cleo managed file transfer (MFT) data theft campaign. This campaign potentially affected over 300 organizations globally, according to Recorded Future ransomware victim data. Alongside the continued activity of groups like Akira and Play, several lesser-known and emerging ransomware groups gained traction, likely reflecting the lingering vacuum and uncertainty that resulted from LockBit's infrastructure [takedown](#) and ALPHV's [exit scam](#) in early 2024.

Two additional events further reshaped the ransomware landscape in early 2025. These were the demise of BlackBasta in early February, which followed a [leak](#) of internal chat logs, and the abrupt [disbandment](#) of RansomHub in late March, which left victims mid-negotiation and affiliates in disarray. Insikt Group assesses that BlackBasta members likely migrated to other operations, including Akira, with whom the group had prior connections. Group-IB also [assessed](#) that some RansomHub affiliates may have joined Qilin, a ransomware-as-a-service (RaaS) group active since July 2022, citing a spike in victim claims, internal restructuring, and increased activity on cybercriminal forums like RAMP. Meanwhile, DragonForce, a ransomware group [active](#) since at least late 2023, [claimed](#) to have absorbed RansomHub's infrastructure and affiliates, potentially as a result of a [hostile takeover](#). DragonForce is not averse to such aggressive tactics; the group was [identified](#) as a potential culprit behind the May 7, 2025, defacement of LockBit's affiliate administrative panels and leak of affiliates' information, and the April 5, 2025, [defacement](#) of Everest's extortion blog.

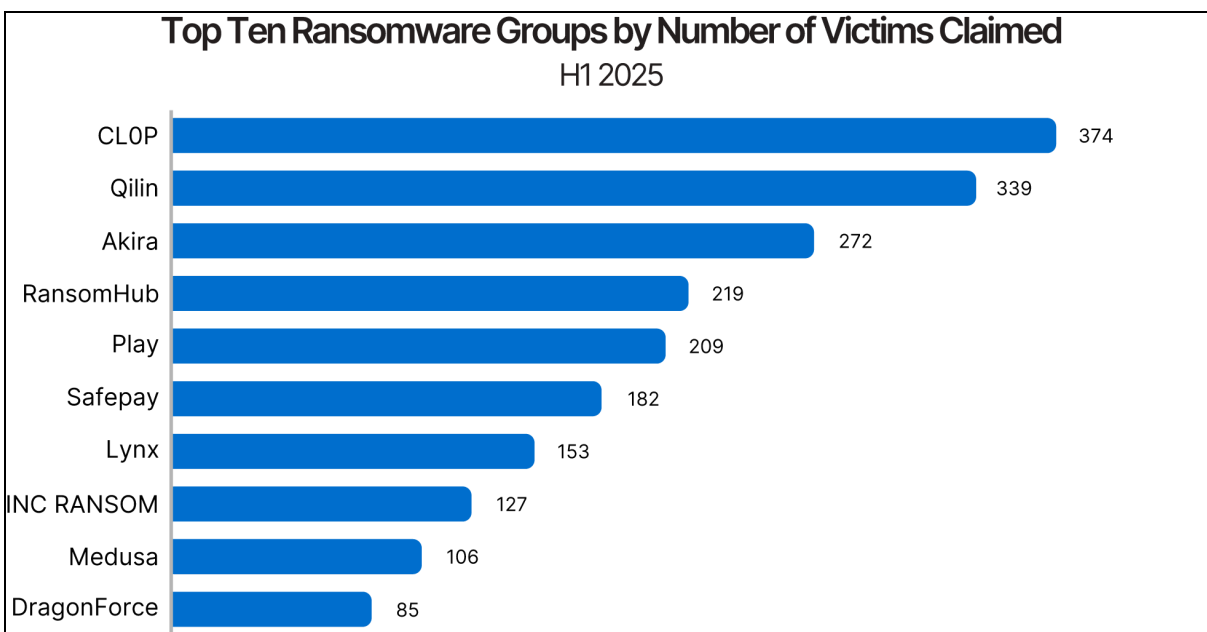


Figure 14: Top ten ransomware groups by number of victims claimed in H1 2025 (Source: Recorded Future)

To gain notoriety in this ever-evolving ransomware landscape, attract affiliates, and scale operations, ransomware threat actors modified their business models. In mid-March 2025, DragonForce [rebranded](#) as a “cartel”, launching a more flexible affiliate model and targeting other ransomware groups. Under the new model, affiliates can [use](#) DragonForce’s infrastructure and ransomware tools while operating under independent brands. DragonForce also [signaled](#) an openness to partner with or absorb other threat actors rather than just individual affiliates. For example, threat actors employing TTPs associated with Scattered Spider, a financially motivated cybercrime collective, reportedly [breached](#) a UK retail company and deployed DragonForce ransomware. The “cartel” approach effectively differentiates DragonForce from other RaaS offerings and is likely to appeal to a range of threat actors, broadening the group’s affiliate base and increasing potential revenue. However, it does not solve issues that have [plagued](#) other, more established RaaS operations. The shared infrastructure continues to introduce an element of risk: if an affiliate is compromised, other affiliates’ operational and victim details could also be exposed.

Anubis, a ransomware operation first [observed](#) in December 2024, used a different tactic to entice affiliates. In late February 2025, the group [debuted](#) an affiliate model that features three modes. The first is a traditional RaaS model in which Anubis provides a ransomware payload and affiliates perceive 80% of any extorted ransom. The second is a data ransom model in which Anubis helps affiliates monetize sensitive data they have already stolen from target companies. The third model allows affiliates to provide Anubis operators with initial access to corporate networks in return for 50% of any extorted ransom.

Lastly, in mid-June 2025, Qilin [introduced](#) a new function dubbed “Call Lawyer,” offering affiliates legal consultation on how to intimidate victims during the negotiation phase.

New Initial Access, Defense Evasion, and Malware Deployment Techniques

Parallel to changes in the broader ransomware landscape and RaaS offerings, Insikt Group observed ransomware threat actors adopt new TTPs across multiple phases of the attack chain, including initial access, defense evasion, and payload deployment.

- **Initial Access:** According to Sekoia, Interlock ransomware [used](#) ClickFix in social engineering attacks impersonating IT tools between January and February 2025. As mentioned in the **Malware TTP Trends and Insights** section of this report, ClickFix is a social engineering method that uses fake error messages or verification prompts to deceive victims into executing malicious scripts, either manually or via automatic clipboard manipulation.
- **Defense Evasion:** Per Palo Alto's Unit42 and ESET, ransomware threat actors are [increasingly using](#) "EDR killers," tools designed to terminate defensive software, further confirming a trend that has been [ongoing](#) since 2022. Notably, ransomware threat actors are also employing new "bring-your-own-installer" (BYOI) techniques to disable EDR altogether. As reported by Aon, a Babuk ransomware intrusion saw the attacker [exploiting](#) a flaw in SentinelOne's upgrade/downgrade process to bypass its anti-tamper protections without needing the management console code. By running a legitimate installer for a different version and terminating the `msiexec.exe` process mid-upgrade, the attacker left the system without active EDR protection. This created a window in which Babuk ransomware could be executed on an unprotected endpoint. The bypass was confirmed to work across multiple SentinelOne versions unless the "Online Authorization" setting was enabled.
- **Payload Deployment:** Trend Micro [reported](#) that Qilin ransomware attacks used a custom and heavily obfuscated .NET-based loader dubbed NETXLOADER to deliver ransomware payloads and SmokeLoader in memory. NETXLOADER is protected by .NET Reactor. It stealthily decrypts and directly injects payloads into memory using dynamic API calls and JIT hooking to evade detection.

Additionally, ransomware threat actors employed uncommon and legitimate software tools during their intrusion, almost certainly to collect data, achieve persistence, and move laterally, while avoiding detection. For example, in mid-June 2025, Symantec [reported](#) that a May 2025 Fog ransomware attack targeting a financial institution in Asia involved dual-use and open-source penetration testing tools not typically associated with ransomware operations. These included the following:

- **Syteca:** A legitimate employee monitoring software with keylogging and screen capture capabilities, which Fog operators likely used for espionage and credential theft, followed by cleanup actions to evade detection
- **GC2:** An open-source C2 framework that uses Google Sheets or SharePoint for command execution and file exfiltration, which Fog operators likely used for remote access, persistence, and defense evasion via cloud-based communications

- **Adaptix:** An open-source post-exploitation agent similar to Cobalt Strike, which Fog operators likely used for remote access and internal lateral movement through encrypted C2
- **Stowaway:** An open-source proxy tool for creating covert communication tunnels between compromised hosts and operators, which Fog operators likely used to evade defenses by proxying communications and delivering Syteca

This pattern was not unique to Fog ransomware. A July 2025 CISA report [detailed](#) Interlock ransomware campaigns that likewise repurposed legitimate tools to evade detection and maintain access. Threat actors installed AnyDesk, a remote monitoring and management application, to preserve access and facilitate file transfers, and used PuTTY, a widely used SSH client, to establish tunnels for covert communications and pivot between compromised systems.

Incorporating commercially available and dual-use software into their intrusion workflows, ransomware threat actors can blend in with routine administrative activity, making malicious actions less likely to trigger security alerts. This continued adoption of legitimate or dual-use software by ransomware actors underscores a broader trend toward intrusion methods designed to evade detection while enabling adaptable, multi-purpose operations inside victim networks.

Magecart Infections Remained High in H1 2025

In the first half of 2025, Magecart e-skimming continued to threaten online merchants at scale. Infection volumes remained near the record highs seen in late 2024, albeit with a slight decline from the peak. Thousands of e-commerce domains were impacted in H1 2025, keeping Magecart a widespread concern for payment security. This sustained activity follows an unprecedented [spike](#) in Magecart incidents during 2024, when the number of affected e-commerce domains roughly tripled compared to 2023. That surge was largely driven by the [exploitation](#) of a critical Adobe Commerce (Magento) vulnerability dubbed CosmicSting (CVE-2024-34102), which enabled mass compromise of merchant websites. Organized threat groups also amplified the outbreak; for example, one Magecart group (known as “Burunduki”) alone infected over 200 online stores globally in late 2024. By early 2025, patches and defensive measures began curbing the CosmicSting-fueled wave, but overall Magecart infection rates remained significantly elevated above early 2024 levels.

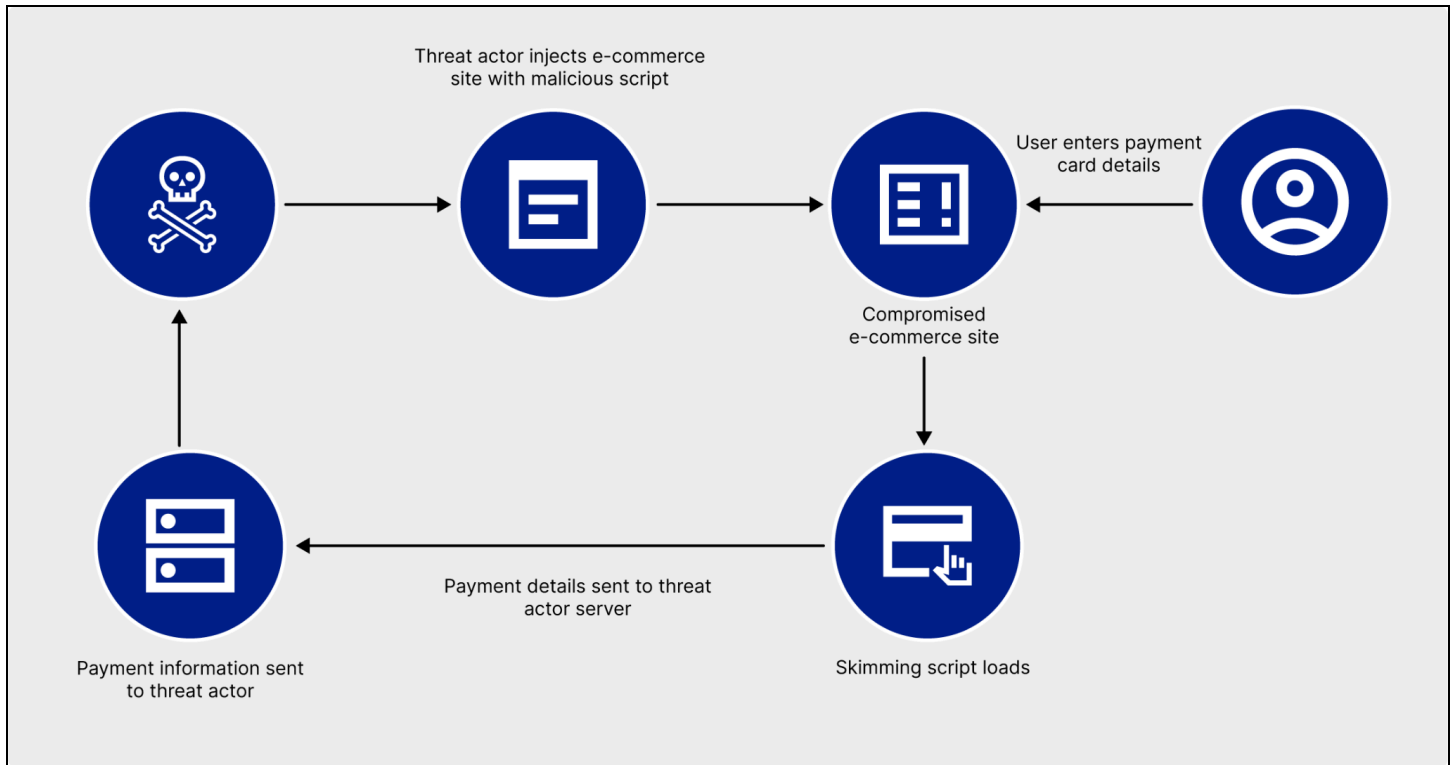


Figure 15: Illustration of Magecart skimming attack flow (Source: Recorded Future)

Magecart operators in H1 2025 continued to leverage malware kits and tactics introduced in the prior year, while also expanding into new platforms. Out-of-the-box e-skimmer kits such as “Sniffer by Fleras”, first [observed](#) in 2024, remained active in compromises of online stores. Meanwhile, attackers broadened their focus beyond Magento; notably, Magecart skimmers extended to WordPress-based retail sites by [exploiting](#) WooCommerce plugins. These campaigns underline how Magecart techniques have widened in scope, targeting a broader range of e-commerce platforms rather than just traditional Magento stores.

Finally, Magecart skimming techniques continued to evolve in H1 2025. Threat actors experimented with more covert loading methods to evade detection. In one example, attackers [used](#) a modular chain of Google Tag Manager (GTM) containers, where one container loaded a fake CSS file that embedded JavaScript within a `::before` content property. A second GTM container then extracted and executed this hidden code by targeting a specific `<link>` element in the Document Object Model (DOM), initiating a WebSocket connection for real-time data exfiltration. These technical refinements underscore the adaptability of Magecart operations and the ongoing need for vigilant web security measures.

Mitigations

Organizations can use the following measures to mitigate the threats discussed in this report.

Vulnerability Exploitation

- **Recorded Future Vulnerability Intelligence:** Recorded Future customers can use [Vulnerability Intelligence](#) to gain timely and comprehensive insights into publicly and privately known vulnerabilities tailored to specific security needs that can help prioritize remediation measures. With Vulnerability Intelligence, customers also gain access to Nuclei templates created by Insikt Group, enabling proactive scanning and rapid detection of emerging vulnerabilities.
- **Recorded Future Attack Surface Intelligence:** Recorded Future customers can use external [Attack Surface Intelligence](#) to maintain real-time visibility into network assets, prioritize exposures to remediate, and enforce security controls.
- **Asset and Exposure Inventory:** Conduct regular inventories of all internet-facing hosts, including remote access appliances, edge devices, and third-party software. Prioritize monitoring gateway-layer products (such as SSL-VPNs, firewalls, and virtualization underlays), which were frequently exploited in H1 2025. Run scheduled scans to identify shadow IT assets and newly exposed services to fill critical security gaps.
- **Agile Patch Management:** Develop and enforce rapid patch deployment workflows for vulnerabilities with known public PoCs or active exploitation. Prioritize vulnerabilities that are remotely exploitable, require no authentication, or affect widely deployed software (such as Microsoft, Ivanti, or Fortinet). When immediate patching is not possible, apply mitigation controls (such as WAF rules or IPS signatures) and restrict access to the affected service.
- **Harden Internet-Facing and Security Appliances:** Enforce multi-factor authentication on all administrative interfaces and disable unused or legacy services (such as insecure SSH or Telnet). Segregate edge-device management networks from production networks, and restrict the internal subnets a compromised VPN or firewall can reach.

Malware Intrusions

- **Recorded Future Hunting Packages:** Recorded Future customers can implement Hunting Packages developed by Insikt Group to monitor for intrusions associated with prominent malware families.
- **EDR, Heuristic, and Behavior-Based Analysis:** Implement heuristic and behavior-based analysis through EDR solutions to detect and respond to threat actor TTPs, such as JIT hooking, protected payloads, and memory injection. Ensure that EDR tools are not only deployed but also

actively monitored and updated.

- **Application Allowlisting and Script Control:** Enforce strict application allowlisting and execution control policies to prevent unauthorized script executions.
- **Employee Education:** Educate employees on the latest delivery and execution techniques prominent malware use to spread, such as new or updated social engineering lures like ClickFix.

Magecart Attacks

- **Recorded Future Payment Fraud Intelligence:** Recorded Future customers can use [Payment Fraud Intelligence](#) to monitor ongoing Magecart e-skimmer infections, stay current with the latest Magecart TTPs, enhance prevention strategies, and take action on compromised cards before fraud occurs.
- **Regular Security Audits and Vulnerability Scanning:** Conduct security audits and automated vulnerability scans regularly to identify and remediate vulnerabilities affecting the technologies underpinning e-commerce websites.
- **Content Security Policy (CSP):** Deploy and update a strict CSP to control resources loaded on e-commerce websites and prevent the execution of unauthorized scripts.
- **Third-Party Integrations Monitoring:** Frequently audit and secure all third-party scripts and integrations used on e-commerce websites. Monitor and restrict access to these integrations to prevent unauthorized modifications.
- **Enforce PCI DSS 4.0 Requirements 6.4.3 and 11.6.1:** As of March 31, 2025, requirements 6.4.3 and 11.6.1 are now mandatory for organizations handling payment card data. These provisions require a documented inventory of all payment-page scripts, explicit authorization and business justification for each script, integrity monitoring, and real-time change detection with alerts for unauthorized modifications.

Outlook

In the remainder of 2025, Insikt Group assesses that exploitation of edge-security appliances, remote access tools, and other gateway-layer software will almost certainly remain a top priority for both state-sponsored and financially motivated threat actors. The strategic value of these systems — acting as intermediaries for encrypted traffic and privileged access — makes them high-reward targets. As seen in H1 2025, vulnerabilities in products from Microsoft, Fortinet, Ivanti, and others continue to be exploited even after public disclosure, particularly when PoC code becomes available. Insikt Group expects this trend to accelerate, especially given the growing lag between vulnerability disclosure and patch implementation across enterprises.

Given its steep adoption curve, Insikt Group assesses that ClickFix will almost certainly remain a favored initial access technique through the rest of 2025. Unless widespread mitigations or awareness campaigns reduce its effectiveness, the technique's ease of deployment and efficacy will likely sustain its prevalence in the near term.

Malware development is also expected to continue along two concurrent paths: the repurposing of legacy code and the refinement of stealth techniques. The resurgence of Salty and Tofsee, alongside more advanced loaders and evasive delivery mechanisms like JIT hooking, suggests that actors will continue blending old tools with modern obfuscation to defeat signature-based defenses. Insikt Group anticipates that commodity RATs will remain prominent due to their accessibility and versatility for persistent access and data theft.

Mobile malware will likely play an increasingly important role in cybercriminal operations, particularly with the growth of contactless payment fraud and virtualization-based evasion techniques. Threat actors will almost certainly continue targeting mobile banking and NFC technologies, leveraging both fake app distribution and supply-chain compromises to infect devices at scale.

In the ransomware ecosystem, Insikt Group expects to see continued experimentation with business models and affiliate structures. "Cartel"-style approaches, such as those introduced by DragonForce, alongside flexible affiliate tiers and services like legal intimidation support, are likely to gain traction as groups seek differentiation and resilience in a post-LockBit landscape. Parallel innovation in defense evasion and deployment, including BYOI exploits and password-protected payloads, will likely persist as defenders improve endpoint and network monitoring.

Magecart activity is expected to remain steady or increase in sophistication through the end of 2025. With e-commerce remaining a lucrative target, threat actors will likely adopt even more modular and covert skimming methods, abusing legitimate services like Google Tag Manager or exploiting under-patched plugins across platforms like WooCommerce. Continued abuse of obscure HTML tags, CSS properties, and obfuscated JavaScript delivery mechanisms is likely as attackers aim to bypass increasingly strict content security policies.

Overall, the H1 2025 trends suggest that defenders must prepare for a hybrid threat environment in which aging malware resurfaces alongside cutting-edge delivery chains and mobile platforms and edge systems become focal points of exploitation. Cross-platform visibility, tighter app and gateway security, and proactive intelligence integration will be critical to managing these evolving risks through the second half of the year.

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

About Insikt Group®

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

About Recorded Future®

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

Learn more at recordedfuture.com