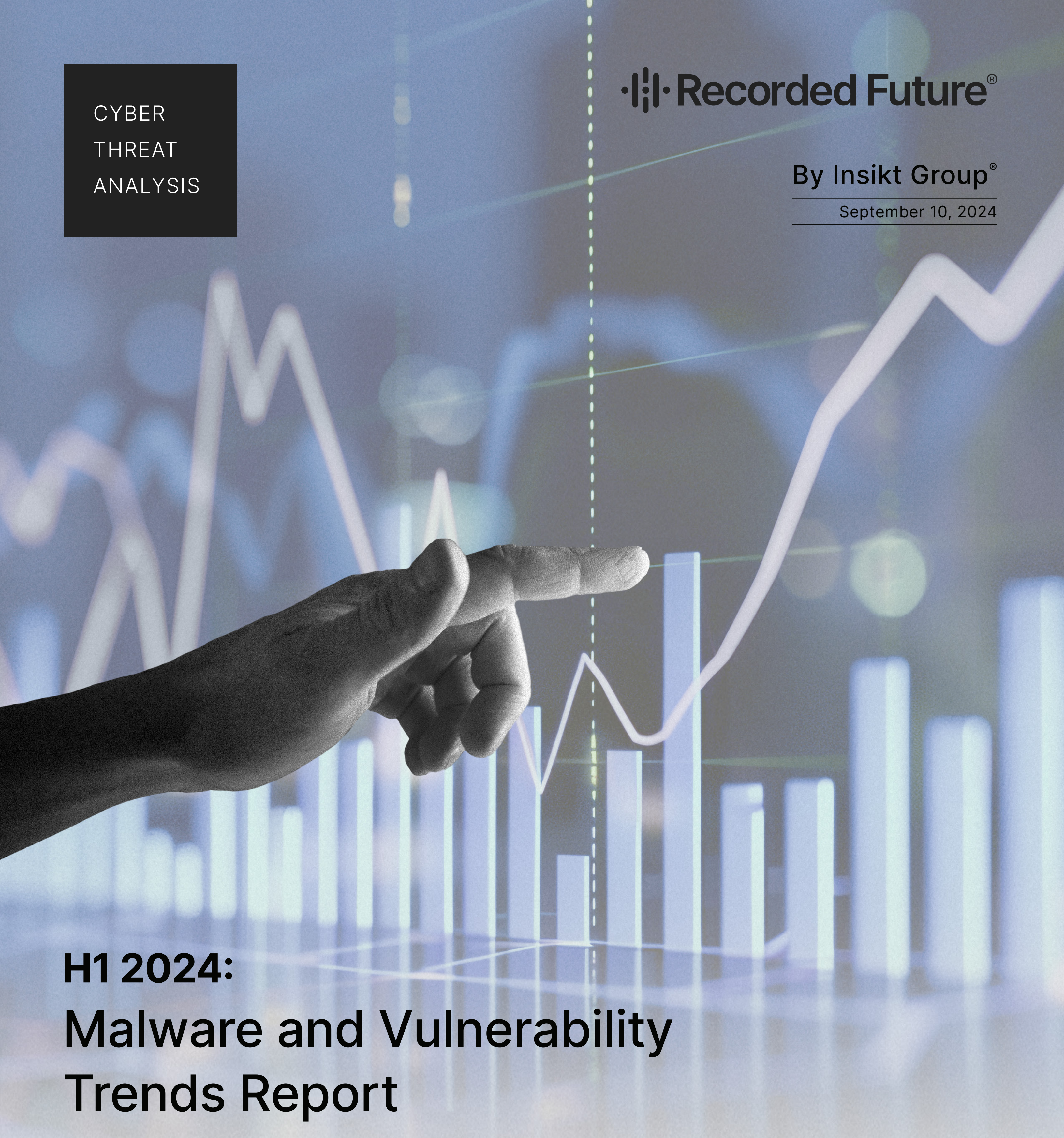


CYBER THREAT ANALYSIS

Recorded Future®

By Insikt Group®

September 10, 2024

H1 2024: Malware and Vulnerability Trends Report

Vulnerabilities affecting widely used remote access and security software, such as Ivanti Secure Connect, Palo Alto Networks PAN-OS, and Microsoft Windows SmartScreen, were the most exploited in the first half of 2024.

Infostealers dominated the malware landscape in the first half of 2024, with LummaC2 being the most prevalent strain. Insikt Group also observed a 103% increase in Magecart infections since the second half of 2023.

Fog, Raspberry Robin, and SocGholish malware operators, among others, updated existing tools and introduced new techniques to their ransomware, trojans, infostealers, and malware loaders to increase the chances of evading detection and impeding analysis.

Executive Summary

The malware and vulnerability exploitation landscape in the first half of 2024 (H1 2024) largely saw threat actors refining known tactics, techniques, and procedures (TTPs) and experimenting with new ones to disrupt and circumvent the defenses enterprises rely on.

We observed the prolonged exploitation of newly disclosed vulnerabilities (zero-days) affecting remote access and security solutions even after patches became available (at which point the vulnerabilities became n-days). Threat actors also updated their malware capabilities and refined their delivery mechanisms to evade detection and hinder analysis, such as ransomware operators requiring passwords for malware to run on victim systems. Overall, information stealing (infostealer) malware dominated the malware landscape, and Magecart attacks, whereby threat actors compromise e-commerce websites with malicious code designed to steal customers' personal and financial information, increased by approximately 103% in the first six months of 2024.

Taken together, zero-day vulnerability exploitation and new malware TTPs to prevent detection and analysis heighten threats for organizations because both factors lower defenders' ability to detect malicious activity in a timely manner. As a result, threat actors can gain more time to act on their objectives, increasing the likelihood of more severe harm to targeted organizations.

To address the threat trends of H1 2024, a layered defense and proactive monitoring are essential. Enhancing patch management procedures, particularly for highly targeted software like remote access and security tools, helps counter n-day vulnerabilities. Minimizing permissions and promptly detecting abnormal behavior, on the other hand, can help manage zero-day exploits. Companies should also familiarize themselves with prominent infostealers and e-skimmers and adapt security controls to their respective delivery methods, such as phishing and the exploitation of vulnerabilities in e-commerce platforms. In the long term, investing in threat intelligence can help security teams remain aware of and capable of responding to the latest TTPs.

Key Findings

- The five most-referenced vulnerabilities in our dataset in H1 2024 were three vulnerabilities affecting Ivanti Secure Connect, a vulnerability in PAN-OS, and a vulnerability in Microsoft Windows SmartScreen.

- These vulnerabilities were initially exploited as zero-days by state-sponsored actors, with targeting by cybercriminals persisting after the release of patches, almost certainly fueled by the availability of proof-of-concept (PoC) exploit code.

- Infostealers remained the dominant malware category in the first half of 2024. LummaC2 was the most prevalent of this type of malware, based on Recorded Future's Malware Intelligence data.

- Updates to ransomware, trojans, infostealers, and malware loaders focused on hindering analysis and evading detection through H1 2024, by updating existing TTPs and introducing new ones.

- The operators of Fog, RansomHub, and 3AM, three relatively new ransomware strains, adopted passwords as a means to validate their payload's execution and avoid analysis by sandbox and other security solutions.

- Malware like Raspberry Robin, SocGholish, and HijackLoader implemented new anti-emulation, execution, and process hollowing techniques. ClearFake, RedLine, and Coyote experimented with new delivery techniques featuring the use of less-popular programming languages and software tools.

- Magecart infections increased by approximately 103% between H2 2023 and H1 2024, based on statistics from Recorded Future's Payment Fraud Intelligence module. We assess that factors like the exploitation of a newly discovered vulnerability in Adobe Commerce (CVE-2024-20720), and the debut of a new Magecart skimmer dubbed "Sniffer By Fleras" were partially responsible for the upward trend.

Vulnerability Exploitation Trends

The first half of 2024 was dominated by the exploitation of five vulnerabilities affecting widely adopted security and remote access software. These were three vulnerabilities affecting Ivanti Secure Connect (formerly Pulse Secure), one vulnerability affecting Palo Alto Networks PAN-OS, and one vulnerability affecting Microsoft Windows SmartScreen. Additional information on each of these vulnerabilities is provided in **Table 1** below.

Vulnerability	Affected Product	Recorded Future Risk Score	CVSS v3	Summary
CVE-2024-21887	Ivanti Connect Secure	89	9.1	A command injection vulnerability in web components of Ivanti Connect Secure (9.x, 22.x) and Ivanti Policy Secure (9.x, 22.x); if exploited, it allows an authenticated administrator to send specially crafted requests and execute arbitrary commands
CVE-2023-46805	Ivanti Connect Secure	89	8.2	An authentication bypass vulnerability in the web component of Ivanti ICS (9.x, 22.x) and Ivanti Policy Secure; if exploited, it allows a remote attacker to access restricted resources by bypassing control checks
CVE-2024-21893	Ivanti Connect Secure	89	8.2	A server-side request forgery vulnerability in the SAML component of Ivanti Connect Secure (9.x, 22.x), Ivanti Policy Secure (9.x, 22.x), and Ivanti Neurons for ZTA; if exploited, it allows an attacker to access certain restricted resources without authentication
CVE-2024-3400	Palo Alto Networks PAN-OS	89	10	A command injection vulnerability in the GlobalProtect feature of specific PAN-OS versions and distinct feature configurations; if exploited, it can enable an unauthenticated attacker to execute arbitrary code with root privileges on the firewall
CVE-2024-21412	Microsoft Windows SmartScreen	99	8.1	A security bypass vulnerability in Microsoft Windows SmartScreen arising from an error in handling maliciously crafted files; if exploited, it allows a remote attacker to bypass the SmartScreen security warning dialog and deliver malware

***Table 1**: Summaries of the top five vulnerabilities associated with exploitation activity in H1 2024, based on Recorded Future data (Source: Recorded Future)*

CVE-2024-3400, the vulnerability affecting PAN-OS, had the most references to cyberattack and cyber exploitation activity in the Recorded Future Intelligence Cloud in H1 2024 (**Figure 1**). Two threat actors were reported exploiting it (TAG-100 and UTA0218), with additional exploitation activity distributing RedTail. However, the three vulnerabilities affecting Ivanti Connect Secure had the most references when combined. Furthermore, they were exploited by the highest number of individual threat actors (both cybercriminals and state-sponsored) according to Insikt Group and third-party reporting, with individual malicious entities chaining two or three of them in their operations.

Per Mandiant reporting, China-nexus threat actors UNC5325 and UNC5221 exploited both CVE-2024-21893 and CVE-2024-21887 as zero-days since December 2023 in likely espionage operations involving web shells like BUSHWALK, THINSPOOL, LIGHTWIRE, and other malware [1, 2]. Volexity tracked the same campaign, attributing it to a suspected Chinese state-sponsored group dubbed UTA0178.

Similarly, the cybercriminal threat actor Magnet Goblin exploited all three Ivanti Connect Secure vulnerabilities during the first half of 2024, incorporating exploit code only one day after the code was publicly disclosed online [1, 2]. Magnet Goblin targeted exposed Ivanti Connect Secure VPN instances to deliver a bundle of malware that included a new Linux version of NerbianRAT, a JavaScript credential stealer called WARPWIRE, and Ligolo, an open-source tunneling tool written in Go.

Other exploitations of the Ivanti Connect Secure vulnerabilities involved cybercriminal operations distributing botnets like Skibidi and Mirai, the cryptominer RedTail, and potential state-sponsored activity involving the backdoors ArcSilt and DSLog [1, 2, 3, 4].

As for CVE-2024-21412, exploitation activity involving the vulnerability was attributed to DarkCasino, a cybercriminal group; the operators of DarkGate, a commodity loader; and cybercriminal operations distributing Phemedrone, an infostealer.

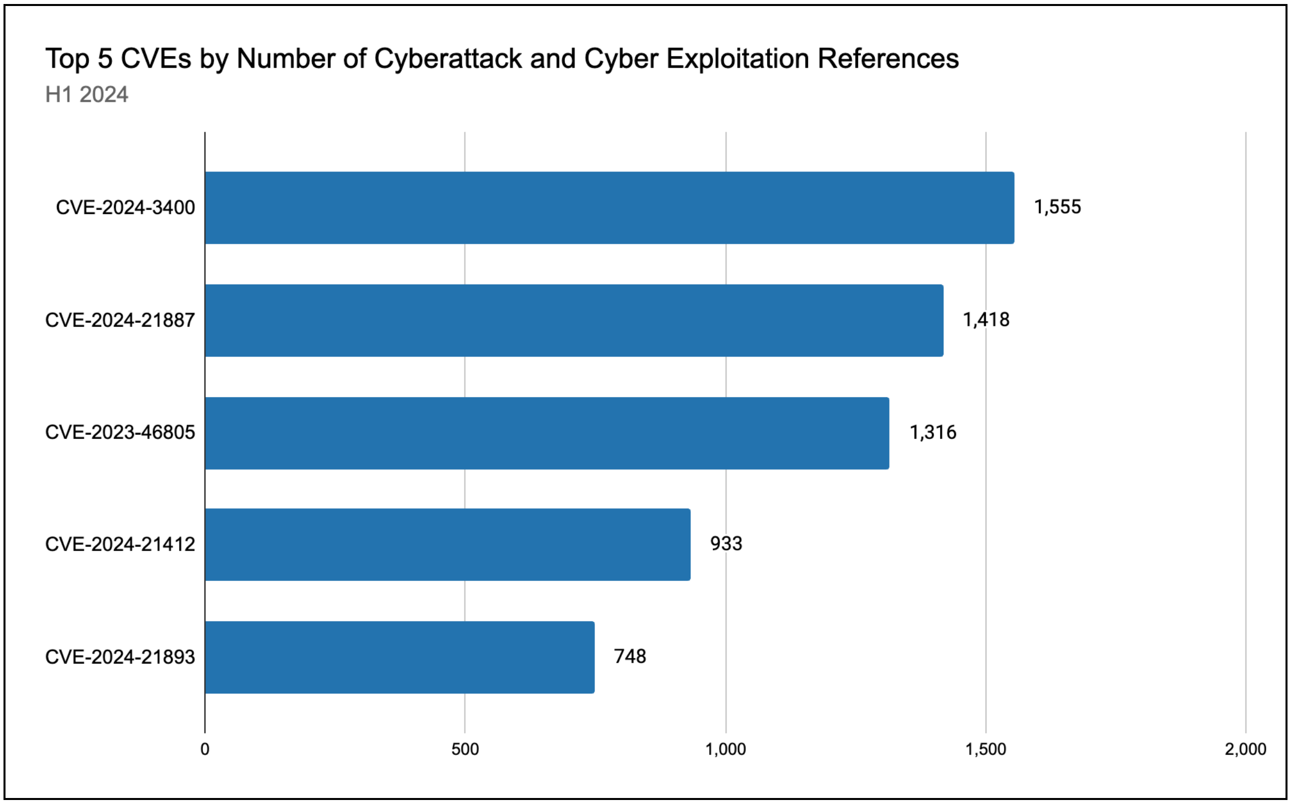


***Figure 1**: The top five vulnerabilities by cyberattack and cyber exploitation references, H1 2024 (Source: Recorded Future)*

Several factors almost certainly contributed to the five vulnerabilities' popularity among threat actors. These include ease of exploitation, the availability of exploit code, and the wide adoption of the software affected:

- **Ease of Exploitation**: All five vulnerabilities are characterized by a low attack complexity — they require no particular privileges to be exploited, based on the US National Vulnerability Database (NVD) and other vendors' data. As an example, Volexity reported that CVE-2023-46805 and CVE-2024-21887 make it "trivial" for attackers to run commands on targeted systems when chained together.

- **Availability of Proof-of-Concept (PoC) Exploit Code**: PoC exploit code became available for all five vulnerabilities after their disclosure and evidence of zero-day exploitation [1, 2, 3, 4, 5, 6]. This significantly lowered entry barriers, allowing less-sophisticated threat actors to probe for and target vulnerable instances. A notable example is Magnet Goblin, as mentioned above. We also identified chatter involving the five vulnerabilities and PoC exploit code on various underground and dark web forums and on messaging platforms.

- **Ubiquity of Affected Products**: Ivanti Secure Connect, PAN-OS, and Microsoft Windows SmartScreen are widely adopted, providing threat actors with thousands of potential targets to compromise. Ivanti reports that over 40,000 customers, including 96 of the Fortune 100, use its products, and we were able to identify over 21,000 Ivanti Secure Connect hosts running on the internet using Censys. PAN-OS powers Palo Alto Networks' next-generation firewalls (NGFWs), a product with a market share of 8.27% in the perimeter-security-and-firewalls market, according to 6Sense. Palo Alto itself reports that over 85,000 customers worldwide use its network security products. Microsoft Windows SmartScreen, meanwhile, is installed by default on supported versions of the Windows operating system. We also note that threat actors have already exploited vulnerabilities in Ivanti Secure Connect, PAN-OS, and SmartScreen in recent years [1, 2, 3].

Other vulnerabilities that saw significant references to cyberattack and cyber exploitation activity in H1 2024 affected SmartScreen and other products of a similar nature to Ivanti Connect Secure. We assess that this further highlights threat actors' preference for remote access and enterprise solutions, largely due to their ubiquitous nature and the level of access obtained once compromised. These additional vulnerabilities are as follows:

- CVE-2024-21762: A critical out-of-bounds write vulnerability affecting Fortinet FortiOS SSL VPN. On February 9, 2024, CISA added the vulnerability to its Known Exploited Vulnerabilities Catalog, based on evidence of active exploitation.

- CVE-2024-1709: A critical authentication bypass vulnerability affecting ConnectWise ScreenConnect, which threat actors exploited to deliver LockBit, BlackBasta, and Bl00Dy ransomware [1, 2].

- CVE-2024-4577: A critical vulnerability in PHP that threat actors exploited to deliver TellYouThePass ransomware, Gh0st RAT, and the RedTail and XMRig cryptominers [1, 2].

- CVE-2024-27198: A critical authentication bypass vulnerability affecting JetBrains TeamCity, which threat actors exploited to deliver Jasmin ransomware, XMRig, Cobalt Strike Beacons, and SparkRAT, and execute domain discovery and persistence commands.

- CVE-2023-36025: A high-severity feature bypass vulnerability in Windows SmartScreen Security, which threat actors exploited to deliver Mispadu, Phemedrone, and Darkgate [1, 2, 3].

Trends in vulnerability exploitation observed in the first half of 2024 partially align with Insikt Group observations in 2023. Although we did not witness a repetition of broad exploitation activity involving vulnerabilities in file transfer solutions (as was the case in H1 2023 with CL0P's GoAnywhere and MOVEit campaigns [1, 2]), threat actors continued to favor vulnerabilities in remote access solutions. As highlighted in Recorded Future's 2023 Annual Report, in the second half of 2023, both state-sponsored and ransomware groups exploited vulnerabilities in Citrix products and successfully compromised hundreds of organizations worldwide [1, 2, 3].

Malware Trends

The malware landscape in the first half of 2024 continued to be dominated by infostealers. More generally, malware authors introduced new techniques to hinder analysis and evade detection, such as tricking victims into executing malicious PowerShell code and combining process hollowing with process doppelgänging. We also observed an increase in Magecart intrusions, almost certainly driven by factors such as the exploitation of newly discovered vulnerabilities in e-commerce platforms and the debut of new e-skimmers.

Infostealers Dominate, Offensive Security Tools Climb in C2 Detections

References to command-and-control (C2) detections in the Recorded Future Intelligence Cloud underwent a notable transformation between H1 2023 and H1 2024 in terms of malware families (**Figure 2**). The Recorded Future Intelligence Cloud identifies C2 servers based on malware configurations extracted from samples submitted to Recorded Future Malware Intelligence.

Infostealers have remained the dominant malware category over the past year. This is consistent with the majority of threat actors being financially motivated, as threat actors can monetize stolen data, such as credit card information or cryptocurrency wallet credentials, by stealing funds directly from the victim or selling the data to other threat actors on dark web and underground markets. While some malware families driving this category have carried over from H1 2023 to H1 2024, like Vidar, RedLine, and LokiBot (Windows variant), some families have debuted in the top ten this year, such as the newly prominent RisePro. The most striking development is the ascent of LummaC2 to the top of the malware family rankings in H1 2024 after not being in the top ten in H1 2023. While this infostealer has been active since at least August 2022, Insikt Group recently discovered LummaC2 employing new TTPs. Specifically, LummaC2 has begun abusing the usernames of Steam Community profiles to distribute C2 server configurations, a behavior previously observed in Vidar campaigns. Simultaneously, the resurgence of Sality, a polymorphic botnet first observed in the wild in 2003, highlights the ongoing prevalence of legacy malware.

We also note RedLine's massive decline in references to C2 detections. We assess that this is due to ESET Research and GitHub's collaborative April 2023 disruption of RedLine operations. GitHub removed four repositories that broke authentication for panels currently in use by the malware. These panels acted as C2 servers that allowed for the generation of new samples and managed stolen information.

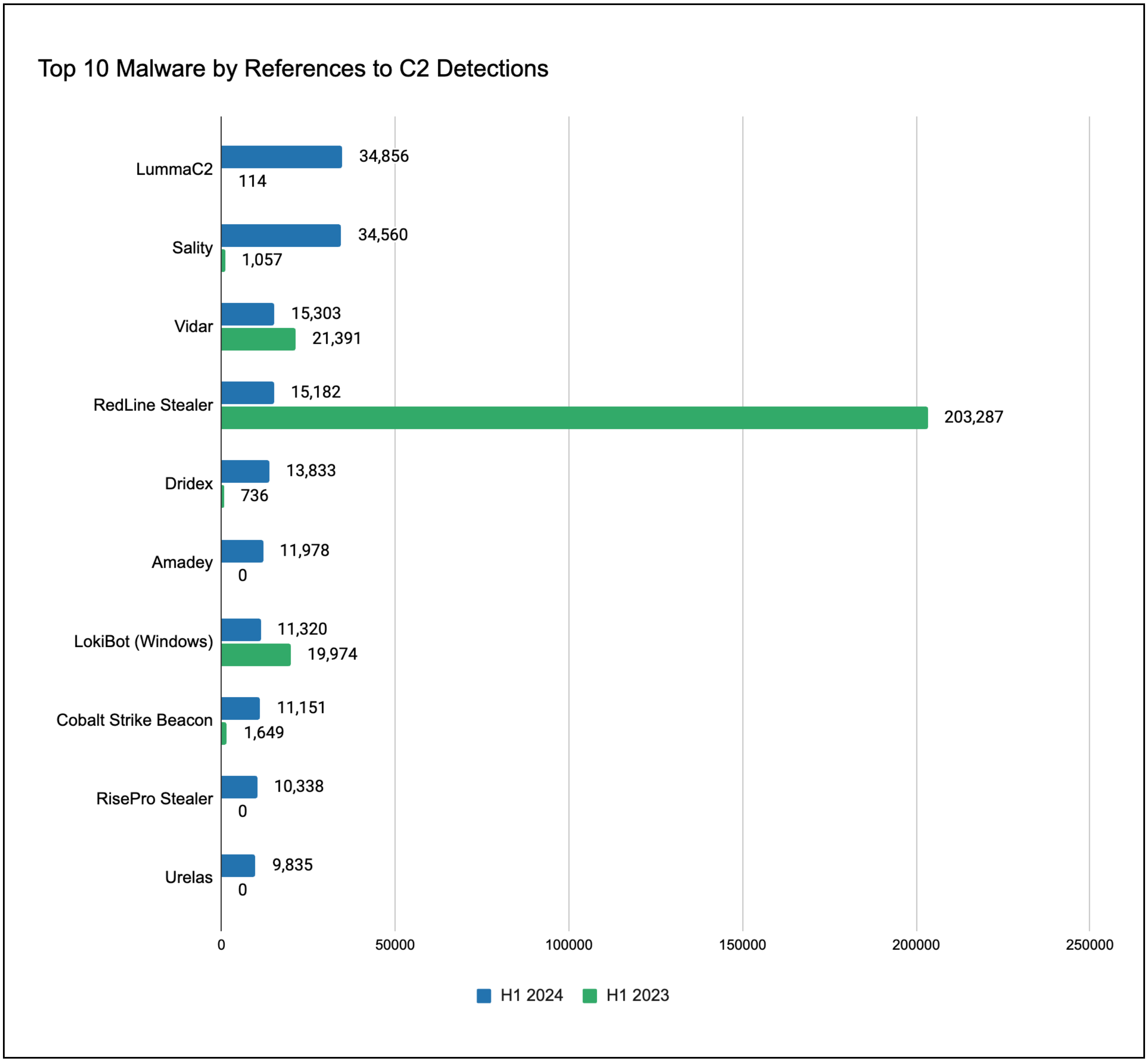


Figure 2*: The top ten malware families by number of references to C2 detections in H1 2024 and H1 2023 (Source: Recorded Future)*

Another emerging trend in these C2 detections is the increased presence of offensive security tools (OSTs), such as Cobalt Strike. While these tools are often legitimate penetration testing instruments, their misuse by malicious actors has become common, as evidenced by their involvement in recent cyberattacks. For example, in June 2024, Fortinet reported on a campaign using Excel files with embedded VBA macros to deliver Cobalt Strike Beacon payloads. We also regularly observe open-source tools designed to be used with the Cobalt Strike framework originally published on GitHub, such as OdinLdr, a custom tool for dynamic code loading, released in May 2024.

Ransomware Strains Focus on Hindering Analysis

The ransomware landscape witnessed a general reshuffling in the first half of 2024 following the departure of ALPHV and the disruption of LockBit's operation by an international law enforcement operation dubbed Cronos. Following these two events, existing and newer ransomware groups moved to fill in the void left by ALPHV and attract affiliates who were moving away from LockBit. Despite these changes, however, ransomware capabilities remained largely unchanged since the beginning of 2024.

One prominent feature we observed was the use of passwords to validate the execution of commands as an anti-analysis measure by three emerging ransomware: Fog, RansomHub, and 3AM. Using passwords for defensive purposes is not a new technique among ransomware groups. LockBit 3.0 has used passwords to hinder analysis since July 2022 and both ALPHV and Knight ransomware were also observed using this technique. That said, the use of passwords to hinder analysis by Fog, RansomHub, and 3AM speaks to the technique's ongoing popularity and effectiveness.

- Fog was first observed in early May 2024 [1, 2]. Static analysis of a Fog ransomware sample by Recorded Future indicated that it requires a password for execution.

- RansomHub surfaced in February 2024 and quickly rose in prominence as a multi-platform RaaS offering. Insikt Group's analysis of the ransomware revealed that RansomHub Windows, Linux, and ESXi versions require a `-pass` argument to be specified when the ransomware is run. The provided value decrypts the embedded configuration, which provides instructions for that particular RansomHub sample. If the wrong password is supplied, the RansomHub sample will not properly execute. RansomHub shares several code overlaps with ALPHV and Knight; although unconfirmed, it is likely that it inherited the use of passwords from them as a safeguard against forensic analysis.

- 3AM was first observed in September 2023 being deployed as a fallback piece of malware in failed LockBit ransomware attacks. According to Kaspersky, 3AM implements an "access key" feature to protect against automatic sandbox execution.

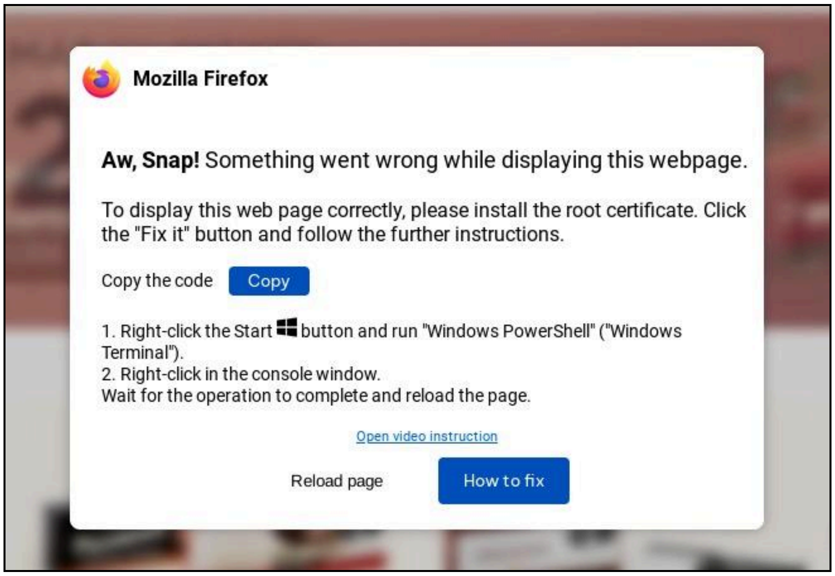
Another trend we observed in the first half of 2024 was the combination of malware loaders and ransomware. As of June 26, 2024, upon review of Recorded Future's Collective Insights data, we identified attack chains involving GuLoader and Remcos, which ultimately led to the deployment of LockBit. GuLoader is a sophisticated loader first observed in 2019. It is known for its robust evasion techniques for delivering various malware. In addition to Remcos, these malware include Formbook, XLoader, 404Keylogger, Lokibot, Agent Tesla, Nanocore, and Netwire. Remcos, on the other hand, is a commodity RAT that was first discovered being sold on criminal forums in the second half of 2016.

The attack chain began with phishing emails delivering GuLoader, which then retrieved and executed Remcos to gain control over the system. This access was ultimately used to install LockBit ransomware, leveraging double-extortion tactics to steal and encrypt data before demanding ransom. In the 90 days before June 26, 2024, Recorded Future documented nearly 100 instances where GuLoader and Remcos were used together in Recorded Future Malware Intelligence executions, underscoring the growing prevalence of this attack sequence.

Trojans, Infostealers, and Loaders Introduce New Defense Evasion Techniques

In line with our observations surrounding ransomware strains, malware like trojans, infostealers, and loaders focused extensively on improving their defense evasion capabilities in H1 2024. Malware such as Raspberry Robin, SocGholish, and HijackLoader sought to bypass security solutions by implementing new anti-emulation, execution, and process hollowing techniques. Additionally, ClearFake, RedLine, and Coyote experimented with new delivery techniques featuring the use of less-popular programming languages and software tools.

- In May 2024, ReliaQuest reported a phishing campaign distributing ClearFake that prompted victims to manually copy a provided PowerShell code into Windows terminal, which then automatically executed. ClearFake is a JavaScript framework typically spread via drive-by downloads and fake browser update notifications. This new execution technique bypassed detections, including suspicious parent–child process relationships, malicious file downloads, and Mark-of-the-Web signatures.



Mozilla Firefox

Aw, Snap! Something went wrong while displaying this webpage.

To display this web page correctly, please install the root certificate. Click the "Fix it" button and follow the further instructions.

Copy the code

1. Right-click the Start button and run "Windows PowerShell" ("Windows Terminal").
2. Right-click in the console window.
Wait for the operation to complete and reload the page.

***Figure 3**: Phishing message in ClearFake's campaign prompting victims to copy malicious PowerShell code (Source: ReliaQuest)*

- In April 2024, HarfangLab reported that a new Raspberry Robin variant was the first malware to use virtual dynamic-link library (VDLL) specific function import to prevent emulation and sandbox environments. VDLLs are modified versions of standard Windows DLL files that exist only within emulator environments. Raspberry Robin attempts to dynamically import functions known to exist only in emulators. If the import succeeds, indicating the presence of a sandbox, Raspberry Robin exits. Raspberry Robin was first identified in 2021 and has been associated with cybercriminal threat actors like CL0P, Evil Corp, FIN11, and TA505 [1, 2].

- In April 2024, McAfee reported observing a new variant of RedLine using Lua bytecode. Attackers delivered RedLine via a ZIP file hosted in the `vcpkg` repository of Microsoft's official GitHub account. If clicked and executed, the MSI file created a scheduled task to execute `compiler.exe` with `readme.txt` (the Lua bytecode) as an argument. Lua is a less common programming language and security tools often lack the capability to analyze it. Threat actors took advantage of this to obfuscate malicious strings and evade detection.

- In February 2024, ReliaQuest observed a new variant of SocGholish, a malware active since at least early 2018 and linked to TA569 and EvilCorp [1, 2], introducing Python to compromised environments for persistence and defense evasion purposes. The new SocGholish variant created a scheduled task (`pypi-py`) that executed a malicious Python script (`hklib.py`) every five minutes, ensuring the script would run continuously. The SocGholish variant also employed `pythonw.exe`, a Python interpreter that does not display a console window, hiding its execution.

- In February 2024, Kaspersky profiled a new banking trojan likely developed by Brazilian cybercriminals dubbed Coyote that uses Squirrel, a relatively new tool for installing and updating Windows applications, in its infection chain instead of the typical MSI installers. Using Squirrel allowed Coyote to hide its initial stage loader as an update packager. To further evade detection, Coyote also combined Node.js and a loader written in NIM to run obfuscated JavaScript and its final payload.

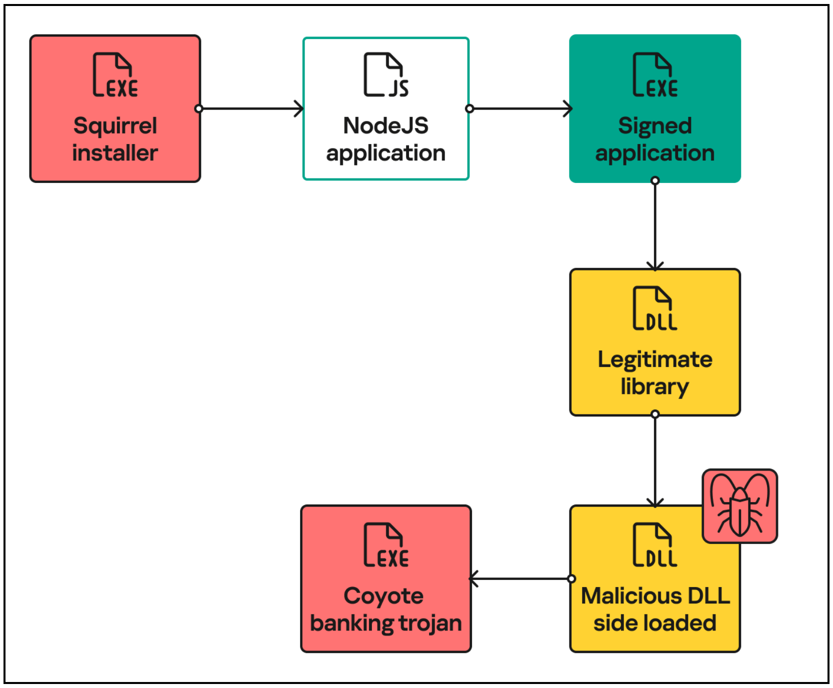


***Figure 4**: Overview of Coyote's infection chain (Source: Kaspersky)*

- In February 2024, CrowdStrike noted that HijackLoader expanded its defense evasion capabilities, by combining process hollowing with process doppelgänging. This involved using pipes to redirect input/output, modifying the `.text` section of loaded DLLs like `mshtml.dll` with shellcode, and leveraging techniques such as Heaven's Gate and transacted section hollowing to inject and execute malicious payloads stealthily in target processes like `cmd.exe` and `logagent.exe`. HijackLoader was first documented in September 2023 delivering DanaBot, SystemBC, and RedLine.

Magecart Infections Increased in H1 2024

Magecart infections increased significantly in the first half of 2024 compared to the second half of 2023. Based on evidence from Recorded Future's Payment Fraud Intelligence, we observed an approximately 103% increase in the number of Magecart intrusions between H2 2023 and H1 2024 (**Figure 5**).

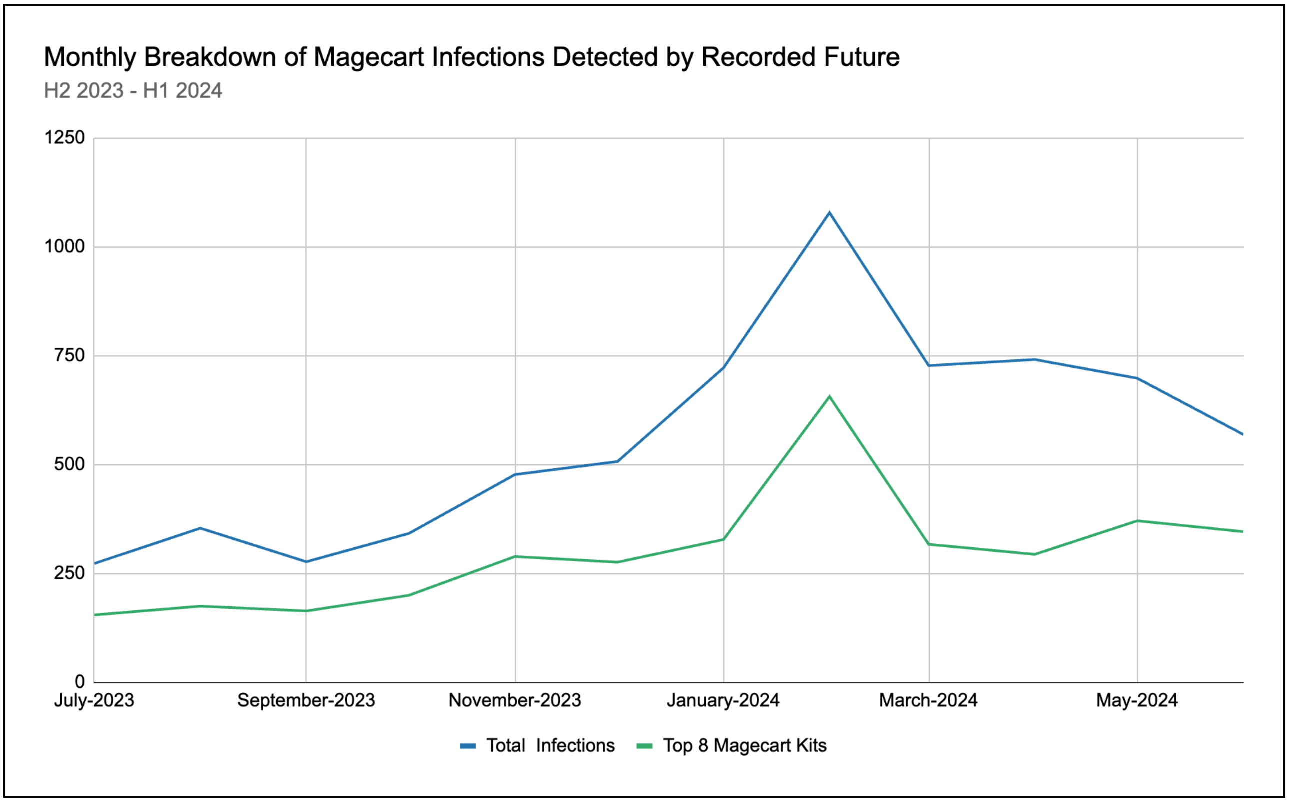


Figure 5*: Magecart intrusions detected by Recorded Future between H2 2023 and H1 2024 (Source: Recorded Future)*

Although the observed increase could have been driven by the addition of new indicators of compromise (IoCs) and e-commerce domains into Recorded Future's Magecart scanner, we assess that other factors were highly likely responsible for the trend. These include the exploitation of new vulnerabilities affecting e-commerce platforms and the arrival of new Magecart kits in the threat landscape.

- In April 2024, Sansec reported that threat actors have been targeting Magento websites vulnerable to CVE-2024-20720, a critical flaw affecting Adobe Commerce disclosed in February 2024, and infecting these with a fake Stripe payment skimmer.
- In March 2024, Insikt Group identified “fleras”, a member of the top-tier forums XSS and Exploit, advertising a reportedly easy-to-use sniffer malware (dubbed “Sniffer By Fleras”) that was capable of intercepting network traffic and user input on infected devices for $1,500. Between March and July 2024, threat actors used Sniffer By Fleras to infect at least 488 e-commerce websites. The uptick in recent detections of Sniffer By Fleras is shown in **Figure 6** below.

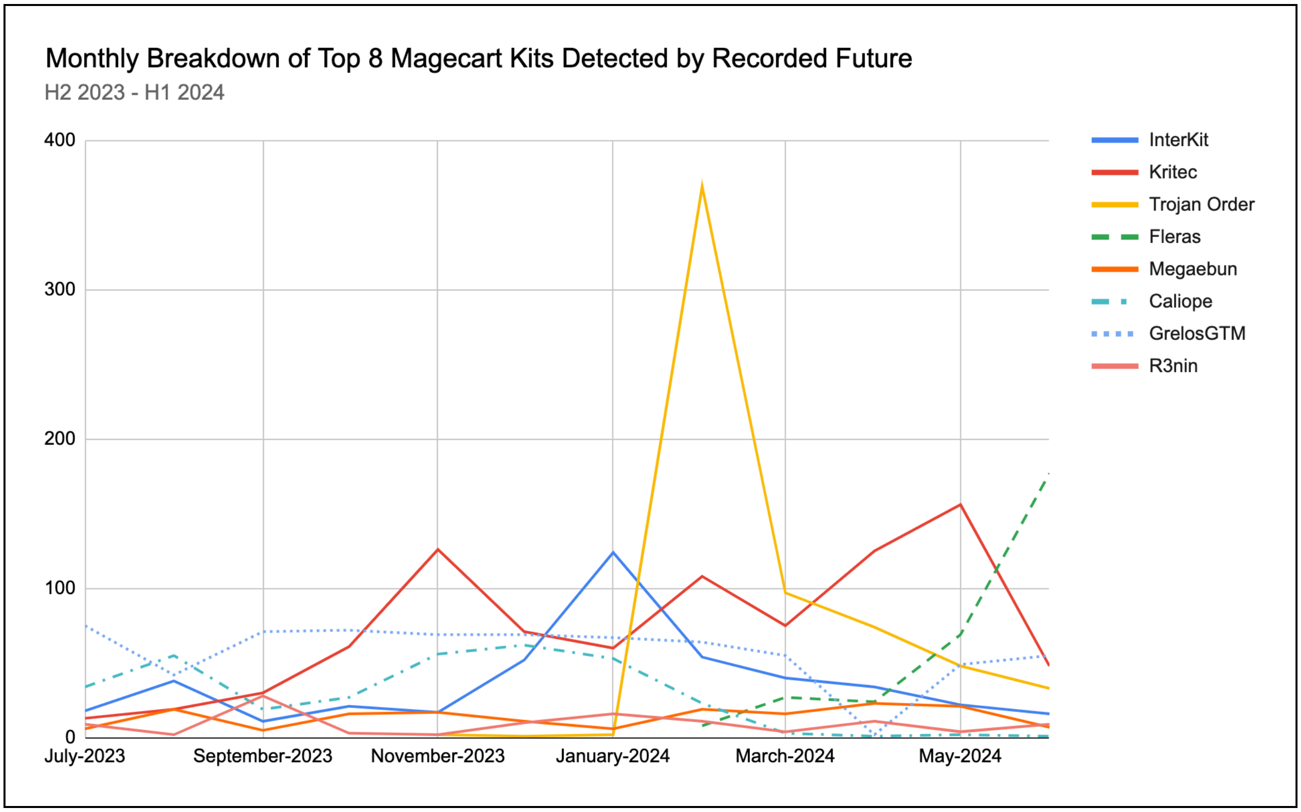


Figure 6*: Intrusions associated with the top eight Magecart kits Recorded Future detected between H2 2023 and H1 2024 (Source: Recorded Future)*

E-skimming has remained relatively consistent in recent years, with only minor advancements in the core scripting methods employed by cybercriminals. However, the methods used to construct the e-skimmer scripts have continued to adapt, as have the obfuscation techniques used to disguise them. Actors continue to move away from the injection of e-skimmer URLs directly into websites, opting for loader scripts that deobfuscate the e-skimmer URL upon execution. Even loaders that inject the e-skimmer URL into the page are being phased out and replaced with loaders that retrieve the script from the e-skimmer URL and execute it directly. HTML tags capable of embedding client-side scripts are becoming the injection point of choice for malicious actors. We continue to see abuse of free services, such as Amazon CloudFront, Google Tag Manager (GTM), and Telegram Bot API, within the Magecart attack chain. These services are used for hosting loaders and e-skimmer scripts, and in the case of Telegram, serving as the receivers of stolen data.

Mitigations

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

Vulnerability Exploitation

- **Inventory Scan**: Conduct comprehensive inventories and regular scans of technology stacks to identify third-party software in use and help detect outdated or unpatched products. Focus on software types most exploited by threat actors, such as remote access and security solutions.

- **Robust Patch Management Cycles**: Establish a routine patch management process to ensure software is updated promptly. Learn vendors' typical patch release schedules and implement automated tools to manage and deploy patches efficiently. Expedite patching for any vulnerability for which PoC is available online.

- **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.

- **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.

Malware Intrusions

- **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 interactive process hollowing and malware written in less commonly used programming languages like Lua and NIM.

- **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.

- **Recorded Future Hunting Packages**: Recorded Future customers can implement Hunting Packages developed by Insikt Group to monitor for intrusions associated with prominent malware families.

Magecart Attacks

- **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.

- **Advance PCI-DSS 4.0, Para. 6.4.3 Compliance:** This new Payment Card Industry Standard is scheduled for implementation in March 2025, but pursuing early compliance can be very beneficial. Validating all scripts used by a merchant website along with change management controls around the scripts will help detect magecart infections and shorten the infection window.

- **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.

Outlook

In the remaining months of 2024, the exploitation of newly discovered vulnerabilities affecting ubiquitous enterprise and remote access software will almost certainly remain a favored attack vector among cybercriminals and state-sponsored groups. This is primarily due to the ubiquitous nature of such products. Since the COVID-19 pandemic, companies have increasingly come to rely on remote access solutions to maintain remote workforces. Furthermore, security solutions like next-generation firewalls (NGFWs) are widely adopted for security and compliance reasons.

Three major factors of a more general nature further underpin this prediction. First, because patching systems is often a complicated process requiring systems to be taken offline, companies continue to struggle to patch vulnerabilities in a timely manner. According to Skybox Security, the average time companies took to patch vulnerabilities in 2023 exceeded 100 days. This is a significant period of time, especially when considering that in 2023 threat actors reportedly exploited 75% of vulnerabilities in nineteen days or less. Second, the number of zero-days disclosed and exploited each year is increasing, a trend driven primarily by Chinese state-sponsored threat actors, the business practices of the commercial surveillance industry, and gray vulnerability marketplaces. Finally, threat actors are increasingly benefiting from proof-of-concept (PoC) exploit code, with recent evidence from Cloudflare demonstrating that some attacks occur as quickly as 22 minutes after the exploit code for newly discovered vulnerabilities becomes available online.

In terms of malware developments, we anticipate that infostealers will continue to play a major role in the threat landscape in the coming months. Infostealers are one of the primary sources of compromised credentials, a highly prized commodity in the underground economy that can facilitate follow-on malicious activity. For example, in April 2024, Kaspersky reported a 643% increase between 2020 and 2023 in the number of devices that fell victim to infostealers. As long as demand persists for compromised credentials, and the criminal forums and markets where they can be sold remain available, infostealers will almost certainly remain a prevalent threat.

We also expect threat actors to continue improving their social engineering and defense evasion capabilities, adapting to the ever-evolving security landscape to ensure successful infections. To this end, threat actors will almost certainly increasingly turn to less-common cross-platform programming languages, such as Lua, and alternatives to file types that defenders and security solutions have come to expect in malware execution chains, such as MSI.

Lastly, we do not anticipate any significant slowdown in Magecart intrusions for the remainder of 2024 as threat actors exploit newly disclosed vulnerabilities in e-commerce platforms and take advantage of new e-skimmers. In line with our assessments for other malware types, we expect threat actors to continue experimenting with new delivery mechanisms in Magecart attacks. Primarily, we anticipate that threat actors will almost certainly continue abusing HTML tags and legitimate services as long as doing so lowers the likelihood of detection.

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 clients, enables tangible outcomes, and prevents business disruption.

About Recorded Future®

Recorded Future is the world's largest threat intelligence company. Recorded Future's Intelligence Cloud provides end-to-end intelligence across adversaries, infrastructure, and targets. Indexing the internet across the open web, dark web, and technical sources, Recorded Future provides real-time visibility into an expanding attack surface and threat landscape, empowering clients to act with speed and confidence to reduce risk and securely drive business forward. Headquartered in Boston with offices and employees around the world, Recorded Future works with over 1,800 businesses and government organizations across more than 75 countries to provide real-time, unbiased, and actionable intelligence.

Learn more at recordedfuture.com