CYBER
THREAT
ANALYSIS

Recorded Future®

By Insikt Group®

August 17, 2023

H1 2023: Ransomware's Pivot to Linux and Vulnerable Drivers

This report examines trends in malware use, distribution, and development, as well as high-risk vulnerabilities disclosed by major hardware and software vendors between January 1 and June 30, 2023.

Executive Summary

Ransomware attacks defined the nexus of malware development and vulnerability exploitation in H1 2023, particularly since ransomware groups increasingly relied on vulnerability exploitation. In 4 separate, prominent ransomware campaigns, attackers used vulnerability exploitation to compromise many organizations in a relatively short time, as was the case with VMware ESXi hypervisors in February 2023.

A part of this increase in vulnerability exploitation is likely due to ransomware groups' increased preference for targeting Linux servers. Linux and Linux-related operating systems (such as ESXi) allow for much faster scaling of attacks, but they typically feature a less user-rich environment than traditional corporate and consumer platforms like Windows or MacOS. As a result, they are harder to compromise via exposed credentials, making vulnerability exploitation a higher priority for initial access.

Given this likely trend, organizations in all industries and geographies need to increase real-time visibility into their vendors and software supply chains. As a starting point, organizations should inventory not just vendors whose products have been known to be exploited, but also product types known to be exploited, such as managed file transfer (MFT) systems, and review patch management programs for these products. Strategically, defenders should adopt the attacker's perspective by focusing on products and vendors that generate significant revenue, centralize large amounts of data, and lack redundancy.

Further highlighting the prominence of ransomware, the malware variants associated with cyberattacks that were most referenced in our data set in H1 2023 were LockBit ransomware, ALPHV ransomware, Royal ransomware, ESXiArgs, and Pegasus. Aside from these, we observed a rise in malware that exploited vulnerable drivers as a means of bypassing endpoint detection and response (EDR) solutions. Because these attacks exploit the trust that the operating system has in legitimate system components, defenders need to keep an accurate inventory of drivers used by their organizations and ensure that these drivers are patched against known vulnerabilities.

An exploitation event with very high financial consequences was the exploitation of the zero-day vulnerability CVE-2023-2868 affecting Barracuda's email security gateway (ESG), leading Barracuda to instruct users to completely replace their ESG appliances regardless of previous patching — a fallout that could cost Barracuda and its users up to 50% of the company's annual revenue. This event in particular showcases the costs associated with a lack of IT and security redundancy. Aside from Barracuda, the top-referenced vulnerabilities associated with cyberattacks in H1 2023 affected VMware ESXi hypervisors, Microsoft Outlook, Ruckus Wi-Fi access points, Apache's Log4J, and Oracle's WebLogic servers.

For the rest of 2023, we assess that both ransomware attacks through exploited vulnerabilities and attacks involving malware targeting vulnerable drivers will continue to be popular among threat actors. In light of attacks affecting third-party vendors and security software, defenders should focus on optimizing resources and budgets to ensure redundancy in their security architecture. Redundancy ensures that risk is more evenly distributed across resources in case of a vendor breach.

Ransomware and Infostealers Joined by Driver Malware in Popularity

It is impossible to discuss malware trends throughout H1 2023 without discussing ransomware and information stealer (infostealer) malware. These 2 kinds of malware have been prominent for some time, as we previously noted in our H1 2022 report. However, we also observed malware targeting vulnerable drivers during the H1 2023 reporting period. This type of malware exploits the trust between the operating system and system components, all while evading EDR detection. The most broadly referenced malware associated with cyberattacks are listed below, followed by a discussion of malware trends throughout the time period.

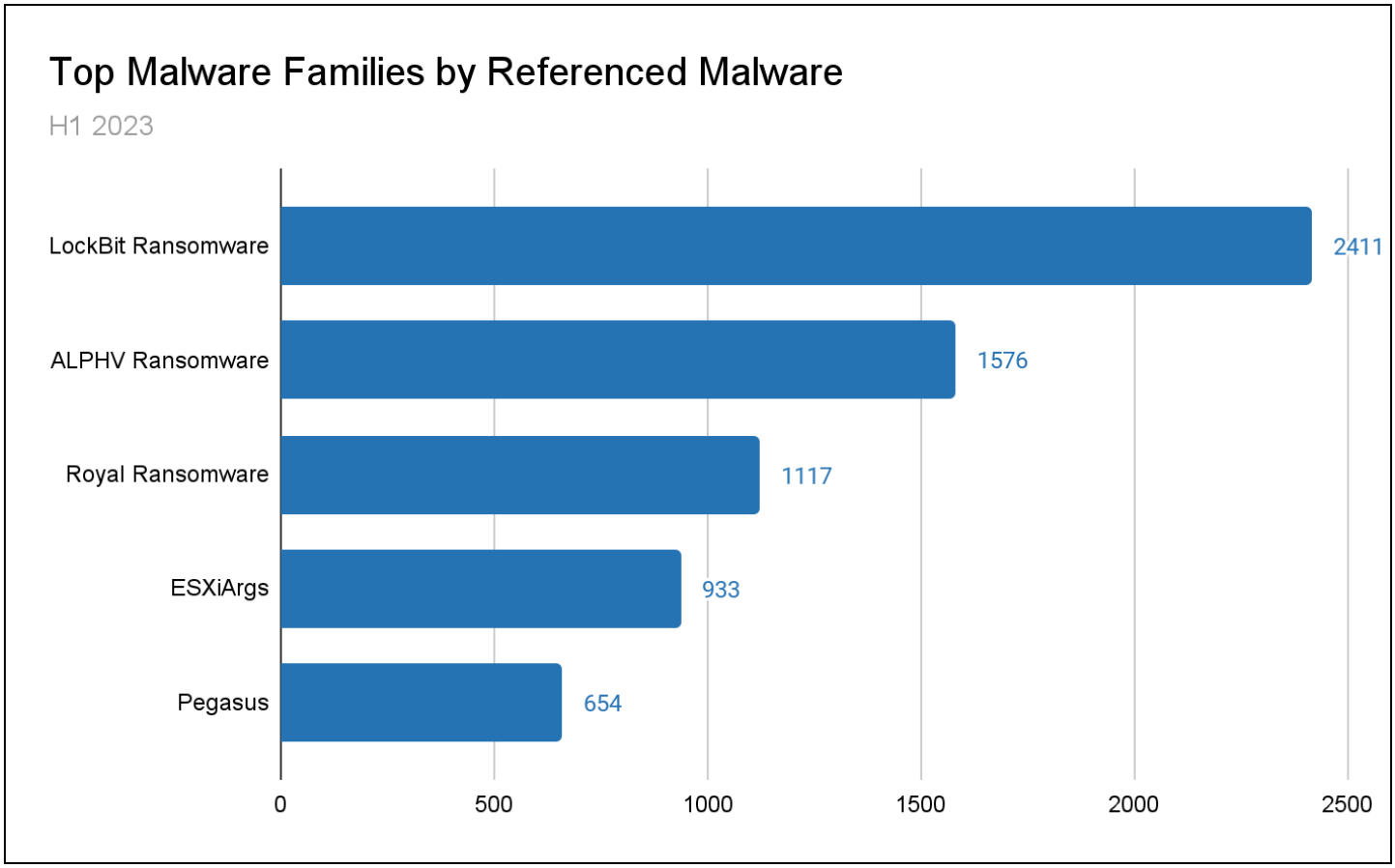

Figure 1: *Malware appearing in the most references to reported cyberattacks in H1 2023 (Source: Recorded Future)*

Ransomware Threat Landscape

As demonstrated by the preponderance of ransomware variants in the chart above, the threat of ransomware and cyber extortion continues to be a prevalent trend affecting all major industry verticals. Many ransomware groups practice double extortion, in which they exfiltrate victim data to hold for ransom before encrypting victim files and threatening to release the data publicly if victims do not comply with their ransom demands. Many ransomware groups also operate ransomware-as-a-service (RaaS) business models, which allow them to profit from their commodity ransomware. Both LockBit and ALPHV follow this model, likely contributing to both LockBit and ALPHV's ubiquity as demonstrated by their nearly 60% share of the top references to malware (as shown above). While the vast majority of ransomware is designed to target Windows systems, we have seen ransomware groups increasingly modifying their attack arsenals in the first half of 2023 to be compatible with Linux operating systems. One such example is IceFire Ransomware, which deployed novel Linux versions of its ransomware variant in a campaign of network intrusions against several media and entertainment enterprises in March 2023.

The expansion of IceFire's capabilities to target Linux systems is consistent with similar capability expansions for other ransomware groups, as notable shifts to targeting Linux machines have also occurred this year. CL0P ransomware also modified its ransomware source code to be compatible with targeting Linux servers. Compatibility with Linux machines increases the number of potential targets for ransomware attacks. However, Linux systems are typically servers, which means that scalable initial access techniques such as phishing, drive-by compromise, or credential stuffing are less effective as means to gain access to these machines. Instead, vulnerability exploitation, where it can be implemented, is a more certain way for attackers to target these machines. The exploitation of vulnerabilities at scale is further discussed in the following sections of this report.

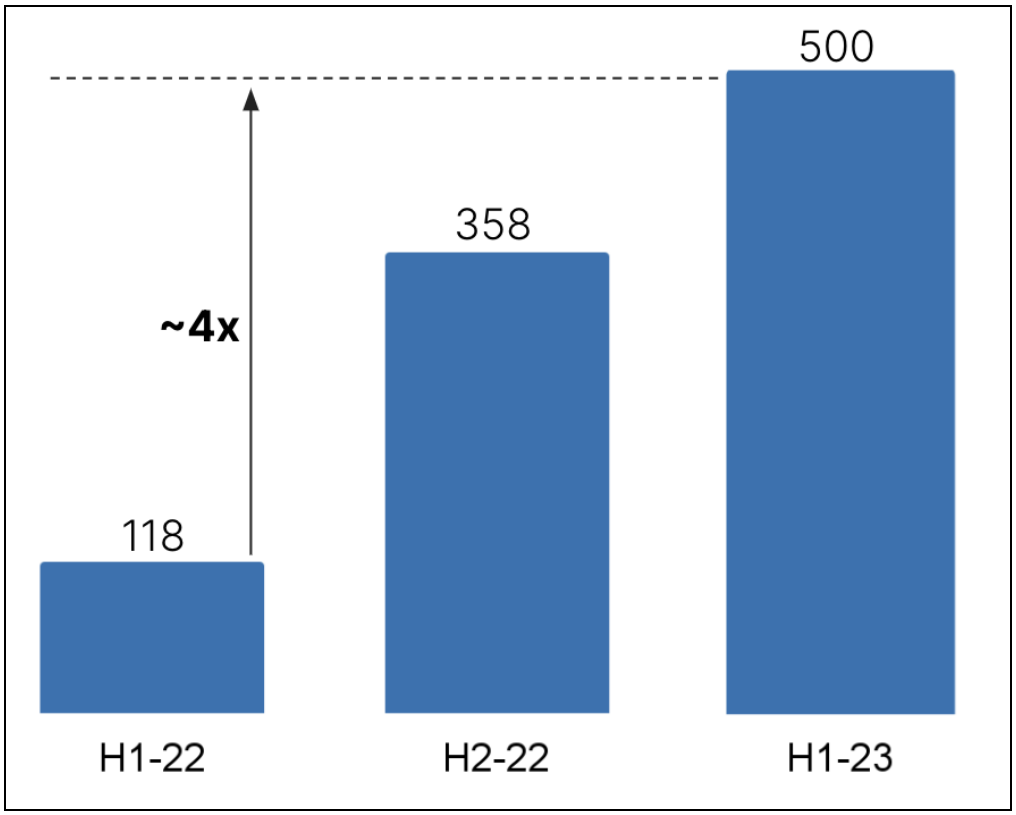

Figure 2: *Increased rate of references to ransomware attacks on Linux systems (Source: Recorded Future)*

Ransomware Groups Force Profits from Fewer Paying Victims

In addition to expanding their target pool, ransomware groups have had to get resourceful in other ways to keep turning profits. While total revenue and payments have increased in 2023 compared to 2022, the monetization rate of ransomware itself has struggled to keep up. Last year signaled a 40% decline in ransomware revenue, subsequently threatening ransomware groups' business models as fewer victims paid ransoms and had improved incident responses to attacks. Although worsening monetization indicates that some efforts to combat ransomware have been effective, in the short term (including H1 2023) it means that groups have become incentivized to seek bigger payouts where they can. Because ransomware groups are almost all exclusively motivated by financial gain, they are less concerned about where a target sits geographically or within a certain sector than whether the target can pay; hence, their trend toward targeting victims opportunistically.

A good example of a large (and potentially foolhardy) ransom demand was when LockBit demanded a $70 million sum from the semiconductor chip manufacturing giant TSMC in early July 2023. In reality, LockBit had breached a third-party technology supplier of TSMC, Kinmax Technology, and there is no indication that Kinmax paid any ransom.

Other prolific groups, like CL0P, ran in the opposite direction, looking for as wide a target set as possible rather than counting on 1 big payout since victims are less likely to pay. During CL0P's

exploitation of Fortra's GoAnywhere product in Q2 2023 (further discussed below), research estimated a 30% to 45% drop in victims paying ransom demands compared to another spree in 2021, when CL0P exploited 4 zero-day vulnerabilities in Accellion file transfer software to launch ransomware attacks. In its most recent campaign exploiting MOVEit, CL0P was likely able to extort more money due to the increased numbers of victims involved. For example, while CL0P claimed that it was able to breach around 130 victims of GoAnywhere exploitation, some estimate that the group has exploited over 350 organizations as a result of MOVEit — resulting in an estimated $75 million earned from ransom payments.

While the collective refusal to pay ransoms will burn a hole in attackers' savings over time, it means that in the short term, attackers will attempt large ransom demands or high-volume exploitation to squeeze profits out of the victims that do pay. Thanks to big-game hunting, ransomware groups are sitting at $449 million in revenue for just the first half of 2023, putting 2023 on track to be the second-most lucrative year for ransomware groups (after 2021).

Infostealer Malware Threat Landscape

Infostealer malware is increasingly available to cybercriminals on the dark web as a malware-as-a-service (MaaS), increasing the threat of account takeover and credential stuffing attacks. Infostealer malware is designed to steal full fingerprints of logins from victim devices, including items like session tokens that can bypass multi-factor authentication (MFA). As a result, infostealers can provide cybercriminals with immediate account access without requiring them to test thousands of credentials in credential-stuffing attacks or use paid proxy traffic services. Credential sales remain popular on dark web sources, and we assess that it is unlikely there will be a decrease in the threat of infostealer malware, barring any changes in threat actors' incentives or network defenses.

Attackers are increasingly innovating their methods for distributing infostealers at scale. One of these methods has been poisoning code packages in popular software libraries frequented by developers, such as the Python Package Index (PyPI). A zero-day supply-chain attack against PyPI in January 2023 involved 3 identical, malicious executable packages that imitated legitimate ones. The 3 poisoned packages reportedly boasted complete project descriptions to lure unsuspecting developers into downloading the packages, which infected their machines with infostealers. In February 2023, security researchers identified 3 separate package-poisoning campaigns that targeted PyPI as well as node package manager (npm). Researchers at Fortinet, Phylum, and Check Point published findings about the campaigns, in which attackers injected malicious packages into these popular developer software repositories in order to distribute infostealers to developers who fell for the lures. This trend has continued past H1 2023, with reports of the Lazarus Group tricking victims into downloading malicious repositories and npm package dependencies.

Apart from deploying infostealers, threat actors have also deployed cryptominers and ransomware via poisoned PyPI and npm packages. To counter this overall threat, defenders should create a private registry with pre-vetted allowlisted packages for developers to use. Employees should always check packages against checksums provided by vendors. While this does not address a situation in which a

vendor's build process is compromised and malicious code is inserted during development, many vendors provide the SHA1, SHA256, or MD5 checksums of their software products. Where possible, defenders should also segment the network to isolate tools such as build environments and source code repositories from the external internet or internal resources that are not needed. Lastly, defenders should ensure that logging is enabled and unexpected accesses to development systems are evaluated.

Increased Popularity of "BYOVD" Attacks

While ransomware and infostealers have been and will likely continue to be prevalent malware threats, the use of another kind of malware, specifically driver-based malware, significantly grew during the reporting period. In H1 2023, "bring your own vulnerable driver" (BYOVD) attacks and exploit development increased by 180% compared to H2 2022 (see Figure 3) as a means of bypassing antivirus (AV) and endpoint detection and response (EDR) solutions. BYOVD is a technique in which threat actors drop a legitimate driver signed with a valid certificate onto a target system, enabling them to run malware with kernel privileges on the victim device, disable existing security solutions, and obtain control of the system. The growing availability of tools with built-in driver exploitation capabilities on underground forums or public code repositories is likely a major factor in this recent increase.

Use of this technique dates back to as early as 2012 when the Shamoon campaign used the RawDisk driver — which allowed manipulation of hard drives from user space without any special permissions — to deliver the Disttrack wiper to a Saudi Arabian energy company. Since then, various threat groups have continued to use BYOVD attacks, ranging from state-sponsored advanced persistent threat (APT) groups, like Lazarus in 2021, to financially motivated ransomware gangs, like BlackByte in 2022.

The BYOVD technique has also gained traction recently in discussions on dark web and underground forums, such as in the case of Terminator, an offensive security tool advertised on Ramp Forum by threat actor "spyboy" in May 2023. Terminator exploits a signed Zemana AntiMalware kernel driver to gain kernel privileges and terminate processes related to AV software and EDR platforms. In June 2023, multiple security researchers reproduced the tool and made their versions publicly available on GitHub. Terminator was also deployed as part of an ALPHV ransomware campaign in July 2023.

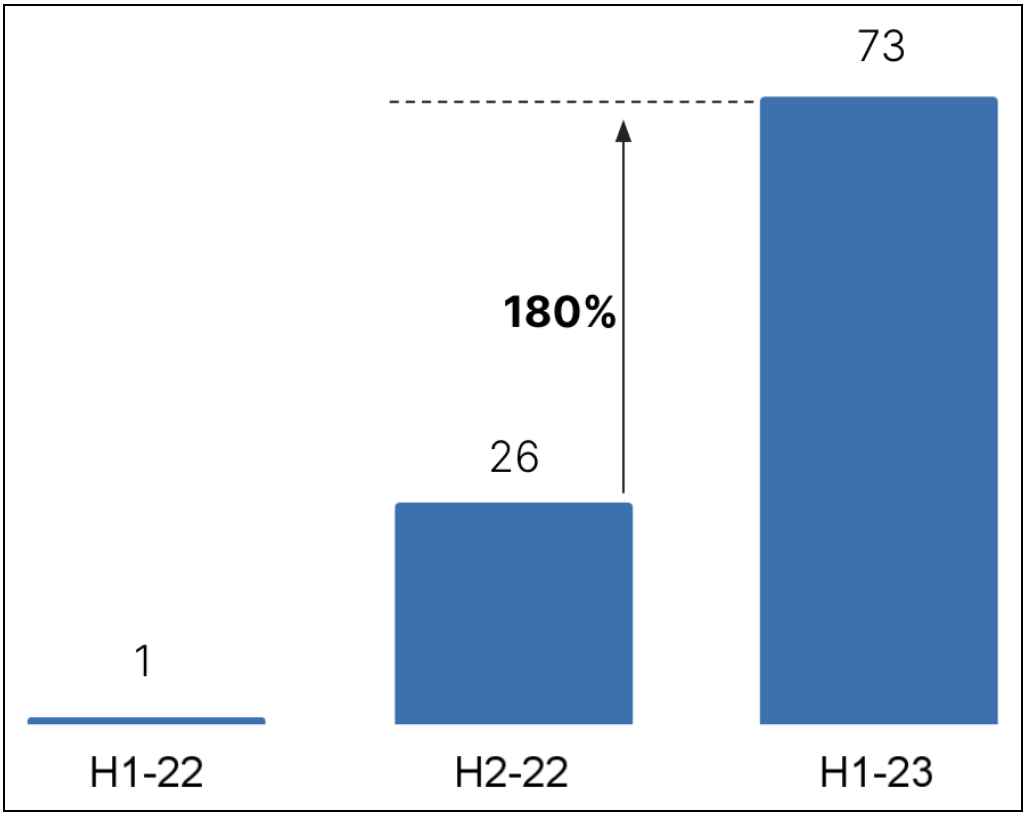

Figure 3: *Comparison of reported BYOVD attacks and exploit development in H1 2022, H2 2022, and H1 2023 (Source: Recorded Future)*

In H1 2023, AuKill, a malware derived from the open-source tool Backstab that targets EDR systems, was the most prevalent threat associated with reported BYOVD attacks. In April 2023, Sophos reported that AuKill had been used in 3 ransomware attacks since the beginning of 2023. In January and February 2023, the MedusaLocker ransomware gang used AuKill in 2 separate ransomware attacks; and in February 2023, threat actors used AuKill to deploy LockBit ransomware.

AuKill attempts to disable EDR solutions either by forcing them to shut down or by preventing them from running. To run AuKill, the attacker must have administrative privileges on the target system. An attacker must also run a vulnerable driver in kernel mode to bypass the Protected Antimalware Services feature introduced in Windows 8.1. To do this, AuKill exploits a legitimate but out-of-date and vulnerable driver (version 16.32) of the Microsoft utility Process Explorer. This behavior is very similar to AuKill's predecessor, Backstab, which was first published in June 2021. Backstab also uses a Process Explorer driver to disable EDR solutions operating on a compromised device.

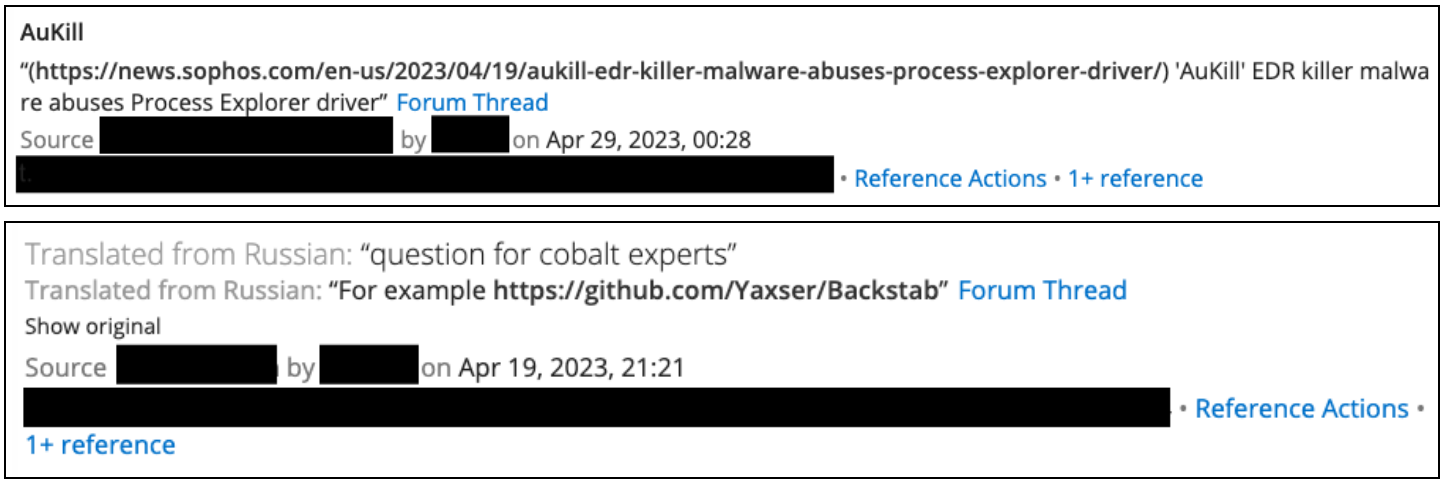

Figure 4: *Discussion of AuKill and Backstab on dark web and special-access sources (Source: Recorded Future)*

Threat actors who are members of dark web and special-access forums such as Exploit and XSS discuss the use of both Aukill and Backstab malware families and share news articles regarding them. As part of the attack chain, these malware families exploit legitimate driver software for privilege escalation and evade detection by disabling security products designed to interfere with malicious campaigns, allowing for efficient and stealthy operations. Thus, we believe AuKill and Backstab operators will continue to use vulnerable drivers in their attacks to obtain privileged access to systems.

Apple, Microsoft, and MFT Service Providers Disproportionately Affected by Zero-Day Exploitation

Apple and Microsoft software products were disproportionately affected by zero-day vulnerabilities in H1 2023, including Microsoft Office and Apple's iOS and Safari Webkit. Outside of these, zero-day exploitation of hardware appliances like Barracuda's ESG by a suspected Chinese threat group resulted in the forced replacement of ESGs, the cost of which is likely to be equal to a majority portion of the company's revenue. Below, we list the most broadly referenced vulnerabilities used in cyberattacks, followed by a discussion of vulnerability trends throughout the time period.

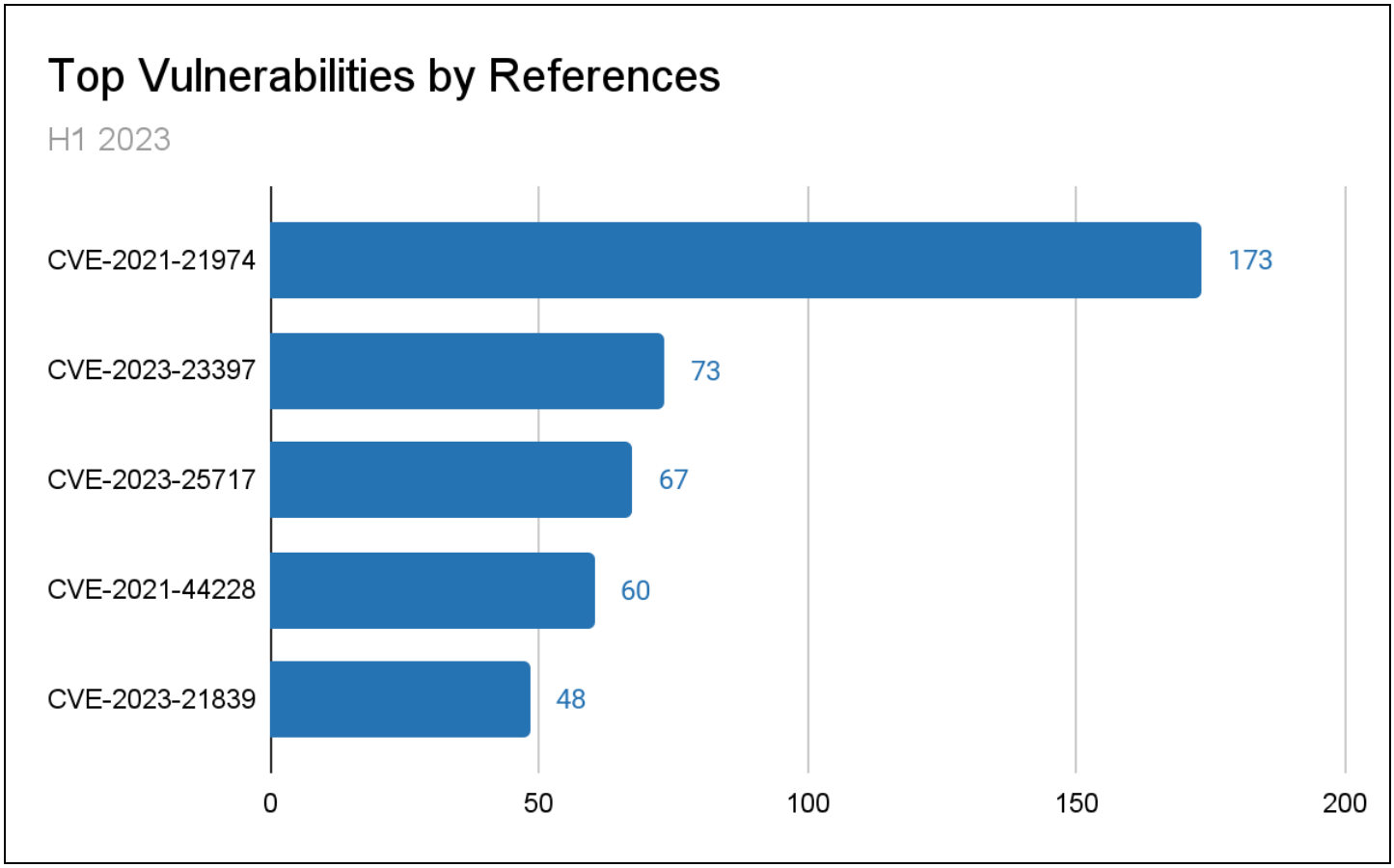

Figure 5: *Vulnerabilities appearing in the most references to reported cyberattacks, H1 2023 (Source: Recorded Future)*

Frequently Exploited Zero-Day Vulnerabilities Affected Third-Party MFT Tools

By confirmed victim counts, the most widely exploited zero-day vulnerabilities so far in 2023 have affected 2 third-party MFT tools: Progress Software's MOVEit Transfer (CVE-2023-34362) and Fortra's GoAnywhere MFT (CVE-2023-0669). More information on these vulnerabilities and their exploitation can be found in the **Cost to Victims** section later in this report.

Apple and Microsoft Disproportionately Affected by Zero-Day Vulnerabilities

Apple and Microsoft were disproportionately affected by zero-day vulnerabilities compared to other software vendors. Apple patched 9 zero-day vulnerabilities in the first half of 2023; Microsoft patched at least 10. Some of these zero-day vulnerabilities were connected to publicized threat campaigns, detailed further below.

H1 2023 saw the exploitation of 3 zero-day Apple vulnerabilities in a spyware campaign dubbed Operation Triangulation, which the Russian government previously blamed on the US (there is no additional evidence from open sources to confirm that these accusations are true). The vulnerabilities are found in various Apple products such as Apple iOS, iPadOS, macOS, watchOS, and Safari WebKit. The first vulnerability is an integer overflow vulnerability, tracked as CVE-2023-32434, which allows an application with kernel privileges to perform code execution when exploited. The 2 other vulnerabilities, tracked as CVE-2023-32435 and CVE-2023-32439, are Apple WebKit vulnerabilities that lead to code execution when executing maliciously crafted web content.

The details of Operation Triangulation — and TriangleDB, an iOS spyware component used in the operation — were publicized by the Moscow-based cybersecurity company Kaspersky in June 2023, after the malware was detected on iPhones within its network. Operation Triangulation operators attack their targets by sending iMessages with malicious attachments. Kaspersky stated that attackers deployed the implant on targeted devices after exploiting an unspecified kernel vulnerability. On June 21, 2023, Apple released updated patches for all 3 zero-day vulnerabilities.

The best way to mitigate all actively exploited zero-day vulnerabilities affecting Apple devices is to apply patches as soon as they are released. To ensure the timely implementation of critical patches like the ones outlined above, Apple product users should ensure that automatic updates are enabled on their devices. Steps to enable automatic iOS and iPadOS updates are outlined here, and steps to enable automatic updates for macOS are outlined here.

Top Vulnerabilities by Reference Count

According to the Recorded Future Intelligence Cloud, there are 3 zero-day vulnerabilities associated with threat actors deploying malware that received the highest number of references in H1 2023: CVE-2023-23397, CVE-2023-28252, and CVE-2023-24932.

CVE-2023-23397 is a privilege escalation flaw in Microsoft Outlook that allows a remote, unauthenticated attacker to send a specially crafted email that leaks the targeted user's hashed Windows account password. The vulnerability has been observed in a months-long cyber-espionage campaign conducted by a threat actor tracked as UNC4697, likely linked to the APT28 group, against government, transport, energy, and military sectors in Europe. CVE-2023-23397 has gained significant attention from security bloggers, analysts, and researchers, indicating its severity, and it required a follow-up patch in May 2023 to be fully patched. A proof of concept exploit for CVE-2023-23397 has also been shared, further emphasizing the need for immediate patching.

CVE-2023-28252 is a zero-day vulnerability in the Windows Common Log File System (CLFS) that threat actors have been exploiting to deploy Nokoyawa ransomware payloads. The vulnerability is an out-of-bounds write vulnerability that allows an authenticated threat actor to gain SYSTEM privileges. A threat actor could exploit the vulnerability by manipulating base log files and modifying the registry

contents of the *HKEY_LOCAL_MACHINE|SAM*, allowing for privilege escalation exploits and access to credentials.

Kaspersky observed that threat actors used similar exploits to the CLFS elevation-of-privilege vulnerability as early as June 2022, targeting businesses related to retail, energy and natural resources, manufacturing, healthcare, and software providers. CVE-2023-28252 was exploited to deploy Nokoyawa ransomware between June 2022 and February 2023 in attacks linked to the Nokoyawa Ransomware Group. The majority of the attacks targeted small to medium-sized businesses in the Middle East, North America, and Asia. During the campaign, Nokoyawa Ransomware Group also used post-compromise tools, such as Cobalt Strike Beacons, to bypass antivirus detection.

CVE-2023-28252 affects all versions of Windows servers and clients. Microsoft addressed CVE-2023-28252 as part of the April 2023 Microsoft Patch Tuesday. The US Cybersecurity and Infrastructure Security Agency (CISA) also added CVE-2023-28252 to its Known Exploited Vulnerabilities Catalog (KEV) and ordered the Federal Civilian Executive Branch (FCEB) agencies to secure their systems until May 2, 2023.

According to Microsoft's advisory, CVE-2023-24932 can allow threat actors to bypass the Secure Boot on the Unified Extensible Firmware Interface (UEFI) level of a targeted system. Once threat actors have bypassed the Secure Boot, they can perform arbitrary code execution. Microsoft noted that a threat actor can perform these activities if they have administrator privileges on the affected device. The flaw had been exploited by malicious actors to deploy the BlackLotus bootkit malware. BlackLotus has various persistence and defense evasion capabilities, including disabling security programs such as BitLocker, hypervisor-protected code integrity (HVCI), and Windows Defender. Microsoft released a security update to address the zero-day vulnerability affecting Microsoft Windows Server.

Most-Costly Vulnerabilities

The most expensive vulnerabilities, in terms of the cost of remediation after organizations were attacked via the exploitation of those vulnerabilities, can be categorized in 2 primary ways: (1) the cost to organizations and individuals victimized by attacks via exploitations of that vulnerability; and (2) the cost to the software and hardware vendors whose products were affected by those vulnerabilities.

Cost to Victims

In terms of the cost to victims, exploitation by CL0P of the 2 critical vulnerabilities affecting MFTs — Progress Software MOVEit Transfer (CVE-2023-34362) and Fortra's GoAnywhere MFT (CVE-2023-0669) — would qualify as the most costly due to the volume of high-profile ransomware attacks and sensitive data exposures that they enabled. In addition to the upfront cost of paying a ransom amount (as described above in the section "Ransomware Groups Force Profits from Fewer Paying Victims"), victims of ransomware attacks can face disruptions to business operations and may have to provide identity protection services to parties affected by sensitive data exposure. Furthermore, according to the Harvard Business Review, publicly traded companies "suffered an

average decline of 7.5% in their stock values after a data breach, coupled with a mean market cap loss of $5.4 billion".

IBM reported in its Cost of a Data Breach Report 2023 that the current average global cost of a data breach is $4.45 million. This figure takes into consideration the costs associated with detection and mitigation, post-breach response, notification, and lost business, not to mention the money associated with individual instances of identity theft that can be enabled by these exposures. For reference, just 1 of the hundreds of attacks on MOVEit Transfer resulted in the exposure of names, Social Security numbers (SSNs), birthdates, and addresses of nearly the entire population of Louisiana.

Cost to Vendors

CVE-2023-2868, a zero-day vulnerability in Barracuda Networks's Email Security Gateway (ESG) appliance, very likely qualifies as the most costly vulnerability in terms of cost to product vendors for H1. Researchers assess that the vulnerability was exploited by a China-nexus group known as UNC4841. According to several online resources, Barracuda likely generates between $300 and $500 million in annual revenue. Per a Reddit thread, Barracuda was willing to replace relevant Barracuda hardware above the 300 model of its Email Security Gateway (ESG) at no cost, but clients would need to pay to replace any version below that model. According to Rapid7, there were roughly 11,000 publicly findable Barracuda appliances that would need to be replaced when the news of the vulnerability was disclosed. Using a very rough median figure of ~$15,000 for the cost of Barracuda ESG appliances from the 200 model up to the 900 model, this amounts to ~$165 million (potentially up to 50% of Barracuda's annual revenue) in remediation costs, just for Barracuda hardware replacement.

Most-Advertised Vulnerability Exploits on the Dark Web

The most frequently advertised exploits on dark web sources in H1 2023 were for CVE-2022-41082, CVE-2021-44228, and CVE-2023-23397. While exploitation of CVE-2022-41082 (ProxyNotShell RCE) and CVE-2021-44228 (Log4Shell) has been observed for the past 2 years and was addressed in our 2022 Annual Report, CVE-2023-23397 (the privilege escalation flaw in Microsoft Outlook that was tied to a months-long cyber-espionage campaign) is new. In many cases, threat actors advertised tools that can help less-skilled threat actors automate and expedite the process of deploying exploits in support of their threat campaigns. Such cybercrime-as-a-service offerings lower the barriers to entry into cybercrime.

Vulnerabilities with Very Critical (99+) Risk Scores

The vulnerabilities that had the highest risk scores in the Recorded Future Intelligence Cloud and were disclosed in H1 2023 are shown in the table below. All of these vulnerabilities were identified as having been exploited in the wild, either based on open-source reporting or our internal honeypot tracking. This chart reflects our assessment that Microsoft and Apple products were disproportionately affected by actively exploited vulnerabilities.

Vulnerability	Risk Score	Affected Vendor/Product
CVE-2023-21716	99	Microsoft Office, Sharepoint, Word
CVE-2023-23397	99	Microsoft Office
CVE-2023-24932	99	Microsoft Windows
CVE-2023-20887	99	VMware Aria Operations
CVE-2023-20867	99	VMware Tools
CVE-2023-27992	99	Zyxel NAS Firmware
CVE-2023-32439	99	Apple Webkit
CVE-2023-32434	99	Apple Kernel
CVE-2023-32435	99	Apple Webkit
CVE-2023-26258	99	Arcserve Unified Data Protection

Table 1: *Vulnerabilities with Very Critical Risk Scores in H1 2023 (Source: Recorded Future)*

Exploited Vulnerabilities Fuel Ransomware Sprints in H1 2023

Ransomware threat actors increasingly turned to exploiting vulnerabilities to compromise victim environments during H1 2023. These vulnerabilities affected software products more likely to be used by enterprises, such as MFT or print management software products. In some cases, this allowed threat actors to target a high number of victims in a short amount of time, resulting in sprints of ransomware activity throughout the time period.

The most notable examples of ransomware sprints in H1 2023 were 2 campaigns that targeted VMware ESXi hypervisor servers and Progress MOVEit File Transfer applications, respectively. In early February 2023, reports emerged that VMware ESXi hypervisor servers were infected, seemingly suddenly, with a new ransomware strain called ESXiargs. Servers were initially exploited through a vulnerability that had been patched for 2 years, CVE-2021-21974, which is the most widely referenced vulnerability in cyberattacks. Researchers estimate that there were 500 ESXiargs host infections within the span of a few days. In another instance of widespread, rapid exploitation of enterprise software, in late May 2023, CL0P ransomware affiliates started exploiting a vulnerability in MOVEit File Transfer (CVE-2023-34362); by July 2023, CL0P had listed over 350 victims on its data extortion site that were breached via vulnerable MOVEit Transfer instances. CL0P was able to rapidly steal data using a "smash and grab" technique, bypassing the encryption process and instead only exfiltrating stolen data from victim networks.

Preceding the widespread MOVEit Transfer attacks, CL0P ransomware also exploited a zero-day Fortra GoAnywhere vulnerability (CVE-2023-0669) in February 2023, leading to the compromise of approximately 130 organizations. In April, we observed the exploitation of CVE-2023-27350 and CVE-2023-27351 in PaperCut Multifunction (MF) and Next Generation (NG) software to deliver LockBit and CL0P ransomware variants; although the number of organizations infected is unclear, PaperCut software is used by hundreds of thousands of organizations. By the following month, CVE-2023-27350 was being used in attacks launched by the Bl00Dy Ransomware Gang against schools in the US.

The trend of exploiting enterprise technologies speaks partly to how ransomware actors are subverting organizations' increasing reliance on cloud-based services and platforms. A corporation with robust internal security controls can be well protected from compromise; however, any internet-facing enterprise software it employs is more likely to contain vulnerabilities outside of the organization's purview that can be exploited. According to Verizon's Data Breach Investigation report, roughly 30% of all intrusions that started by exploiting vulnerabilities involved those found in web applications, and among the top action vectors for ransomware specifically were desktop-sharing software and web applications. Insufficient security controls and lack of visibility into vulnerabilities in enterprise software, paired with fast-paced ransomware extortion tactics, create conditions for widespread damage.

Cloud-based enterprise software can also be a lucrative target because it often centralizes sensitive data that can later be monetized. This data often belongs not only to the targeted organization but also to those up and down the supply chain. Threat actors' focus on exploiting enterprise technology, and the bursts of ransomware activity elicited when vulnerabilities are found, are unlikely to subside, to the extent that vulnerabilities afford threat actors the ability to launch attacks against multiple victims at once and successfully demand ransoms at scale.

Outlook

We previously noted that ransomware threat actors will continue to look for and exploit vulnerabilities in third-party software to gain entry into victim systems when such activity allows them to launch attacks at a larger scale to increase profits. CL0P's exploitation of vulnerabilities in the GoAnywhere and MOVEit breaches indicates that the same features that make certain enterprise software easy to implement can make exploiting it a dangerous attack vector against many organizations at scale.

This means that in addition to mitigations that defenders already take against ransomware, they should also prioritize the review of security policies around third-party software. This review especially applies to products known to be targeted during H1 2023 such as print management software, hypervisor servers, and MFT tools— especially if they are not sold by Progress or Fortra, as those companies' products were previously targeted and are thus likely to be a higher focus of security teams, disincentivizing future attacks. To mitigate against ransomware threats, organizations should take the following steps:

- Inventory the MFT systems used

- Maintain a high-functioning vulnerability patch-management program and real-time supply-chain visibility, with a specific focus on areas in which there is no vendor redundancy
- Ensure that this patch-management program includes up-to-date staffing rotation shifts and patching schedules
- Maintain an updated intelligence feed of pertinent vulnerabilities
- Maintain coordinated communications with vendors to ensure a consolidated response and solid understanding of roles and responsibilities in the event of a high-criticality or zero-day vulnerability disclosure

Threat actors will almost certainly continue to employ vulnerable drivers to avoid detection and gain access to systems with elevated privileges. We assess that the frequency of driver abuse will continue to grow in the coming months, and we suspect that it is only a matter of time before an "as-a-service" model appears for this particular attack vector. Defenders should subsequently:

- Use internal and external intelligence to keep track of which legitimate drivers are being abused by adversaries in the wild
- Identify known driver blocklists and block these drivers, where possible, to minimize the chance of them being used inside the organization's network
- Log and regularly audit drivers installed on company systems; similar to third-party software discussed above, defenders should focus on drivers' patching cycle to minimize the possibility that they are exploited by threat actors

As threat actors continue to exploit enterprise technology, including security technology like Barracuda's ESG, companies that rely on a single security or IT solution are more likely to feel the effects of an attack on any one single vendor. As a result, organizations should focus on software and system redundancy when reviewing cybersecurity and enterprise technology budget allocations, as redundancy will help better distribute cyber risk within companies.

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 1,700 businesses and government organizations across more than 75 countries to provide real-time, unbiased and actionable intelligence. Learn more at recordedfuture.com.