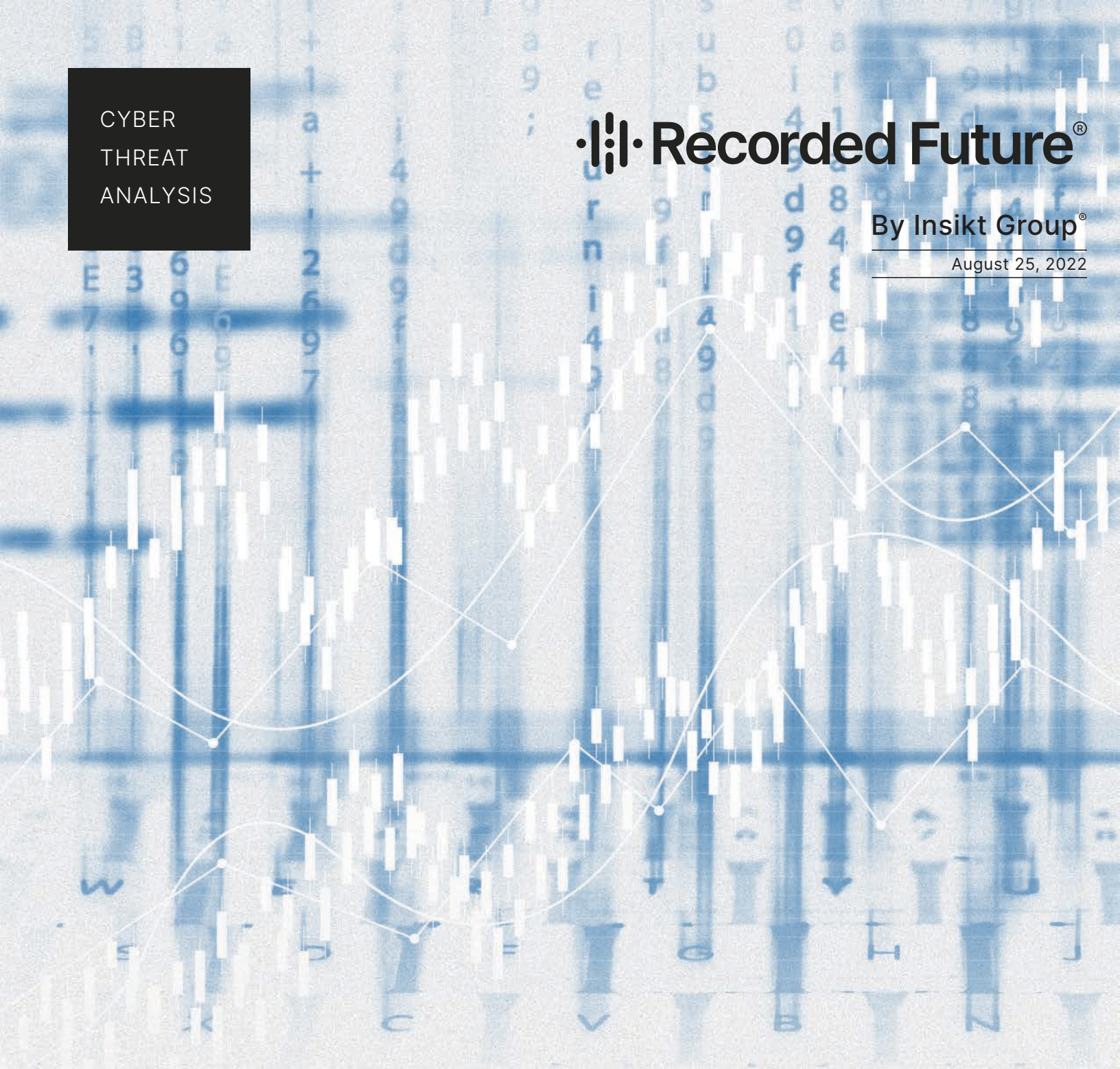
CYBER
THREAT
ANALYSIS

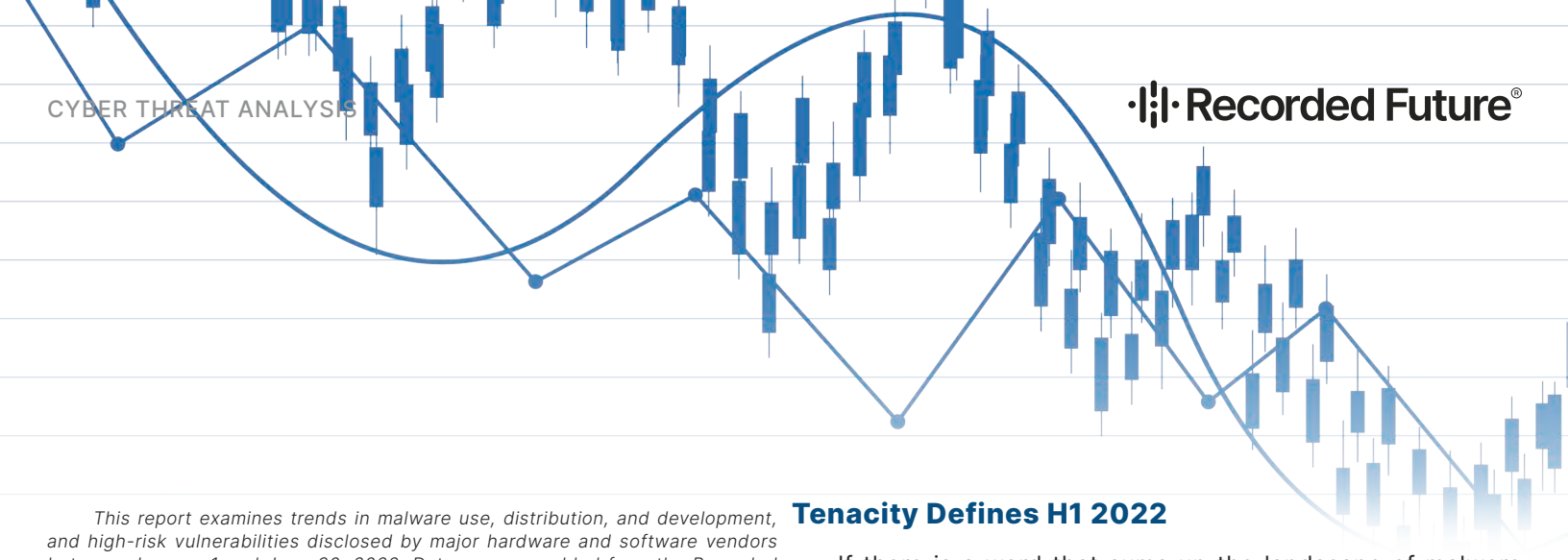
Recorded Future®

By Insikt Group®

August 25, 2022



H1 2022:
Malware and Vulnerability Trends Report



This report examines trends in malware use, distribution, and development, and high-risk vulnerabilities disclosed by major hardware and software vendors between January 1 and June 30, 2022. Data was assembled from the Recorded Future® Platform, open-source intelligence (OSINT), and public reporting on NVD data. This report will assist threat hunters and security operations center (SOC) teams in strengthening their security posture by prioritizing hunting techniques and detection methods based on this research and data along with vulnerability teams looking for ways to prioritize patching and identify trends in vulnerability targeting.

Executive Summary

Malware development and vulnerability exploitation in H1 2022 were defined by tenacity along several aspects, including criminal services, exploit targets, infrastructure maintenance, and operational longevity. The malware categories that were at the forefront of public and criminal attention were wipers, such as were observed targeting Ukraine, infostealers, with some popular variants resurging after an initial disappearance, and ransomware, which continues to victimize all sectors worldwide. The vulnerability most in defenders' sights at the beginning of the year was Log4Shell, while by the end of June, the Follina vulnerability (which can be exploited via a malicious document without using macros) indicated a future potential direction for zero-day exploits for the rest of the year.

The top referenced malware variants associated with cyberattacks in H1 2022 were Cobalt Strike, Conti ransomware, Pegasus, DeadBolt ransomware, and Emotet. References to Cobalt Strike were sharply higher than for the others, demonstrating its continued prevalence across many types of cyberattack campaigns.

The top referenced vulnerabilities associated with cyberattacks in H1 2022 affected Apache's Log4J (Log4Shell), Microsoft Windows (Follina), Microsoft Exchange Server (ProxyShell), Atlassian's Confluence, and the Java Spring Framework. This landscape reflects both zero-day exploitation and continued targeting of known vulnerabilities, and Log4Shell exploitation was observed up to the end of June.

Our outlook for the rest of 2022 based on H1 2022 is that ransomware remains a major threat (although a decline is overdue), more widespread multi-factor authentication (MFA) will reshape many areas of the criminal landscape, and Russia's war against Ukraine is likely to result in yet more novel malware from that region.

Tenacity Defines H1 2022

If there is a word that sums up the landscape of malware development and vulnerability exploitation in H1 2022, it is almost certainly "tenacious". The high-volume creation of wiper malware against Ukraine, the re-emergence of a popular infostealer, the ongoing attention to major vulnerabilities like Log4Shell and ProxyShell, the disbandment of the Conti ransomware group to support other ransomware operations, the appearance of new tactics in the (still not dead) Emotet botnet, and the continuing evolution in tactics from major cybercrime group FIN7 exemplify a criminal underground and APT threat landscape in which many threats can disappear or change temporarily but are very difficult to stop entirely. While not directly within H1 2022, the emergence of Lockbit 3.0 as the most recent version of that ransomware further supports this view of the threat landscape.

The criminal underground on which threat actors rely for new malware or vulnerability exploits has shown a similar level of persistence. The "Faceless" proxy service, which we reported on in April 2022, involves many of the aspects we have seen across malware and vulnerabilities in the first half of 2022: malware designed to target online retailers, emphasis on remote code execution (RCE) and zero-day vulnerabilities, and long-term criminal operations that can survive law enforcement action, rebranding, and lack of access to infrastructure. Similarly, the creation of BreachForums after the seizure of Raid Forums by law enforcement shows the persistence of criminal networks and the ease with which new forums can replace closed ones where there is continued demand.

The charts below show the top most referenced malware variants and vulnerabilities associated with reported cyberattacks in H1 2022. These were based on queries for any malware entity or any vulnerability entity that appeared in reports of a cyberattack as collected in the Recorded Future Platform.

The malware data set best shows the persistent reliance of threat actors on Cobalt Strike for command-and-control (C2) infrastructure, although a larger shift to the pentesting tool Brute Ratel C4 may be in the near future. Another trend highlighted in Figure 1 is the persistent ransomware threat, with attackers continuing to develop novel ransomware for specific targets like QNAP (in the case of DeadBolt).

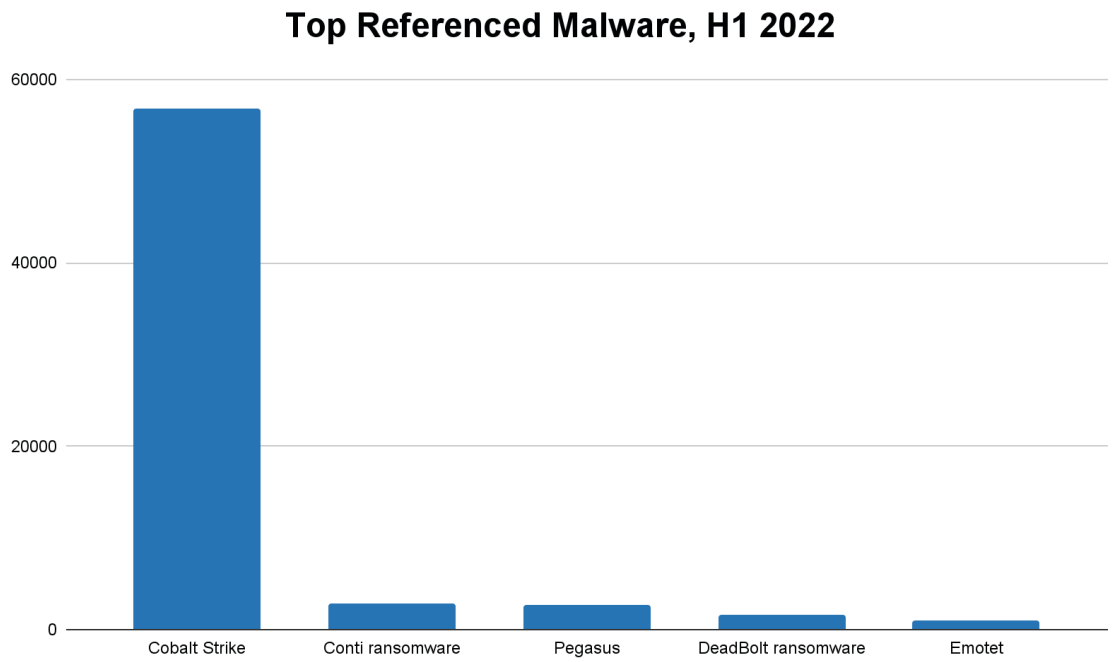


Figure 1: Malware appearing in the most references to reported cyberattacks, H1 2022 (Source: Recorded Future)

The vulnerability data set summarized in Figure 2 highlights the continued dominance of Microsoft vulnerabilities in cybercriminal and APT exploitation.

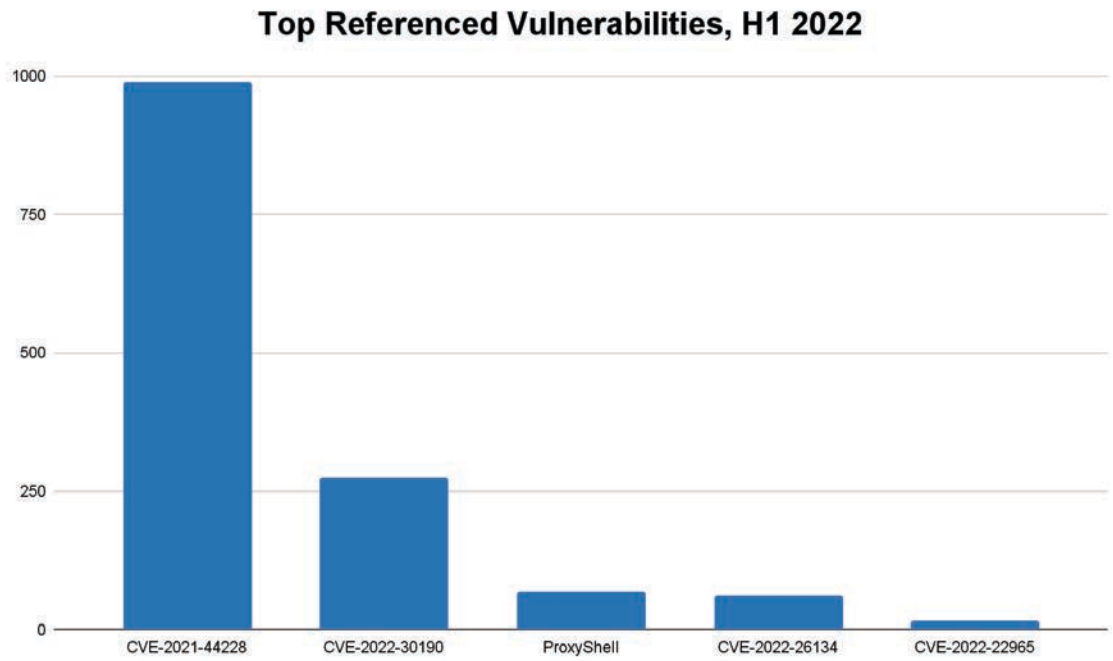


Figure 2: Vulnerabilities appearing in the most references to reported cyberattacks, H1 2022. ProxyShell includes 3 distinct vulnerabilities (CVE-2021-34473, CVE-2021-34523, and CVE-2021-31207). (Source: Recorded Future)

Wipers, Infostealers, and Ransomware at Forefront of Malware Reporting

In H1 2022, one of the biggest drivers of discussion of new malware and vulnerability exploitation was Russia's invasion of Ukraine and the subsequent appearance of cyber threat campaigns apparently designed to support Russia in disrupting Ukrainian targets or destroying sensitive Ukrainian data. In particular, the disclosure of 9 distinct variants of wiper malware in line with previous Russian state-sponsored activity exemplified the Russian government's total approach to warfare against its neighbor, including both kinetic and cyber attacks. This trend also appeared to show a hostile government enjoying less time and fewer resources to develop malware against key geopolitical targets: the 9 pieces of wiper malware that were deployed against Ukraine were found to be increasingly simplistic over time, with devolution including less obfuscation and fewer stages between variants.

A malware category that has consistently fed compromised data to dark web marketplaces like Russian Market is infostealers, which are designed to identify and exfiltrate sensitive data from victim machines. After the popular infostealer malware Raccoon Stealer temporarily halted operations in March 2022, many threat actors switched from Raccoon Stealer to other infostealer brands such as Mars Stealer, MetaStealer, BlackGuard, RedLine, and Vidar. However, Raccoon Stealer 2.0 has reemerged at the end of H1 2022, proving to be again as popular as it was when we analyzed it in 2019 and saw it "spiking in popularity and activity across underground forums".

Perhaps the most dramatic moment in a malware operation for H1 2022 occurred when the operators of the Conti ransomware targeted the government of Costa Rica, said that they were "determined to overthrow" that government as part of a series of crippling attacks, and then shut down their extortion website infrastructure as part of a disbandment that allowed individual members to support other ransomware gangs. Conti's antics aside, its disruption of critical government services in Costa Rica is one of numerous examples in H1 2022 of ransomware attackers bringing organizations' operations to a halt, with some of the most prolific operators being those behind the LockBit 3.0 and Hive ransomware families.

Mirroring the bravado of the Conti Gang, the financially motivated cybercrime group FIN7 was identified by Recorded Future as having created a fake cybersecurity company, Bastion Secure, which it used to try to distribute post-exploitation tools like Carbanak as if they were information technology (IT) management and security monitoring tools. This was one example of the group's evolution of new tactics. Mandiant's update report on the activities of FIN7 pointed out that the group heavily uses junk strings to obfuscate its malware. Its LOADOUT downloader, a VBS-based payload, has used junk code (such as the not-so-subtle string "FUCKAV") for obfuscation. Additionally, Mandiant found that FIN7 would use public code analysis repositories to test whether versions of LOADOUT were being recognized by antivirus engines, and if they were, the group would quickly add in even more junk code to stay ahead of detection.

Overlapping malware and vulnerability trends, throughout H1 2022 multiple researchers reported cyberattack campaigns from the DeadBolt ransomware operators that narrowly targeted QNAP network-attached storage (NAS) devices, including via exploitation of the Linux vulnerability "Dirty Pipe" (CVE-2022-0847). When Dirty Pipe was first disclosed, our analysis of this local privilege escalation (LPE) Linux vulnerability found that multiple proof-of-concept (POC) exploits existed for it, making it easy for exploitation from numerous threat actors. More generally, Linux-targeting ransomware is at this point a yearslong trend that reflects cybercriminals' desire to quickly target high volumes of virtualized storage, which often relies on the Linux-based VMWare ESXi hypervisor.

Log4Shell and Follina Bookend Half-Year of Zero-Day Exploitation

From 2021 to 2022, one of the most discussed topics with respect to cybersecurity was Log4Shell, the simple-to-exploit vulnerability in Apache's Log4J software that exposed hundreds of thousands of organizations based on the logging utility's ubiquitous use. As recently as June 2022, we have continued to see news of cyberattackers conducting Log4Shell exploitation. Exploitation of an earlier set of vulnerabilities known as ProxyShell, which affect Microsoft Exchange, was also an ongoing threat from multiple threat actors. As we have identified in vulnerability research within the last several years, cybercriminals prefer to target a small set of known vulnerabilities that they can count on to be present on victim systems.

The vulnerabilities that had the highest risk scores in the Recorded Future Platform and were disclosed in H1 2022 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. From a product perspective, the most notable aspect of this list is that vulnerabilities affecting Linux outnumber those from Microsoft.

Vulnerability	Risk Score	Affected Vendor/Product
CVE-2022-22718	99	Microsoft Windows
CVE-2022-23222	99	Linux
CVE-2022-0847	99	Linux
CVE-2022-0995	99	Linux
CVE-2022-0609	99	Google Chrome
CVE-2022-1388	99	F5 BIG-IP
CVE-2022-26134	99	Atlassian Confluence Server and Data Center
CVE-2022-30190	99	Microsoft Windows
CVE-2022-30075	99	TP-Link Router AX50

Table 1: Highest Risk Score for vulnerabilities in H1 2022 (Source: Recorded Future)

As disclosed in late H1 2022, Insikt Group identified multiple Chinese state-sponsored groups exploiting a zero-day vulnerability in Sophos Firewall. This was in line with our observation that Chinese APT groups have moved away from exploiting user-grade products like web browsers or word processors and towards enterprise-grade products like mail servers and firewalls.

In June 2022, Google's Project Zero published a blog stating that as of that point, they had identified exploitation of 18 zero-day vulnerabilities for the first half of 2022, and that half of those were variations of previously disclosed zero-day vulnerabilities. While Google's definition of a variation can be more or less flexible (for example, identifying a flaw in the Windows MSDT service [CVE-2022-30190] as a variation of a flaw in the MSHTML browser engine [CVE-2021-40444]), their findings suggest that once a critical vulnerability is identified in one software component, it is likely to attract further criminal and security researcher attention, thereby finding even more flaws.

While H1 2022 began with responses to Log4Shell, it was the disclosure of CVE-2022-30190 ("Follina") that defined the end of the first half of the year. Follina represents a new arena of exploitation of Microsoft Windows systems without recourse to malicious macros, which have been a mainstay of cyber intrusion campaigns in the last several years. With Microsoft rolling back their previous decision to block macros by default, and then rolling back their rollback, the criminal underground and APT groups are likely both waiting to see whether macros or Windows utilities are the future of maldocs.

Outlook

The persistence of ransomware operations, criminal forums, botnet deployment, and zero-day exploitation throughout H1 2022 is part of a general landscape of cyber threat activity that has low barriers to entry and multiple avenues for monetizing stolen data, disrupting victim organizations, and gaining access through flaws in user- and enterprise-grade software. Based on this multi-pronged and constantly evolving group of threats, organizations across all sectors, and of all sizes, must rely on a comprehensive security program that can track cyber threat actors at multiple stages of intrusion.

It has become a common refrain, year over the last several years, to say that we expect ransomware to continue to be a major threat for all industry verticals. H1 2022 is no different, since at this point many ransomware operators very likely have access to "war chests" of funds from victim payments that they can rely on to continue attacks and develop malware for the long term, even in the midst of less profitable seasons. Unlike stealing payment card data or installing e-skimmers on retailer websites, ransomware allows cybercriminals to monetize access to any organization, effectively making it the most widely lucrative form of cyberattack based on victim sector. However, there were hints of a decline in ransomware attacks at the end of 2021 and we are likely closer to a point at which a combination of changes in cyber insurance policies and better security postures overall force criminals to rethink the current model.

On a related note, credential and browser fingerprint theft is a continuing issue that is likely to see a radical shift in malware and criminal markets once MFA policies have reached a certain level of saturation across industries and platforms. The continued high-volume use of infostealers by criminals looking to monetize stolen financial data or personally identifiable information (PII) contradicts the notion that "all my data is out there anyway": if that were true, criminals would not put so much stake in getting more of it through stealers like Raccoon Stealer and Mars Stealer. Modern infostealers allow criminals to steal cookies and other specialized data often required to bypass modern security features of retailers, financial enterprises, and other organizations' systems that have over time improved their effectiveness and rendered personal data such as email addresses, usernames, and passwords by themselves worthless in many respects. Already in 2022, we have seen criminal attempts at one-time-password (OTP) and MFA bypass as an indicator of the likely direction of malware development once other forms of data theft have been made more difficult or impossible.

Forecasting the future of a war is beyond our subject matter expertise and a good way to be wrong within a very short time. This applies completely to Russia's war against Ukraine, with the caveat that as long as Russia's current government remains in power, it is very likely that we will see continued disruptive attacks against Ukrainian targets featuring novel malware or vulnerability exploitation. Finally, with respect to zero-day exploitation, it would be an unprecedented surprise for a half-year of exploitation like we saw in H1 2022 to not be followed by similar activity into the rest of the year.

About Insikt Group®

Insikt Group is Recorded Future's threat research division, comprising analysts and security researchers with deep government, law enforcement, military, and intelligence agency experience. Their mission is to produce intelligence on a range of cyber and geopolitical threats that reduces risk for clients, enables tangible outcomes, and prevents business disruption. Coverage areas include research on state-sponsored threat groups; financially-motivated threat actors on the darknet and criminal underground; newly emerging malware and attacker infrastructure; strategic geopolitics; and influence operations.

About Recorded Future®

Recorded Future is the world's largest intelligence company. Recorded Future's cloud-based Intelligence Platform provides the most complete coverage across adversaries, infrastructure, and targets. By combining persistent and pervasive automated data collection and analytics with human analysis, Recorded Future provides real-time visibility into the vast digital landscape and empowers clients to take proactive action to disrupt adversaries and keep their people, systems, and infrastructure safe. Headquartered in Boston with offices and employees around the world, Recorded Future works with more than 1,400 businesses and government organizations across more than 60 countries.

Learn more at recordedfuture.com and follow us on Twitter at @RecordedFuture.