Mandiant

M-Trends

2024 Special Report

Attacker Operations Involving Zero-Days Vary Depending on Motivation

In the ever-evolving landscape of cybersecurity, zero-day exploits remain a potent weapon in the hands of attackers. These vulnerabilities, unknown to software vendors, can provide attackers with a stealthy means to gain unauthorized access to systems and sensitive data.

> **Zero-day:** Vulnerabilities disclosed before patches are made available.

In 2023, we tracked a combined total of 97 unique zero-day vulnerabilities exploited in-the-wild, surpassing the volume tracked in 2022 by nearly 56%. People's Republic of China (PRC) cyber espionage groups were the most prolific attackers to exploit zero-days in 2023, and demonstrated a focus on stealth in their zero-day exploitation campaigns. The state-sponsored groups tracked by Mandiant primarily utilize zero-days for intelligence gathering and strategic advantage.

Another consistent component of cyber espionage exploitation has been the rise of commercial commercial surveillance vendors selling what are often turnkey or off-the-shelf capabilities. In many instances, these vendors offer not just the technical expertise to build an exploit chain, but also the subsequent tools necessary to identify and exfiltrate data from the targeted victim. The growth of these capabilities suggests internal expertise is no longer required to exploit zero-day vulnerabilities. This expands the access to zero-day exploits for attackers, even if they lack the technical sophistication to conduct zero-day research.

At the same time, financially motivated attackers have continued to embrace zero-days, aiming to infiltrate systems and steal valuable data for financial gain. During 2023, financially motivated attackers and espionage groups appear to represent roughly the same proportion of total zero-days exploited as they had in the previous two years. FIN11, a financially motivated group active since at least 2016, exploited two zero-days in 2023 in widespread campaigns. FIN11's investment in developing zero-days demonstrates their continued sophistication. Zero-day vulnerability research is a time and resource intensive process, and FIN11's exploitation of multiple zero-day vulnerabilities indicates the group has consistent access to both. Notably, FIN11 has frequently targeted file transfer applications, which can provide quick and efficient access to large amounts of sensitive data without the need for lateral movement within a victim network.

The diverse motivations of attackers translate into distinct approaches to the utilization of zero-day exploits. Espionage groups prioritizing stealth and long-term access may employ zero-days sparingly, and meticulously craft exploits to minimize detection. Financially motivated attackers, on the other hand, often prioritize speed and efficiency, potentially sacrificing stealth for quicker returns and wider exploitation.

Two case studies, derived from frontline Mandiant engagements, exemplify the varying behavior of attackers when driven by distinct objectives. The financially motivated campaign that exploited Progress Software's MOVEit Transfer demonstrates the adaptability and speed of financially motivated attackers. In contrast, the espionage-driven campaign that targeted the Barracuda Email Security Gateway (ESG) highlights the persistence and sophistication of state-sponsored groups. These case studies exemplify the varied tactics, techniques, and procedures (TTPs) of two groups that have distinctly different objectives, but prosecute those objectives with similar ingenuity and adaptability.

Cybercrime Campaign Case Study: MOVEit

In May 2023, Mandiant observed the exploitation of CVE-2023-34362,[1] a zero-day vulnerability in Progress's managed file transfer solution MOVEit Transfer. This vulnerability, affecting all MOVEit Transfer versions prior to May 31, 2023, allowed attackers to gain unauthorized access to MOVEit Transfer's database, potentially leading to data breaches and financial losses. To exploit CVE-2023-34362, the attacker had to send a specially crafted request to a vulnerable server, which injected malicious SQL statements into application queries on the vulnerable systems. After gaining access to a vulnerable application's database, the attacker could perform additional actions to gain elevated privileges and execute arbitrary code, including accessing, modifying or deleting data within the database. Mandiant investigated 31 attacks related to this vulnerability, providing valuable insights into the TTPs employed by FIN11, to which we've attributed all exploitation. Mandiant's analysis revealed a pattern of automated attacks, during which FIN11 appeared to focus on speed and efficiency of exploitation. FIN11's approach to campaigns has evolved to become more sophisticated, and pose greater risks to targeted organizations.

FIN11's Attack Campaign

FIN11 emerged as the key player exploiting the MOVEit Transfer zero-day. Mandiant's investigations revealed that FIN11 began testing the vulnerability as early as April 2022. However, public reporting indicates testing might have begun even earlier. Testing likely continued until a reliable exploit and means for data exfiltration was developed.

Beginning in May 2023, FIN11's attack methodology primarily involved the deployment of web-based backdoors, data enumeration, and data theft. Upon gaining initial access, FIN11 deployed a web-based backdoor, which Mandiant tracks as LEMURLOOT, on compromised systems. These backdoors masqueraded as legitimate software components, and provided functionality for the enumeration and theft of data. FIN11 executed commands through LEMURLOOT to enumerate files and folders, retrieve configuration information, and create or delete a user with a hard-coded name.

Impact and Remediation

Nearly 2,600 organizations across various sectors and industries were targeted by FIN11 during this campaign. The scale of the attacks further indicates that FIN11 relied on automated methods, as it would be impractical for them to engage in hands-on-keyboard intrusions on such a broad scale. Based on data posted on the FIN11 data leak site , FIN11 stole terabytes of potentially sensitive data during their campaign.

Mandiant did not identify evidence of lateral movement during any of the investigations related to FIN11's use of the MOVEit Transfer vulnerability. It is likely that FIN11's primary objective was the immediate theft of data rather than establishing long-term persistence or compromising additional systems within the target networks. Access to file transfer appliances likely provided FIN11 with sufficient access to sensitive data they could use to extort victims without needing to move laterally in the network.

Remediation efforts surrounding FIN11's targeting of MOVEit Transfer appliances involved applying a sequence of patches released by Progress Software. Organizations were urged to prioritize patching and to implement robust cybersecurity measures to safeguard against similar attacks.

Espionage Campaign Case Study: Barracuda

PRC cyber espionage groups conducted multiple high-profile zero-day exploitation campaigns in 2023. One of the most notable, and likely the most widespread, was a campaign targeting Barracuda ESG appliances.[2] UNC4841, a cluster of Chinese cyber espionage activity, targeted Barracuda ESGs through a remote command injection vulnerability (CVE-2023-2868), which was publicly disclosed in May 2023. However, Mandiant investigations identified evidence of exploitation dating back to at least October 2022. UNC4841 exploited ESG appliances by taking advantage of a flaw in the parsing logic for processing of TAR files. By formatting TAR files in a particular way, UNC4841 was able to trigger a remote command injection attack that enabled them to execute system commands. UNC4841 carefully crafted their attack strategy, employing emails cleverly designed to appear as low quality spam, and including malicious TAR archive attachments. The filenames included in the TAR archive email attachments contained malicious commands, which were leveraged to establish a foothold on vulnerable appliances. After gaining access, UNC4841 deployed a wide range of second-stage backdoors specifically tailored to Barracuda ESGs to establish long-term access, enabling them to conduct their espionage activities undetected for more than eight months.

Stealing Sensitive Data with Precision

With long-term access firmly established, UNC4841 focused on quietly stealing sensitive data from targeted organizations. Their tactics centered on harvesting email from the ESG's temporary mail storage component, which enabled them to conduct broad email collection on compromised appliances. UNC4841 also targeted email collection through shell scripts, which targeted specific email domains and users deemed to

be of strategic importance to China. Additionally, Mandiant observed UNC4841 targeting email being sent to Barracuda appliances for collection as they may originate from sources of particular intelligence value. The staging file naming conventions utilized by UNC4841 throughout the campaign were indicative of a large-scale espionage operation. UNC4841 primarily staged data in the /mail/tmp/ directory and utilized a consistent file naming convention containing three letters corresponding to the victim organization followed by a number.

Targeting Trends

UNC4841's targeting patterns evolved over the campaign, which lasted longer than eight months. While initially focusing on government organizations, as the campaign progressed, UNC4841 expanded their reach to include organizations in the information technology sector, as well as a wide range of others. After the public notification of the vulnerability, UNC4841 prioritized government agencies and high-tech organizations for deployment of specific malware families. UNC4841 deployed a series of backdoors across organizations in the post notification period in order to maintain access and continue operation.

Mitigating the Threat

On May 31, 2023, Barracuda strongly advised organizations to replace all compromised ESGs immediately regardless of patch level. This incident underscores the importance of proactive cybersecurity measures, including prompt vulnerability patching, regular security audits, and continuous monitoring of networks for attempted lateral movement or suspicious activity stemming from edge appliances. While defenders cannot anticipate a zero-day, these measures can help expose other security flaws that could allow an attacker to more easily move throughout a network or escalate privileges. Limiting the damage and breadth of an attack from undisclosed vulnerabilities helps limit the risks organizations face as attackers evolve.

A Comparative Analysis: Lessons Learned and the Evolving Threat Landscape

The campaigns targeting MOVEit Transfer and Barracuda ESG vulnerabilities highlight the evolving threat landscape, and the stark differences between how financially motivated and espionage-driven attackers operationalize the use of zero-day exploits. FIN11 prioritized a fast and efficient approach to its exploitation of MOVEit, targeting a large number of organizations for brief but efficient access to sensitive data.

Feature	Financially Motivated	Espionage
Quantity vs Quality of Victims	Vastly more victims (reportedly over 2,600)	Relatively few victims (~5% of vulnerable appliances)
Approach to Weaponization of CVE	Quick monetization	Sustained intelligence gathering
Impact	Loss of PII, potential exposure of trade secrets, impact on personal privacy and business operations	Implications to national security, targeted attacks on government organizations
Response/Containment	Requires minimizing data exfiltration and preventing ransomware deployment	Requires thorough understanding of the compromise, attacker tactics, and malware detection

Meanwhile, UNC4841 exhibited a more meticulous and targeted approach during its Barracuda ESG exploitation, seeking long-term, surreptitious access to sensitive data for intelligence purposes.

The means through which various attackers have historically acquired and leveraged zero-day exploits should inform the decision-making and prioritization for organizations that may become future targets. While there is no reliable way to defend against zero-day exploits, organizations can mitigate risk

by working to protect and segregate critical systems, while also ensuring they have the visibility needed for continued monitoring of suspicious activity.

Organizations traditionally prioritize patching by risk scores, with a higher risk score often getting patched prior to those with lower risk scores. However, evidence of active exploitation of a vulnerability should escalate patching priority,[3] and affected organizations should launch an immediate investigation into impact.

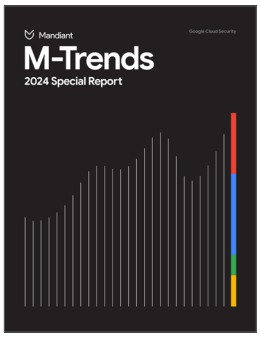
Organizations that have an existing incident response plan and broad environmental monitoring are often better prepared to assess the potential impact of a vulnerability on their environment. Layering network segmentation and logging with advanced endpoint detection and response solutions provides organizations with an efficient means through which investigations can be started and brought to a swift close.

Similarly, thoroughly evaluating the security practices and network requirements for vendors prior to deploying hardware or software into the environment allows defenders to build a quality baseline of what should be considered "normal" use. Vendor vetting also allows for the creation of comprehensive detection mechanisms as the definition of non-standard use is clarified. Any detections for non-standard use within the context of a vendor's product should be prioritized and investigated to ensure the legitimacy of the actions on which the detection fired. A blending of policy, threat intelligence, and active monitoring can act as an early warning system for attackers leveraging zero-day vulnerabilities.

Conclusion

Zero-day exploitation is no longer a niche capability accessible to only a handful of attackers, and Mandiant anticipates that the growth we have seen across the last few years will continue. The rise of zero-day exploitation by ransomware and data theft extortion groups, continued state-sponsored exploitation, and the growth of turnkey or off-the-shelf capabilities that can be purchased from commercial commercial surveillance vendors will continue to drive the identification of zero-day vulnerabilities and exploits that target them. By understanding the motivations and TTPs of attackers, organizations can build defensive strategies that prioritize the types of threats that are most likely to impact their environments. Strengthening cybersecurity posture, adopting robust vulnerability management practices, and fostering a culture of security awareness are key steps in safeguarding against zero-days. The MOVEit and Barracuda campaigns offer a stark reminder that cyber threats are not merely a nuisance, but a threat that demands our attention and action. Defenders must adopt a proactive approach to cybersecurity, recognizing that zero-day vulnerabilities are a reality and that preparation reduces their impact.

1 https://cloud.google.com/blog/topics/threat-intelligence/zero-day-moveit-data-theft
2 https://cloud.google.com/blog/topics/threat-intelligence/barracuda-esg-exploited-globally
3 https://cloud.google.com/blog/topics/threat-intelligence/putting-model-work-enabling-defenders-vulnerability-intelligence-intelligence-vulnerability-management-part-four



Read the full report: M-Trends 2024 Special Report

Google Cloud

For more information, visit cloud.google.com/security.