loginsoft

Monthly Report

Threat & Vulnerabilities Report – March 2025

Executive Summary

March 2025 witnessed a notable surge in critical vulnerabilities and ransomware activity, with several zero-day exploits actively leveraged by threat actors. A total of 32 new entries were added to the CISA Known Exploited Vulnerabilities (KEV) catalog, reflecting the expanding threat landscape. High-impact vulnerabilities were discovered across key vendors including Edimax, Google, Mozilla, Juniper, VMware, Microsoft, and Apple—highlighted by sandbox escape flaws in Chromium and Firefox that raised concerns over privilege escalation on Windows platforms.

Concurrently, ransomware groups such as Babuk2, Ransomhub, and SafePay ramped up attacks, focusing on sectors like healthcare, finance, education, and government by exploiting known vulnerabilities for initial access. These trends emphasize the urgent need for timely patching, continuous threat monitoring, and a layered, intelligence-driven cybersecurity approach to effectively defend against evolving threats.

Actively Exploited Vulnerabilities

CVE-ID	Vendor	Product	Description	Exploited as Zero-day	Abused by Malware	CISA KEV	OSS
CVE-2025-1316	Edimax	IC-7100 IP Camera	An OS Command Injection Vulnerability in the Edimax IC-7100 network camera that can be exploited by an attacker to achieve remote code execution on vulnerable devices by means of a specially crafted request	Yes	Yes	Yes	False
CVE-2025-2783	Google	Chromium Mojo	A Sandbox Escape Vulnerability in the Google Chromium Mojo on Windows arises due to logic error, where an incorrect handle is assigned under certain	Yes	Yes	Yes	False

			unspecified conditions.				
CVE-2025-2857	Mozilla	Firefox	Sandbox Escape vulnerability in Mozilla Firefox on Windows systems. It involves an incorrect handle management in the browser's inter-process communication (IPC) code, which could allow a compromised child process to obtain elevated privileges by causing the parent process to return an unintentionally powerful handle, leading to a sandbox escape.	False	False	False	False
CVE-2025-21590	Juniper	Junos OS	Improper Isolation or Compartmentalization Vulnerability in Juniper Junos OS allows a local attacker with high privileges to inject arbitrary code	Yes	Yes	Yes	False
CVE-2025-22224	VMware	ESXi and Workstation	A TOCTOU (Time-of-Check Time-of-Use) vulnerability in the VMWare ESXi and Workstation	Yes	Yes	Yes	False
CVE-2025-22225	VMware	ESXi	An Arbitrary Write Vulnerability in the VMWare ESXi	Yes	Yes	Yes	False
CVE-2025-22226	VMware	ESXi, Workstation and Fusion	An Information Disclosure Vulnerability in the VMWare	Yes	Yes	Yes	False

			ESXi, Workstation and Fusion				
CVE-2025-24201	Apple	Multiple Products	An Out-of-Bounds Write Vulnerability in the Apple's WebKit browser engine	Yes	No	Yes	False
CVE-2025-24472	Fortinet	FortiOS and FortiProxy	Authentication Bypass Vulnerability in Fortinet FortiOS and FortiProxy allows remote attackers to gain super-admin privileges	No	Yes	Yes	False
CVE-2025-24983	Microsoft	Windows	A Use-After-Free Vulnerability in Microsoft Windows Win32k	Yes	No	Yes	False
CVE-2025-24984	Microsoft	Windows	An Information Disclosure Vulnerability in Microsoft Windows NTFS	Yes	No	Yes	False
CVE-2025-24985	Microsoft	Windows	An Integer Overflow Vulnerability in the Microsoft Windows Fast FAT File System	Yes	No	Yes	False
CVE-2025-24991	Microsoft	Windows	An Out-of-Bounds Read Vulnerability in the Microsoft Windows NTFS	Yes	No	Yes	False
CVE-2025-24993	Microsoft	Windows	A Heap-Based Buffer Overflow Vulnerability in the Microsoft Windows NTFS	Yes	No	Yes	False
CVE-2025-25181	Advantive	VeraCore	An SQL Injection Vulnerability in Advantive VeraCore enables remote attackers to execute arbitrary SQL commands, potentially compromising	Yes	Yes	Yes	False

			the database and exposing sensitive information				
CVE-2025-26633	Microsoft	Windows	An Improper Neutralization Vulnerability in the Microsoft Windows Management Console (MMC)	Yes	Yes	Yes	False
CVE-2025-30066	tj-actions	changed-files GitHub Action	Embedded Malicious Code Vulnerability in tj-actions/changed-files GitHub Action	No	No	Yes	False
CVE-2025-30154	reviewdog	Action-setup GitHub Action	Embedded Malicious Code Vulnerability in the reviewdog action-setup GitHub Action	No	No	Yes	False
CVE-2025-30355	Synapse	Synapse	A Federation Denial-of-Service (DoS) Vulnerability via malformed events in Synapse Matrix homeserver implementation	No	No	No	True
CVE-2024-3400	Palo Alto Networks	PAN-OS Software	A Command Injection Vulnerability in the Palo Alto Networks PAN-OS software	Yes	Yes	Yes	True
CVE-2024-4885	Progress	WhatsUp Gold	A Path Traversal Vulnerability in the Progress WhatsUp Gold that enables an unauthenticated attacker to achieve remote code execution	No	No	Yes	False
CVE-2024-13159	Ivanti	Endpoint Manager (EPM)	Absolute Path Traversal Vulnerability in Ivanti Endpoint Manager that can	No	No	Yes	False

			be exploited by remote, unauthenticated attackers to disclose sensitive information				
CVE-2024-13160	Ivanti	EPM	Absolute Path Traversal Vulnerability in Ivanti Endpoint Manager that can be exploited by remote, unauthenticated attackers to disclose sensitive information	No	No	Yes	False
CVE-2024-13161	Ivanti	EPM	Absolute Path Traversal Vulnerability in Ivanti Endpoint Manager that can be exploited by remote, unauthenticated attackers to disclose sensitive information	No	No	Yes	False
CVE-2024-20439	Cisco	Smart Licensing Utility	Use of Static Administrative Credential Vulnerability in the Cisco Smart Licensing Utility enables an unauthenticated, remote attacker to log into affected systems.	No	No	No	False
CVE-2024-20440	Cisco	Smart Licensing Utility	Sensitive Information Disclosure Vulnerability in the Cisco Smart Licensing Utility.	No	No	No	False
CVE-2024-25600	Wordpress	Bricks Builde	The Startklar Elementor Addons WordPress	No	No	No	False

			plugin (versions up to and including 1.7.13) is vulnerable to arbitrary file uploads due to inadequate file type validation within the process function of the startklarDropZoneUploadProcess class.				
CVE-2024-27956	Wordpress	Automatic plugin	Unauthenticated SQL Injection vulnerability in ValvePress Automatic pugin. This issue affects Automatic: from n/a through 3.92.0	No	No	No	False
CVE-2024-4345	Wordpress	Startklar Elementor plugin	Startklar Elementor Addons plugin for WordPress is vulnerable to arbitrary file uploads due to insufficient file type validation in the 'process' function in the 'startklarDropZoneUploadProcess' class in versions up to, and including, 1.7.13.	No	No	No	False
CVE-2024-48248	NAKIVO	Backup and Replication	Absolute Path Traversal Vulnerability in the NAKIVO Backup and Replication enables an attacker to read arbitrary files	No	No	Yes	False
CVE-2024-50302	Linux Foundation	Linux Kernel	A Use of Uninitialized Resource	Yes	No	Yes	True

			Vulnerability in the Linux Kernel				
CVE-2024-55591	Fortinet	FortiOS and FortiProxy	Authentication Bypass Vulnerability in Fortinet FortiOS and FortiProxy allows remote attackers to gain super-admin privileges	No	Yes	Yes	False
CVE-2024-57040	TP-Link	TL-WR845N routers	Use of Hard-coded Credentials Vulnerability in the TP-Link TL-WR845N routers	Yes	No	No	False
CVE-2024-57968	Advantive	VeraCore	An Upload Validation Vulnerability in Advantive VeraCore allows remote authenticated users to upload files to unauthorized folders	Yes	Yes	Yes	False
CVE-2024-8353	GiveWP	GiveWP	The GiveWP WordPress plugin (versions up to and including 3.16.1) is vulnerable to an unauthenticated PHP Object Injection via improper deserialization of user-supplied input in parameters such as give_title and card_address	No	No	No	False
CVE-2023-20118	Cisco	RV Series Routers	A Remote Code Execution Vulnerability in the Cisco small business router models that enables an attacker to	No	Yes	Yes	False

			deploy webshell on the target router				
CVE-2022-43769	Hitachi Vantara	Pentaho Business Analytics Server	A Special Element Injection Vulnerability in Hitachi Vantara Pentaho BA Server	No	No	Yes	False
CVE-2022-43939	Hitachi Vantara	Pentaho Business Analytics Server	An Authorization Bypass Vulnerability in the Hitachi Vantara Pentaho Business Analytics Server	No	No	Yes	False
CVE-2021-20123	Draytek	VigorConnect	An unauthenticated local file inclusion vulnerability DownloadFileServlet endpoint in that enables an unauthenticated attacker to download arbitrary files with root privileges.	No	No	Yes	False
CVE-2021-20124	Draytek	VigorConnect	An unauthenticated local file inclusion vulnerability WebServlet endpoint that enables an unauthenticated attacker to download arbitrary files with root privileges.	No	No	Yes	False
CVE-2021-26855	Microsoft	Exchange Server	A Remote Code Execution Vulnerability in the Microsoft Exchange Server	Yes	Yes	Yes	False
CVE-2021-44228	Apache Server Foundation	Apache Log4j	A Remote Code Execution Vulnerability in	Yes	Yes	Yes	True

			the Apache Log4j2, caused by improper restrictions on JNDI features, allowing attackers to exploit maliciously crafted JNDI lookups and execute arbitrary code remotely.				
CVE-2020-8515	Draytek	• Vigor 3900 • Vigor2960 • Vigor300B	A Remote Code Execution Vulnerability in the DrayTek Vigor3900, Vigor2960, and Vigor300B routers	No	Yes	Yes	False
CVE-2019-9874	Sitecore	Sitecore CMS and Experience Platform (XP)	A Deserialization Vulnerability in the Sitecore CMS and Experience Platform (XP) allows an unauthenticated attacker to execute arbitrary codes.	No	No	Yes	False
CVE-2019-9875	Sitecore	Sitecore CMS and Experience Platform (XP)	A Deserialization Vulnerability in the Sitecore CMS and Experience Platform (XP) allows an authenticated attacker to execute arbitrary codes.	No	No	Yes	False
CVE-2018-8639	Microsoft	Windows	An Improper Resource Shutdown or Release Vulnerability in the Microsoft Windows Win32k	No	Yes	Yes	False
CVE-2017-12637	SAP	NetWeaver Application Server Java	Directory Traversal Vulnerability in the SAP NetWeaver	Yes	No	Yes	False

			Application Server (AS) that allows a remote attacker to read arbitrary files via a "**..**" in the query string.				

Ransomware Insights for March

The Ransomware insights were captured from various data leak sites of respective ransomware. This insight helps us to understand which industries and countries were targeted the most

Ransomware	Description	No.of Affected Organizations for March - 2025	Targeted Industries	Vulnerabilities Abused Most
Babuk2	Babuk2 ransomware, a variant of the Babuk family that surfaced around 2021, is a sophisticated form of ransomware that encrypts a victim's files and demands a ransom for decryption. Known for its double extortion tactics, Babuk2 not only encrypts data but also exfiltrates sensitive files before encryption, threatening to release the stolen data if the ransom is not paid. The ransomware employs strong encryption algorithms to lock files, making them inaccessible without a decryption key. After encryption, it leaves a ransom note with instructions on how to pay, typically in cryptocurrency, for the decryption key. Babuk2 spreads through compromised networks, often using brute-force attacks or exploiting vulnerabilities to gain access. If the ransom is not paid, the attackers may publish the stolen data on a public leak site.	85	• Healthcare • Finance • Manufacturing • Energy • Government • Retail • Legal	• Unknown
Ransomhub	Ransomhub is a self-described Ransomware-as-a-Service	71		CVE-2020-1472

	operation first disclosed in announcements on the Russian-language dark web forum RAMP in February 2024. The encryptor has versions written in C++ and the Go programming language and claims to support encryption of Windows, Linux, and ESXi devices. Initial posts announcing the group explicitly forbid attacks on the Commonwealth of Independent States, Cuba, North Korea, and China, as well as encryption of non-profit hospitals. At the time of this report, Ransomhub has publicly claimed five distinct organizations across nine posts from February 10th to March 4th on its data leak site		• Education • Construction • Government	
Akira	Akira ransomware underscored a critical security vulnerability linked to the lack of Multi-Factor Authentication (MFA). The nations experiencing the fallout encompass the United States, the United Kingdom, Canada, Australia, and South Korea. The repercussions are noteworthy, especially within pivotal domains like Services and Goods, Manufacturing, Education, and Finance.	58	• Education • Manufacture • Finance	• CVE-2020-1472 • CVE-2020-3259
safepay	SafePay is a newly emerging ransomware strain believed to be derived from leaked LockBit source code, distinguished by its ransom note titled "readme_safepay.txt" and encrypted file extensions labeled ".safepay." While bearing similarities to LockBit, SafePay's refined approach establishes it as a formidable new player in the ransomware landscape. It employs a two-phase attack strategy involving initial system infiltration followed by data encryption, often using anti-	41	• Education • Finance • Agriculture • Manufacturing • Healthcare • Logistic	• Unknown

	detection mechanisms to evade security measures. Linked to the LockBit ransomware builder, SafePay is suspected to involve experienced cybercriminals in its creation and deployment. The ransomware primarily targets payment processors and banks, posing a significant threat to financial institutions. With at least 22 victims reported so far, SafePay's sophisticated techniques for spreading and exfiltrating data underscore its potency and highlight the challenges of mitigating its impact.			
Qilin	The Qilin ransomware has been in existence since August 2022, also recognized as Agenda, has posed a substantial threat. Employing Rust and Go programming languages, this ransomware group executes intricate and elusive attack strategies. It's developed in Rust and identified as Ransom.Win32.AGENDA.THIAFBB, was discovered. Remarkably, this ransomware initially scripted in Go language was notorious for its focus on healthcare and education sectors, particularly in nations such as Thailand and Indonesia.	36	• Education • Healthcare	• Unknown
FOG	Fog ransomware, emerging in May 2024, initially targeted educational and recreational sectors by exploiting compromised VPN credentials to infiltrate systems. More recently, the group has shifted focus toward high-revenue sectors like financial services, broadening its victim base and refining tactics to maximize ransom potential. This adaptive approach underscores Fog ransomware's escalating threat, as it	30	• Education • Recreation	• CVE-2024-40711 • CVE-2024-40766

	increasingly prioritizes industries where operational disruption could drive substantial ransom demands.			
Lynx	Lynx ransomware, active since mid-2024, is a sophisticated malware operating under a ransomware-as-a-service (RaaS) model, claiming over 20 victims across various industries. It employs single and double extortion tactics, encrypting critical files with a ".lynx" extension and threatening to leak data if ransoms are unpaid, while also deleting backups like shadow copies to hinder recovery. Notably, Lynx has targeted organizations in the United States, United Kingdom, Canada, Guatemala, and Australia, with a significant attack on Romania's Electrica Group, demonstrating its capacity to disrupt critical infrastructure. The ransomware employs a hybrid encryption method, using AES for file encryption and RSA for key protection, and directs victims to Tor communication channels for ransom negotiations. Key features include targeting specific directories for encryption, terminating processes, encrypting network drives, escalating privileges, and altering system settings, such as background images. By employing these sophisticated techniques, Lynx continues to pose a serious threat to industries worldwide.	25	• Finance • Retail • Real Estate • Manufacture • Construction • Logistic	• Unknown
Inc Ransom	Inc. ransomware, which emerged in June 2023, spread through spear-phishing emails and targeted vulnerable services, such as the exploitation of CVE-2023-3519 in Citrix NetScaler.	19	• Education • Healthcare • Government sectors	• CVE-2023-3519

	Our observations indicate that Inc. ransomware has deliberately targeted a range of sectors, including healthcare, education, and government entities. This ransomware operates as a multi-extortion scheme, involving the theft of victim data and threats to release the data online unless the victim complies with their demands.			
Medusa	Emerging in 2019, the Medusa ransomware operates on a ransomware-as-a-service (RaaS) model and has been observed infecting and encrypting systems in various sectors, notably focusing on the healthcare sector. Attackers typically gain initial access through brute-force assaults on Remote Desktop Protocol (RDP), exploiting leaked RDP credentials, or employing spear-phishing tactics to acquire user credentials. Notably, ransomware affiliates have been leveraging the infrastructure of the United States, potentially indicating preparations for future attacks.	17	• Healthcare • Finance • Technology • Manufacturing	• CVE-2023-0669 • CVE-2023-27350 • CVE-2023-27351 • CVE-2023-34362 • CVE-2023-47246 • CVE-2022-2295
Rhysida	Rhysida ransomware has a new variant that provides Ransomware-as-a-service (RaaS). As of 2023, approximately 50 victims have been identified, targeting the Education, Healthcare, Manufacturing, Information Technology and Government sectors. The deployment of Rhysida involves various methods, including the use of Cobalt Strike or a similar framework, as well as phishing campaigns. Notably, we have observed the threat actor exploiting Zerologon's (CVE-2020-1472) vulnerability, a	8	• Education • Healthcare • Manufacturing • Information Technology • Government sectors	CVE-2020-1472

	critical elevation of privileges flaw in Microsoft's Netlogon Remote Protocol. Upon gaining network access, the Rhysida gang employs Living off the Land Binaries (LoLBins) techniques to execute malicious activities discreetly and avoid detection.			
Play	The Play ransomware group, also identified as Balloonfly and PlayCrypt, has significantly impacted businesses and critical infrastructure across North America, South America and Europe regions. With a primary focus on telecommunications, the group has extended its reach to healthcare, technology and media industries. It was observed that the group focused on managed service providers (MSPs) globally, using remote monitoring and management (RMM) tools to infiltrate customer systems. Their campaigns involve custom tools like "Grixba" and "VSS Copying Tool" written in .NET. Interestingly, Play ransomware affiliates prefer email communication for negotiations and do not provide Tor negotiation page links in ransom notes on compromised systems.	8	• Healthcare • Media • Technology • Telecommunication	• CVE-2021-34523 • CVE-2022-41080 • CVE-2022-41040 • CVE-2022-41082 • CVE-2018-13379 • CVE-2020-12812
Funksec	Funksec is a recently identified extortion group that has claimed 11 victims across sectors such as media, IT, education, and critical infrastructure, including healthcare, financial services, and government entities. Operating a Tor-based data leak site (DLS) created between late November and early December 2024, Funksec centralizes its ransomware activities and advertises a free DDoS tool, with indications that it may develop its own ransomware binary,	8	• Healthcare • Finance • Government • Information technology • Education	• Unknown

	showcasing its technical sophistication. The group's first known advertisement, titled "Funksec Ransomware," was posted on December 3, 2024. Funksec has targeted regions with advanced digital infrastructure, including the United States, Europe, and parts of Asia, where higher financial rewards are anticipated due to the critical nature of operations. Linked to sophisticated threat actors from Russia, China, Iran, North Korea, and other independent cybercriminal groups, Funksec leverages ransomware-as-a-service (RaaS) models and software vulnerabilities to expand its impact. Despite its capabilities, limited information is currently available regarding its tactics, techniques, and procedures (TTPs), and no direct association with other known threat groups has been identified.			
Clop	Clop ransomware is a sophisticated cyber threat first identified in 2019, known for its double-extortion tactics and targeted attacks on large organizations. Operated by the financially motivated cybercrime group TA505, Clop not only encrypts victim data but also exfiltrates sensitive information, threatening public disclosure unless a ransom is paid. The ransomware has been linked to high-profile attacks exploiting vulnerabilities in widely used software, including the MOVEit Transfer and Accellion File Transfer Appliance (FTA). Clop operators gain initial access through phishing campaigns, exploiting zero-day	7	• Healthcare • Bank • Education • Gaming • Transportation	• CVE-2024-55956 • CVE-2023-0669 • CVE-2023-27350 • CVE-2023-27351 • CVE-2023-34362 • CVE-2023-47246

	vulnerabilities, or leveraging compromised credentials.			
Bianlian	BianLian is a Golang-based ransomware that significantly threatens diverse industries, including healthcare, education and government entities. Recognizing the severity of this threat, the Cybersecurity and Infrastructure Security Agency (CISA), Federal Bureau of Investigation (FBI), and Australian Cyber Security Centre (ACSC) have collaboratively issued advisories, emphasizing the group's focus on critical infrastructure sectors in the United States and Australia. Upon infiltrating systems, the BianLian group adeptly utilizes open-source tools and command-line scripts to extract victims' data to a cloud storage controlled by attackers. Initially adopting a double-extortion model, the group shifted its strategy towards data exfiltration attacks after releasing a free decryptor.	7	• Healthcare • Banking • Utilities • Insurance	• CVE-2023-27350 • CVE-2022-27925 • CVE-2022-37042 • CVE-2021-4034 • CVE-2021-31207 • CVE-2021-34473 • CVE-2021-34523
Hunters	Hunters International, identified as a Ransomware-as-a-Service (RaaS) provider, emerged after the detection of source code sharing resemblances with the infamous Hive ransomware strain. Initial examination of the malware code revealed an estimated 60% similarity with samples from Hive ransomware version 61. Detailed technical analysis proposes a plausible scenario in which the ransomware could have been employed in activities associated with the recently dismantled Hive cartel.	6	• Healthcare • Education • Research	• Unknown

Conclusion

March 2025 highlighted a growing wave of zero-day vulnerabilities and sophisticated ransomware attacks targeting critical sectors. Active exploitation of known flaws reinforces the urgent need for timely patching and strong vulnerability management. As threats continue to evolve, proactive defense strategies and real-time threat intelligence remain key to protecting organizational assets. Loginsoft Vulnerability Intelligence (LOVI) remains dedicated to equipping organizations with the insights needed to stay ahead of emerging cyber risks.

Reference Links:

1. https://www.cisa.gov/news-events/alerts/2025/03/03/cisa-adds-five-known-exploited-vulnerabilities-catalog
2. https://www.cisa.gov/news-events/alerts/2025/03/04/cisa-adds-four-known-exploited-vulnerabilities-catalog
3. https://www.cisa.gov/news-events/alerts/2025/03/10/cisa-adds-five-known-exploited-vulnerabilities-catalog
4. https://www.cisa.gov/news-events/alerts/2025/03/11/cisa-adds-six-known-exploited-vulnerabilities-catalog
5. https://www.cisa.gov/news-events/alerts/2025/03/13/cisa-adds-two-known-exploited-vulnerabilities-catalog
6. https://www.cisa.gov/news-events/alerts/2025/03/18/cisa-adds-two-known-exploited-vulnerabilities-catalog
7. https://www.cisa.gov/news-events/alerts/2025/03/19/cisa-adds-three-known-exploited-vulnerabilities-catalog
8. https://www.cisa.gov/news-events/alerts/2025/03/24/cisa-adds-one-known-exploited-vulnerability-catalog
9. https://www.cisa.gov/news-events/alerts/2025/03/26/cisa-adds-two-known-exploited-vulnerabilities-catalog
10. https://www.cisa.gov/news-events/alerts/2025/03/27/cisa-adds-one-known-exploited-vulnerability-catalog
11. https://www.cisa.gov/news-events/alerts/2025/03/27/cisa-adds-one-known-exploited-vulnerability-catalog
12. https://www.cisa.gov/news-events/alerts/2025/03/31/cisa-adds-one-known-exploited-vulnerability-catalog
13. https://www.cisa.gov/news-events/alerts/2025/03/31/cisa-adds-one-known-exploited-vulnerability-catalog
14. https://www.kaspersky.co.in/blog/forum-troll-apt-with-zero-day-vulnerability/28692/

15. https://www.microsoft.com/en-us/security/blog/2021/03/02/hafnium-targeting-exchange-servers/
16. https://www.picussecurity.com/resource/blog/simulating-and-preventing-cve-2021-44228-apache-log4j-rce-exploits
17. https://www.quorumcyber.com/threat-intelligence/zero-day-vulnerabilities-in-vmware-esxi-workstation-and-fusion-exploited/
18. https://asec.ahnlab.com/en/47455/
19. https://blog.xlab.qianxin.com/large-scale-botnet-airashi-en/
20. https://www.akamai.com/blog/security-research/march-edimax-cameras-command-injection-mirai
21. https://patchstack.com/articles/new-year-new-threats-q1-2025s-most-exploited-wordpress-vulnerabilities/

loginsoft

Connect with us

linkedin.com/loginsoft

x.com/loginsoft_inc

www.loginsoft.com