loginsoft

Monthly Report

Threat & Vulnerabilities Report – April 2025

Executive Summary

As threat actors evolve and refine their techniques, tactics and procedures, April showcased a rapidly escalating threat landscape: one where vulnerabilities are not just active but increasingly weaponized and exploited at an alarming pace. From enterprise software to consumer devices, no platform was spared as exploitation campaigns grew sharper and more opportunistic.

This month, 15 vulnerabilities were added to the CISA's Known Exploited Vulnerabilities (KEV) catalog, spanning a broad mix of technologies. Key vendors like Microsoft, Apple, and Google each accounted for two vulnerabilities, while SonicWall, Ivanti, CrushFTP and others rounded out the list with one each, revealing how threat actors are casting wide nets across ecosystems.

Perhaps most alarming, 9 of these vulnerabilities were exploited as zero-days, highlighting a growing gap between vulnerability disclosure and real-world attack.

Notorious ransomware groups Akira, Play, Qilin, and Lynx, have ramped up their operations, zeroing in on high-value targets in the healthcare and IT manufacturing sectors. These cybercriminals are not just opportunistic; they employ advanced, multi-faceted attack strategies that exploit vulnerabilities to breach defenses, leaving organizations grappling with crippling data loss and operational shutdowns.

Actively Exploited Vulnerabilities

CVE-ID	Vendor	Product	Description	Exploited as Zero-day	Abused by Malware	CISA KEV	OSS
CVE-2025-0282	Ivanti	• Connect Secure • Policy Secure • ZTA Gateway	A Stack-Based Buffer Overflow Vulnerability in the Ivanti Connect Secure, Policy Secure and ZTA Gateways that can enable unauthenticated remote code execution.	Yes	Yes	Yes	False
CVE-2025-1976	Brocade Communications Systems	Brocade Fabric OS	A Privilege Escalation via IP Address Validation Flaw in the Brocade Fabric OS that enables a local user with admin privileges to execute arbitrary code with full root privileges	No	No	Yes	False
CVE-2025-2825	CrushFTP	CrushFTP	Improper Authentication vulnerability in CrushFTP	No	No	No	False
CVE-2025-3102	Brainstorm Force	OttoKit WordPress plugin	An Authorization Bypass Vulnerability in the OttoKit WordPress plugin (previously known as SureTriggers) could allow attackers to create administrator-level accounts in specific	No	No	No	False

			scenarios, potentially giving them full control over vulnerable websites.				
CVE-2025-3928	Commvault	Web Server	An Unspecified Vulnerability in the Commvault Web Server that enables a remote, authenticated attacker to create and execute webshells	Yes	No	Yes	False
CVE-2025-22457	Ivanti	• Connect Secure • Policy Secure • ZTA Gateway	A Stack-Based Buffer Overflow Vulnerability in the Ivanti Connect Secure, Policy Secure and ZTA gateways.	No	Yes	Yes	False
CVE-2025-24054	Microsoft	Windows	A Hash Disclosure Spoofing Vulnerability in the Microsoft Windows NTLM enables an unauthorized attacker to perform spoofing over a network.	No	No	Yes	False
CVE-2025-24813	Apache Software Foundation	Tomcat	A Path Equivalence Vulnerability in the Apache Tomcat allows attackers to gain control of servers using a simple PUT request.	No	No	Yes	True
CVE-2025-29824	Microsoft	Windows	A Use-After-Free Vulnerability was identified in the Microsoft Windows Common Log File System (CLFS) Driver.	Yes	Yes	Yes	False
CVE-2025-30406	Gladinet	CentreStack	A Use of Hard-Coded Cryptographic Key Vulnerability in Gladinet CentreStack affects the way the application manages key used for ViewState integrity verification.	No	No	Yes	False
CVE-2025-31103	a-blog cms	a-blog cms	An Untrusted Data Deserialization Vulnerability in a-blog cms.	No	No	No	False
CVE-2025-31161	CrushFTP	CrushFTP	An Improper Authentication Vulnerability in the CrushFTP allows remote, unauthenticated attackers to impersonate users and perform privileged actions.	No	No	Yes	False
CVE-2025-31200	Apple	Multiple Products	A Memory Corruption Vulnerability in Apple's iOS, iPadOS, macOS, and other platforms enables	Yes	No	Yes	False

			remote code execution when a specially crafted media file containing a malicious audio stream is processed.				
CVE-2025-31201	Apple	Multiple Products	An Arbitrary Read and Write Vulnerability in Apple iOS, iPadOS, macOS, and other Apple products enables an attacker to bypass Pointer Authentication.	Yes	No	Yes	False
CVE-2025-31324	SAP SE	SAP NetWeaver Visual Composer	An Unauthorized File Upload Vulnerability in the SAP NetWeaver Visual Composer, specifically within the Metadata Uploader component.	Yes	No	Yes	False
CVE-2025-32432	Craft CMS	Craft CMS	A Remote Code Execution in the Craft CMS enables attackers to send specially crafted requests	Yes	No	No	True
CVE-2025-42599	QUALITIA	Active! mail 6	A Stack Based Buffer Overflow Vulnerability in the Active! Mail 6 allows a remote, unauthenticated attacker to execute arbitrary code or cause a denial-of-service (DoS) condition by sending a specially crafted request.	Yes	No	Yes	False
CVE-2024-4345	wshberlin	Startklar Elementor Addons plugin for WordPress	The Startklar Elementor Addons plugin allows unauthenticated attackers to upload arbitrary files due to weak validation in the startklarDropZoneUploadProcess class	No	No	No	False
CVE-2024-8353	GiveWP	Donation Plugin and Fundraising Platform	An unauthenticated PHP Object Injection vulnerability in GiveWP plugin exploitable via parameters like give_title	No	No	No	False
CVE-2024-11859	ESET	ESET Products	DLL Search Order Hijacking Vulnerability in the ESET products allows an attacker with administrator privileges to load a malicious dynamic-link library and execute its code	No	Yes	No	False
CVE-2024-21762	Fortinet	FortiOS	An Out-of-Bounds Write Vulnerability in the Fortinet FortiOS that enables a remote unauthenticated attacker to execute	No	Yes	Yes	False

			commands via specially crafted HTTPS requests.				
CVE-2024-25600	Codeer Limited	Bricks Builder	Unauthenticated Remote Code Execution vulnerability in Codeer Limited Bricks Builder	No	No	No	False
CVE-2024-27956	ValvePress	WordPress Plugin	Unauthenticated SQL Injection Vulnerability in ValvePress Automatic	No	No	No	False
CVE-2024-38475	SonicWall	SMA 100 Series	A Path Traversal Vulnerability in the SonicWall SMA 100 Series	No	No	No	True
CVE-2024-53150	Google	Android	An Out-of-Bounds Vulnerability in the USB sub-component of Kernel that can lead to information disclosure.	Yes	No	Yes	True
CVE-2024-53197	Google	Android	An Out-of-Bounds Vulnerability in the USB sub-component of Kernel that can lead to information disclosure.	Yes	No	Yes	True
CVE-2024-58136	Yii 2	Yii 2 PHP Framework	An Improper Protection of Alternate Path Vulnerability in the PHP web application framework Yii 2.	No	No	No	True
CVE-2023-27997	Fortinet	• FortiOS • FortiProxy	An SSL-VPN Heap-Based Buffer Overflow Vulnerability in the Fortinet FortiOS and FortiProxy that enables an unauthenticated remote attacker to execute commands via specially crafted requests.	No	Yes	Yes	False
CVE-2023-44221	SonicWall	SMA 100 Series	A Post-Authentication OS Command Injection Vulnerability has been identified in the SonicWall SMA100 SSL-VPN Management Interface	No	No	No	False
CVE-2022-42475	Fortinet	FortiOS	A Heap-Based Buffer Overflow Vulnerability in the Fortinet FortiOS that enables an unauthenticated remote attacker to execute arbitrary commands via specially crafted requests	No	Yes	Yes	False
CVE-2021-20035	SonicWall	SMA100 Appliances	An OS Command Injection Vulnerability in the SonicWall SMA100 Appliances management interface.	No	No	Yes	False

CVE-2019-0708	Microsoft	Windows	A Remote Code Execution Vulnerability in the Microsoft Remote Desktop Services	No	Yes	Yes	False
CVE-2018-0171	Cisco	IOS IOS XE	Remote Code Execution Vulnerability in the Cisco IOS and IOS XE software that can allow an remote attacker to trigger a reload on the affected device and cause a denial-of-service (DoS) condition.	No	Yes	Yes	False
CVE-2017-11882	Microsoft	Office	A Memory Corruption Vulnerability in Microsoft Office that enables remote code execution in the context of the current user	No	Yes	Yes	False

Ransomware Insights for April

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 April - 2025	Targeted Industries	Vulnerabilities Abused Most
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.	65	• Education • Manufacture • Finance	• CVE-2020-1472 • CVE-2020-3259
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	34	• Healthcare • Media • Technology • Telecommunication	• CVE-2022-41040 • CVE-2022-41080 • CVE-2022-41082 • CVE-2021-34523 • CVE-2020-12812 • CVE-2018-13379

	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.			
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.	33	• Education • Healthcare	Unknown
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	27	• Finance • Retail • Real Estate • Manufacture • Construction • Logistic	Unknown

	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.			
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.	18	• Healthcare • Finance • Manufacturing • Energy • Government • Retail • Legal	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. Our observations indicate that Inc. ransomware has deliberately targeted a range of sectors,	16	• Education • Healthcare • Government sectors	• CVE-2023-3519

	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.	14	• Healthcare • Finance • Technology • Manufacturing	• CVE-2023-0669 • CVE-2023-27350 • CVE-2023-27351 • CVE-2023-34362 • CVE-2023-47246 • CVE-2022-2295
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.	13	• Healthcare • Education • Research	Unknown
Lockbit3	Operating since 2019, LockBit ransomware, previously known as ABCD, originated from the Megacortex family and spread through diverse channels such as RDP attacks, phishing, and exploiting public-facing applications. The most recent	12	• Education • Healthcare • Technology • Manufacture • Utilities • Construction • Entertainment	• CVE-2024-1708 • CVE-2024-1709 • CVE-2023-4966 • CVE-2023-20269 • CVE-2023-27350 • CVE-2023-27351 • CVE-2023-40044

	version, LockBit 3.0, functions as a ransomware-as-a-service model.			• CVE-2022-36537 • CVE-2022-41082
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 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.	9	• Education • Healthcare • Manufacturing • Information Technology • Government sectors	• CVE-2020-1472

Conclusion

The message is clear: reactive security measures no longer suffice in today's fast-paced, ever-evolving cyber threat landscape. As zero-day exploits become a standard weapon for threat actors, organizations must pivot to a proactive security posture. This requires accelerating threat detection, adopting smarter patching strategies, and implementing layered defense mechanisms to outpace cybercriminals. Loginsoft Vulnerability Intelligence (LOVI) is the key to this shift. By providing real-time, actionable insights, LOVI empowers organizations to stay ahead of emerging risks, strengthen their defenses, and proactively protect their critical assets. With LOVI, businesses can transform their cybersecurity approach ensuring resilience against current threats and future-proofing their defenses.

Sources Cited:

1. https://www.cisa.gov/news-events/alerts/2025/04/28/cisa-adds-three-known-exploited-vulnerabilities-catalog
2. https://www.cisa.gov/news-events/alerts/2025/04/28/cisa-adds-three-known-exploited-vulnerabilities-catalog
3. https://www.cisa.gov/news-events/alerts/2025/04/16/cisa-adds-one-known-exploited-vulnerability-catalog
4. https://www.cisa.gov/news-events/alerts/2025/04/09/cisa-adds-two-known-exploited-vulnerabilities-catalog
5. https://www.cisa.gov/news-events/alerts/2025/04/08/cisa-adds-two-known-exploited-vulnerabilities-catalog
6. https://www.cisa.gov/news-events/alerts/2025/04/04/cisa-adds-one-vulnerability-kev-catalog
7. https://blogs.jpcert.or.jp/en/2025/04/dslogdrat.html
8. https://asec.ahnlab.com/en/87554/
9. https://securelist.com/toddycat-apt-exploits-vulnerability-in-eset-software-for-dll-proxying/116086/
10. https://www.microsoft.com/en-us/security/blog/2025/04/08/exploitation-of-clfs-zero-day-leads-to-ransomware-activity/
11. https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0018

loginsoft

Connect with us

linkedin.com/loginsoft

x.com/loginsoft_inc

www.loginsoft.com