loginsoft

Monthly Report

Threat & Vulnerabilities Report – May 2025

Executive Summary

As cyber threats continue to evolve at breakneck speed, May emerged as a critical month marked by aggressive exploitation of zero-day vulnerabilities. A total of 25 new vulnerabilities were added to CISA's Known Exploited Vulnerabilities (KEV) catalog, reflecting a growing trend where attackers rapidly weaponize flaws before patches become widely available. Alarmingly, 15 of these vulnerabilities were exploited as zero-days, highlighting the increasing sophistication and preparedness of threat actors.

Among the most impactful were five Microsoft vulnerabilities, all exploited prior to their disclosure and only addressed during May's Patch Tuesday updates. Ivanti also found itself in the crosshairs, with two of its flaws leveraged in targeted zero-day attacks, likely part of state-linked espionage operations.

In the physical security space, GeoVision's surveillance systems were compromised through two exploited vulnerabilities, emphasizing that threats are no longer confined to traditional IT assets. Other affected vendors in this month's threat landscape included Samsung, Fortinet, Google, Apache, and SonicWall, demonstrating a broad attack surface that spans across cloud, enterprise, and consumer technologies.

Ransomware operators such as Qilin, Play and Akira have significantly intensified their campaigns, with a sharp focus on critical sectors like healthcare, educational, and IT manufacturing. These threat actors are far from random attackers; they utilize sophisticated, coordinated techniques, often chaining multiple vulnerabilities to gain access, establish persistence, and maximize impact.

Actively Exploited Vulnerabilities

CVE-ID	Vendor	Product	Description	Exploited as Zero-day	Abused by Malware	CISA KEV	OSS
CVE-2025-3248	Langflow	Langflow	A Missing Authentication Vulnerability in the Langflow that enables an unauthenticated remote attacker to execute arbitrary code via crafted HTTP requests.	No	No	Yes	True
CVE-2025-4427	Ivanti	Endpoint Manager Mobile	An Authentication Bypass Vulnerability in the Ivanti Endpoint Manager Mobile allows attackers to access protected resources without proper credentials.	Yes	No	Yes	False
CVE-2025-4428	Ivanti	Endpoint Manager Mobile	A Remote Code Execution Vulnerability in the Ivanti Endpoint Manager Mobile allows attackers to execute	Yes	No	Yes	False

			arbitrary code on the target system.				
CVE-2025-4632	Samsung	MagicINFO 9 Server	A Path Traversal Vulnerability in the MagicINFO 9 Server that enables an attacker to write arbitrary file as system authority.	Yes	Yes	Yes	False
CVE-2025-4664	Google	Chrome	An Insufficient Policy Loader Vulnerability in the Google Chromium Loader	Yes	No	Yes	False
CVE-2025-27007	Brainstorm Force	OttoKit	An Unauthenticated Privilege Escalation Vulnerability in the OttoKit WordPress Plugin could allow an attacker to gain full control of the affected website.	No	No	No	False
CVE-2025-27363	FreeType	FreeType	An Out-of-Bounds Write Vulnerability in the FreeType font rendering library could result in arbitrary code execution.	Yes	No	Yes	True
CVE-2025-27920	Srimax	Output Messenger	A Directory Traversal Vulnerability in the Srimax Output Messenger that enables an attacker to access sensitive leading to arbitrary file access.	Yes	Yes	Yes	False
CVE-2025-30397	Microsoft	Windows	A Type Confusion Vulnerability in the Windows scripting engine	Yes	No	Yes	False
CVE-2025-30400	Microsoft	Windows	An Use-After-Free Vulnerability in the Microsoft Windows DWM Core Library.	Yes	No	Yes	False
CVE-2025-32701	Microsoft	Windows	A Use-After-Free Vulnerability in the Windows Common Log File System (CLFS) Driver	Yes	No	Yes	False
CVE-2025-32706	Microsoft	Windows	A Heap-Based Buffer Overflow Vulnerability in the Windows Common Log File System (CLFS) Driver	Yes	No	Yes	False
CVE-2025-32709	Microsoft	Windows	A Use-After-Free Vulnerability in the Windows ancillary function driver for WinSock	Yes	No	Yes	False
CVE-2025-32756	Fortinet	• FortiFone • FortiVoice • FortiNDR • FortiMail	A Stack-Based Buffer Overflow Vulnerability in Fortinet multiple products enable a remote unauthenticated attacker to execute arbitrary code	Yes	No	Yes	False

CVE-2025-32819	SonicWall	SMA 100 series	An Arbitrary File Deletion Vulnerability in the SMA 100 series allows a remote attacker with SSLVPN user privileges to bypass path traversal protections and delete critical system files.	No	No	No	False
CVE-2025-34028	Commvault	Command Center	A Path Traversal Vulnerability in the Commvault Command Center that enables a remote, unauthenticated attacker to execute arbitrary code.	No	No	Yes	False
CVE-2025-42999	SAP	Netweaver	A Deserialization Vulnerability in the SAP NetWeaver Visual Composer development server	Yes	No	Yes	False
CVE-2025-47729	TeleMessage	TM SGNL	A Hidden Functionality Vulnerability in the TeleMessage TM SGNL	Yes	No	Yes	False
CVE-2024-6047	GeoVision	Multiple Devices	An OS Command Injection Vulnerability that enables a remote, unauthenticated attacker to inject and execute arbitrary system commands.	No	Yes	Yes	False
CVE-2024-7399	Samsung	MagicINFO 9 server	A Path Traversal Vulnerability in the server component of Samsung MagicINFO solution that enables an attacker to write arbitrary file as system authority.	No	Yes	No	False
CVE-2024-11120	GeoVision	Multiple Devices	An OS Command Injection Vulnerability that enables a remote, unauthenticated attacker to inject and execute arbitrary system commands.	No	Yes	Yes	False
CVE-2024-11182	MDaemon	Email Server	A Cross-Site Scripting (XSS) Vulnerability in the MDaemon Email Server that enables a remote attacker to load arbitrary JavaScript code via an HTML e-mail message.	Yes	Yes	Yes	False
CVE-2024-12987	DrayTek	Vigor Routers	An OS Command Injection Vulnerability in the DrayTek Vigor routers	No	Yes	Yes	False
CVE-2024-27443	Synacor	Zimbra Collaboration Suite	A Cross-Site Scripting (XSS) Vulnerability in the Zimbra Collaboration Suite (ZCS)	No	No	Yes	False

			that can lead to execution of arbitrary JavaScript code.				
CVE-2024-38475	Apache	HTTP Server	An Improper Escaping of Output Vulnerability in Apache HTTP Server that can lead to code execution or source code disclosure.	No	No	Yes	True
CVE-2024-58136	Yiiframework	Yii	An Improper Protection of Alternate Path Vulnerability in the PHP web application framework Yii 2	No	No	Yes	True
CVE-2023-38950	ZKTeco	BioTime	A Path Traversal Vulnerability in the ZKTeco Biotime that enables an unauthenticated attacker to read arbitrary files	No	No	Yes	False
CVE-2023-44221	SonicWall	SMA100 Appliances	An OS Command Injection Vulnerability in the SonicWall SMA100 Appliances	No	No	Yes	True
CVE-2023-20118	Cisco	RV Series Routers	A Command Injection Vulnerability in the Cisco Small Business RV Series Routers enables authenticated, remote attackers to gain root level privileges and access unauthorized data.	No	Yes	Yes	False

Ransomware Insights for May

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 May - 2025	Targeted Industries	Vulnerabilities Abused Most
Qilin	The Qilin ransomware has been in existence since August 2022, also recognized as Agenda, and has posed a substantial threat. Employing Rust and Go programming languages, this ransomware group executes intricate and elusive attack strategies. It developed in Rust and identified as Ransom.Win32.AGENDA.THIAFBB, was discovered. Remarkably, this ransomware initially scripted in Go language was notorious for	54	• Education • Healthcare	• CVE-2025-31324 • CVE-2023-27532

	its focus on healthcare and education sectors, particularly in nations such as Thailand and Indonesia.			
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.	42	• Healthcare • Media • Technology • Telecommunication	• CVE-2022-41040 • CVE-2022-41080 • CVE-2022-41082 • CVE-2021-34523 • CVE-2020-12812 • CVE-2018-13379
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.	35	• 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	24	• Education • Finance • Agriculture • Manufacturing • Healthcare • Logistic	Unknown

	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-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.			
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, 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.	16	• Education • Healthcare • Government sectors	• CVE-2023-3519
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	12	• Finance • Retail • Real Estate • Manufacture • Construction • Logistic	Unknown

	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.			
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.	11	• 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 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
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.	5	• Healthcare • Education • Research	Unknown
Blacksuit	BlackSuit ransomware is designed to affect both Windows and Linux operating systems, exhibiting notable similarities with the Royal ransomware. The resemblance between BlackSuit and Royal extends to their utilization of OpenSSL's AES encryption and shared	3	• Finance • Government • Telecommunications • Manufacture • Healthcare • Education	Unknown

	intermittent encryption techniques, ensuring a rapid and effective encryption process for victim files. Following the encryption of files on a targeted system, BlackSuit adds the .blacksuit extension to the encrypted files and delivers its ransom note.			

Conclusion:

The takeaway from May's surge in zero-day exploitation is unmistakable: reactive security is no longer enough. As critical flaws in products from Microsoft, Ivanti, GeoVision, and others are actively abused, the need for a proactive, intelligence-driven defense has never been more urgent. This is where Loginsoft Vulnerability Intelligence (LOVI) steps in. By offering timely, high-confidence threat intelligence, LOVI equips security teams with the foresight needed to predict exploitation patterns, prioritize critical vulnerabilities, and proactively close gaps in their attack surface. Rather than reacting to incidents, organizations using LOVI can adopt a forward-leaning security posture that ensures operational continuity and long-term resilience in the face of evolving cyber threats. With LOVI, you're not just reacting, you're outmaneuvering the threat.

External References:

- https://www.cisa.gov/news-events/alerts/2025/05/05/cisa-adds-one-known-exploited-vulnerability-catalog
- https://www.cisa.gov/news-events/alerts/2025/05/01/cisa-adds-two-known-exploited-vulnerabilities-catalog
- https://www.cisa.gov/news-events/alerts/2025/05/02/cisa-adds-two-known-exploited-vulnerabilities-catalog
- https://www.cisa.gov/news-events/alerts/2025/05/19/cisa-adds-six-known-exploited-vulnerabilities-catalog
- https://www.cisa.gov/news-events/alerts/2025/05/15/cisa-adds-three-known-exploited-vulnerabilities-catalog
- https://www.cisa.gov/news-events/alerts/2025/05/06/cisa-adds-one-known-exploited-vulnerability-catalog
- https://www.cisa.gov/news-events/alerts/2025/05/14/cisa-adds-one-known-exploited-vulnerability-catalog
- https://www.cisa.gov/news-events/alerts/2025/05/13/cisa-adds-five-known-exploited-vulnerabilities-catalog

- https://blog.sekoia.io/vicioustrap-infiltrate-control-lure-turning-edge-devices-into-honeypots-en-masse/
- https://www.fortinet.com/blog/threat-research/new-rust-botnet-rustobot-is-routed-via-routers
- https://www.fortinet.com/blog/threat-research/new-rust-botnet-rustobot-is-routed-via-routers
- https://thehackernews.com/2025/05/samsung-patches-cve-2025-4632-used-to.html
- https://www.akamai.com/blog/security-research/active-exploitation-mirai-geovision-iot-botnet
- https://www.microsoft.com/en-us/security/blog/2025/05/12/marbled-dust-leverages-zero-day-in-output-messenger-for-regional-espionage/