loginsoft

Monthly Report

Threat & Vulnerabilities Report – May 2026

Executive Summary

May 2026 proved to be a consequential month in the cybersecurity calendar - one that underscored just how broad and relentless the modern threat landscape has become.

CISA's Known Exploited Vulnerabilities catalog grew by 21 entries, a telling sign that attackers aren't just chasing zero-days, they're digging up older wounds that never got properly patched. Microsoft led the vendor tally with 7 CVEs, a mix of fresh disclosures and long-standing flaws finally catching up to unpatched systems. Palo Alto Networks contributed 2 entries, while a cross-section of major vendors - Langflow, Trend Micro, Cisco, Ivanti, and Linux rounded out the catalog additions, painting a picture of systemic exposure across enterprise and infrastructure stacks.

What makes this month particularly interesting is the variety of products seeing active exploitation. Alongside expected enterprise targets, threat actors were observed going after Ghost CMS, Burst Statistics, Digital Knowledge, and the AI agent framework PraisonAI, a clear signal that attackers are expanding their hunting grounds into developer tools, content platforms, and emerging AI infrastructure.

On the ransomware front, Qilin cemented its dominance with 110 confirmed victim organizations, the highest of any group this month by a considerable margin. TheGentlemen, a name that's been turning heads, made a striking showing with 77, while DragonForce held steady at 55. Akira and IncRansom continued their persistent operations, keeping pressure on mid-market and enterprise targets alike.

Vulnerabilities added to the CISA KEV catalog in May 2026

CVE-ID	Vendor	Product	Description	Exploited as Zero-day	Abused by Malware	OSS
CVE-2026-0257	Palo Alto Networks	PAN-OS	Authentication Bypass vulnerability in Palo Alto Networks PAN-OS that allows attackers to bypass security restrictions and establish an unauthorized VPN connection.	No	No	False
CVE-2026-0300	Palo Alto Networks	PAN-OS	Out-of-Bounds Write vulnerability in Palo Alto Networks PAN-OS in the User-ID Authentication Portal (aka Captive Portal) service that can allow an unauthenticated attacker to execute arbitrary code with root privileges on the PA-Series and VM-Series firewalls by sending specially crafted packets.	Yes	Yes	False
CVE-2026-6973	Ivanti	Endpoint Manager Mobile (EPMM)	Remote Code Execution vulnerability in Ivanti Endpoint Manager Mobile (EPMM) that allows a remotely authenticated	Yes	No	False

CVE-ID	Vendor	Product	Description	Exploited as Zero-day	Abused by Malware	OSS
			user with administrative access to achieve remote code execution.			
CVE-2026-8398	Daemon	Daemon Tools Lite	Embedded Malicious Code vulnerability in Daemon Tools that has a high impact on confidentiality, integrity, and availability.	No	Yes	False
CVE-2026-9082	Drupal	Core	SQL Injection vulnerability in Drupal Core that could allow for privilege escalation and remote code execution via specially crafted requests sent with the database abstraction API.	No	No	True
CVE-2026-20182	Cisco	Catalyst SD-WAN	Authentication Bypass vulnerability in Cisco Catalyst SD-WAN that allows an unauthenticated, remote attacker to bypass authentication and obtain administrative privileges on an affected system.	Yes	Yes	False
CVE-2026-31431	Linux	Kernel	Privilege Escalation vulnerability in Linux Kernel	No	No	False
CVE-2026-34926	Trend Micro	Apex One	Directory Traversal vulnerability in Trend Micro Apex One that could allow a pre-authenticated local attacker to modify a key table on the server to inject malicious code to deploy to agents on affected installations.	Yes	No	False
CVE-2026-41091	Microsoft	Defender	Link Following vulnerability in Microsoft Defender that allows an authorized attacker to elevate privileges locally.	Yes	No	False
CVE-2026-42208	BerriAI	LiteLLM	SQL Injection vulnerability in BerriAI LiteLLM that allows an attacker to read data from the proxy's database and potentially modify it, leading to unauthorized access to the proxy and the credentials it manages.	No	No	True
CVE-2026-42897	Microsoft	Microsoft	Cross-Site Scripting vulnerability in Microsoft Exchange Server during web page generation in Outlook Web Access and when certain interaction conditions are met, arbitrary JavaScript can be executed in the browser context.	Yes	No	False
CVE-2026-45321	TanStack	TanStack	Authentication Bypass vulnerability in TanStack that allowed malicious versions of the product to be published to the	No	Yes	True

CVE-ID	Vendor	Product	Description	Exploited as Zero-day	Abused by Malware	OSS
			npm registry to publish credential-stealing malware under a trusted identity.			
CVE-2026-45498	Microsoft	Defender	Denial Of Service vulnerability in Microsoft Defender	Yes	No	False
CVE-2026-48027	Nx	Nx Console	Embedded Malicious Code vulnerability in Nx Console that allowed a malicious version of Nx Console to be published.	No	No	False
CVE-2026-48172	LiteSpeed	cPanel Plugin	Privilege Escalation vulnerability in LiteSpeed cPanel Plugin that is exposed via the user-end cPanel plugin, which can be abused by any cPanel user account to execute arbitrary scripts with root privileges.	Yes	No	False
CVE-2025-34291	Langflow	Langflow	Origin Validation Error vulnerability in Langflow in which an overly permissive CORS configuration combined with a refresh token cookie configured as ***SameSite=None*** allows a malicious webpage to perform cross-origin requests that include credentials and successfully call the refresh endpoint.	No	Yes	True
CVE-2010-0249	Microsoft	Internet Explorer	Use-After-Free vulnerability in Microsoft Internet Explorer that could allow remote attackers to execute arbitrary code by accessing a pointer associated with a deleted object. The impacted product could be end-of-life (EoL) and/or end-of-service (EoS). Users should discontinue product utilization.	No	No	False
CVE-2010-0806	Microsoft	Internet Explorer	Use-After-Free vulnerability in Microsoft Internet Explorer that could allow remote attackers to execute arbitrary code via vectors involving access to an invalid pointer after the deletion of an object. The impacted product could be end-of-life (EoL) and/or end-of-service (EoS). Users should discontinue product utilization.	No	Yes	False
CVE-2009-1537	Microsoft	DirectX	Null Byte Overwrite vulnerability in Microsoft DirectX in the QuickTime Movie Parser Filter in quartz.dll in DirectShow which could allow remote attackers to	No	No	False

CVE-ID	Vendor	Product	Description	Exploited as Zero-day	Abused by Malware	OSS
			execute arbitrary code via a crafted QuickTime media file.			
CVE-2009-3459	Adobe	Acrobat and Reader	Buffer Overflow vulnerability in Adobe Acrobat and Reader that could allow remote attackers to execute arbitrary code via a crafted PDF file that triggers memory corruption.	No	No	False
CVE-2008-4250	Microsoft	Windows	Buffer Overflow vulnerability in Microsoft Windows Server Service that allows remote attackers to execute arbitrary code via a crafted RPC request that triggers an overflow during path canonicalization.	No	Yes	False

Actively Exploited Vulnerabilities in May 2026

CVE-ID	Vendor	Product	Description	Exploited as Zero-day	Abused by Malware	OSS
CVE-2026-5426	Digital Knowledge	KnowledgeDeliver	Unauthenticated Remote Code Execution vulnerability in Digital Knowledge KnowledgeDeliver deployments that allows adversaries to circumvent ViewState validation mechanisms and achieve remote code execution via malicious ViewState deserialization attacks.	No	Yes	False
CVE-2026-8181	Burst Statistics B.V.	Burst Statistics – Privacy-Friendly WordPress Analytics (Google Analytics Alternative)	Authentication Bypass in Burst Statistics WordPress plugin that allows an attacker to obtain admin-level access to websites.	No	No	False
CVE-2026-8732	WP Maps Pro	WP Maps Pro	Unauthenticated Privilege Escalation vulnerability in the WP Maps Pro plugin for WordPress that allows unauthenticated users to gain full administrative control.	No	No	False
CVE-2026-26980	Ghost	Ghost CMS	SQL Injection vulnerability in Ghost's Content API that could allow an unauthenticated attacker to read arbitrary data from the database.	No	No	True

CVE-ID	Vendor	Product	Description	Exploited as Zero-day	Abused by Malware	OSS
CVE-2026-29014	MetInfo	MetInfo	PHP Code Injection vulnerability in MetInfo content management system that could result in arbitrary code execution.	No	No	False
CVE-2026-32661	Canon	GUARDIANWALL MailSuite	Stack-Based Buffer Overflow vulnerability in GUARDIANWALL MailSuite that allows an attacker to execute arbitrary code on the affected systems.	No	No	False
CVE-2026-42945	F5 Networks	NGINX Plus and NGINX Open	Heap Buffer Overflow vulnerability in the NGINX in the ***ngx_http_rewrite_module*** module.	No	No	False
CVE-2026-43284	Linux	Kernel	Local Privilege Escalation vulnerability in Linux Kernel that allows an unprivileged user to escalate permissions to root.	Yes	No	False
CVE-2026-43500	Linux	Kernel	Local Privilege Escalation vulnerability in Linux Kernel that allows an unprivileged user to escalate permissions to root.	Yes	No	False
CVE-2026-44338	PraisonAI	PraisonAI	Authentication Bypass vulnerability in PraisonAI, an open-source multi-agent orchestration framework.	No	No	True
CVE-2024-9643	Four-Faith	F3x36 router	Authentication Bypass vulnerability in Four-Faith F3x36 router that allows an attacker with knowledge of the credentials to gain administrative access via crafted HTTP requests.	No	No	False
CVE-2021-26855	Microsoft	Exchange Server	Remote Code Execution vulnerability in Microsoft Exchange Server	No	Yes	False
CVE-2021-26857	Microsoft	Exchange Server	Remote Code Execution vulnerability in Microsoft Exchange Server	No	Yes	False
CVE-2021-26858	Microsoft	Exchange Server	Remote Code Execution vulnerability in Microsoft Exchange Server	No	Yes	False
CVE-2021-27065	Microsoft	Exchange Server	Remote Code Execution vulnerability in Microsoft Exchange Server	No	Yes	False

Ransomware Insights for May 2026

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 in May 2026	Targeted Industries	Vulnerabilities abused most
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.	110	• Manufacturing • Healthcare • Technology • Business Services • Financial Services	• CVE-2023-4966 • CVE-2023-20269 • CVE-2023-27350 • CVE-2023-27351 • CVE-2023-40044 • CVE-2022-36537 • CVE-2022-41082
TheGentlemen	The Gentlemen ransomware campaign, which surfaced in the summer of 2025, exemplifies the rapid evolution of modern cyber threats. It combines advanced techniques with persistent, targeted operations, leveraging custom defense-evasion tools, adapting to existing security controls, and exploiting both legitimate and vulnerable components to effectively bypass layered defenses. The Gentlemen operators aggressively target and terminate critical services related to backup, database, and security operations, maximizing operational disruption and impact.	77	• Manufacturing • Construction • Healthcare • Insurance • Consumer Services	CVE-2025-7771
Dragonforce	DragonForce is a ransomware group originating from Malaysia. Initially, known as a hacktivist group, DragonForce has transitioned into a ransomware operation, threatening victims with data encryption and extortion demands. They have targeted various industries and organizations globally, including government entities, businesses, and critical infrastructure sectors. The group gained attention for their	55	• Manufacturing • Business Services • Technology • Healthcare • Construction	• CVE-2024-21412 • CVE-2024-21893 • CVE-2024-21887 • CVE-2024-57727 • CVE-2024-57728 • CVE-2024-57726 • CVE-2023-46805 • CVE-2021-44228

	attacks on American companies, with details about data compromise and motives undisclosed. DragonForce has also threatened to release stolen information on dark web leak sites to pressure victims into paying ransoms.			
Akira	Akira is a ransomware-as-a-service (RaaS) operation distinguished by its early and aggressive focus on virtualized infrastructure. Beyond standard double-extortion tactics, Akira rapidly introduced a Linux encryptor specifically designed for VMware ESXi, enabling attackers to halt and encrypt large numbers of virtual machines from a single hypervisor using VM-aware options like vmonly and stopvm. Post-compromise activity prioritizes identity systems, backup platforms, and hypervisors, allowing fast, high-impact disruption of entire environments. This hypervisor-centric design, combined with data exfiltration via tools like rclone and SCP, makes Akira particularly effective against modern, virtualization-heavy networks.	31	• Manufacturing • Business Services • Technology • Construction • Agriculture	• CVE-2024-37085 • CVE-2024-40711 • CVE-2024-40766 • CVE-2023-20269 • CVE-2023-27532 • CVE-2023-28252 • CVE-2020-3259 • CVE-2020-3580
IncRansom	INC is a ransomware-as-a-service (RaaS) operation that emerged in mid-to-late 2023, operating through an affiliate-driven model in which core operators supply the malware and infrastructure while affiliates conduct intrusions and share profits. The group relies on a double-extortion strategy, coercing victims by threatening data leaks under the pretext of “protecting their reputation.” INC maintains two dedicated leak sites a private, credential-protected portal used for victim communication and negotiation, and a public site used to release stolen data. First detected in July 2023 and tracked by Trend Micro as Water Anito, the ransomware encrypts files using AES algorithm, reinforcing its position as a structured and professionally run extortion operation.	29	• Education • Healthcare • Government • Manufacturing • Information	• CVE-2023-3519 • CVE-2023-4966 • CVE-2023-48788

Safepay	SafePay ransomware is an emerging and previously undocumented threat, first observed in October 2024, that relies heavily on valid credentials likely sourced from dark web marketplaces and VPN access to infiltrate target environments. The group employs a multi-stage intrusion chain, commonly initiating attacks via Remote Desktop Protocol (RDP) and exploiting known VPN vulnerabilities while disabling defenses such as Windows Defender using LOLbins. SafePay features a modular and sophisticated design, enabling privilege escalation, UAC bypass, and network propagation, demonstrating a high degree of operational maturity. The ransomware encrypts files with a ***.safepay*** extension and drops a ***readme_safepay.txt*** ransom note, signaling the rise of a globally active ransomware operation targeting diverse industries across multiple countries.	22	• Manufacturing • Technology • Education • Healthcare • Business Services	Unknown
Nightspire	NightSpire, quickly positioned itself as a high-impact ransomware actor by pairing double-extortion operations with exploitation of advanced vulnerabilities. The group maintains a dark-web leak portal with countdown-based coercion and employs stealth techniques LOLBins, MEGACmd, WinSCP to exfiltrate data while remaining undetected inside victim networks. Its campaigns span the U.S., Japan, Taiwan, Egypt, and the U.K., with a notable concentration on manufacturing, reflecting a globally distributed yet technically disciplined threat posture.	15	• Manufacturing • Business Services • Healthcare • Technology • Construction	CVE-2024-55591
Play	Play ransomware (aka Playcrypt), first observed in mid-2022, is a highly disruptive ransomware family known for its multi-extortion strategy, combining data encryption with threats of public data leaks on TOR-based sites. The group primarily gains initial access through vulnerability	12	• Manufacturing • Business Services • Technology • Construction • Logistics	• CVE-2024-57727 • CVE-2022-41040 • CVE-2022-41082 • CVE-2021-34523 • CVE-2020-12812 • CVE-2018-13379

	exploitation and exposed or rented RDP servers, with a notable focus on Fortinet FortiOS flaws and ProxyNotShell exploits. Once inside, Play emphasizes stealth and evasion, heavily leveraging LOLBins, COTS tools, intermittent encryption, and Active Directory abuse via GPOs to spread laterally. Its use of specialized tools like Grixba and AlphaVSS, along with commodity frameworks such as Cobalt Strike and Mimikatz, highlights a mature, operationally disciplined ransomware operation capable of targeting governments, enterprises, and critical institutions worldwide.			
Lockbit5	LockBit 5.0, internally codenamed ChuongDong, was announced on the RAMP dark web forum in September 2025 to mark the group's six-year anniversary, resuming operations after the February 2024 Operation Cronos law enforcement takedown. LockBit 5.0 payloads are built with a leaked version of the LockBit 3.0 builder and subsequently packed and 'branded' as a new variant of LockBit. LockBit 5.0 ransom notes instruct the victim to communicate with the attacker via TOX messenger.	10	• Business Services • Manufacturing • Technology • Healthcare • Construction	Unknown
Payload	The Payload Ransomware is a lightweight C++ based ransomware (~385 KB) that operates without obfuscation, indicating prior attacker access and possible pre-disabling of AV/EDR defenses. The malware encrypts files using the ".payload" extension and drops a ransom note named RECOVER_payload.txt, leveraging a double-extortion model involving data exfiltration and Tor-based negotiation. It performs extensive pre-encryption actions, including deletion of shadow copies, clearing event logs, disabling security controls, and terminating backup and productivity services to maximize impact. The ransomware supports lateral movement via network share	9	• Manufacturing • Business Services • Consumer Services • Healthcare • Financial Services	Unknown

	enumeration, uses multi-threaded execution, and employs ChaCha20 encryption with Curve25519 key exchange for efficiency and security. To evade detection and reduce forensic artifacts, it relaunches in hidden mode, leverages NTFS alternate data streams for self-deletion, and avoids encrypting critical system files to maintain operational stability.			

Conclusion

The events of this month are a reminder that the threat landscape doesn't pause between incidents; it compounds. Attackers are converging tactics across vulnerability exploitation, supply-chain infiltration, cloud abuse, and ransomware into seamless, high-impact campaigns. For security teams, the imperative is clear: static defenses and periodic assessments are no longer sufficient. Platforms like LOVI that deliver continuous threat visibility, real-time monitoring, and actionable vulnerability intelligence are now foundational - not optional to any resilient enterprise security posture.