loginsoft

Monthly Report

Threat & Vulnerabilities Report – January 2025

Executive Summary

As 2025 unfolds, new cybersecurity challenges emerge quickly, signaling a year filled with evolving threats. January saw 14 critical vulnerabilities added to CISA's Known Exploited Vulnerabilities (KEV) catalog. Microsoft leads with three, followed by Mitel with two, while Apple, Ivanti, SonicWall, Fortinet, and Oracle each contribute one.

Alongside the latest KEV updates, CISA has issued a warning regarding critical vulnerabilities in Contec CMS8000 patient monitors, a key device in healthcare environments. In a joint advisory with the FBI, attention was also drawn to the exploitation of vulnerabilities in Ivanti Cloud Service Appliances, which are being targeted as part of an advanced attack chain. Additionally, threat actors have been actively exploiting vulnerabilities in NETGEAR routers, as well as Zyxel and Mitel products, highlighting the escalating risk and the urgent need for enhanced cybersecurity measures.

Moreover, 14 vulnerabilities were exploited as zero-days in January, amplifying the ongoing risk posed by cyber adversaries as we step into the new year.

Ransomware groups Babuk2, Clop, and Lynx made their presence felt in January 2025, compromising major sectors like healthcare, finance, and manufacturing, underscoring the escalating risk to critical industries.

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 Neurons for ZTA Gateways	A Stack-based Buffer Overflow Vulnerability in Ivanti Connect Secure, Policy Secure, and Neurons for ZTA Gateways enables remote unauthenticated attackers to execute arbitrary code on affected systems	Yes	Yes	Yes	False
CVE-2025-0626	Contec Health	CMS8000 Patient Monitor	A Hidden Functionality Vulnerability in Contec Health CMS8000 Patient Monitor leads to upload and overwrite files on the device.	Yes	No	No	False
CVE-2025-0683	Contec Health	CMS8000 Patient Monitor	An Exposure of Private Personal Information to an Unauthorized Actor Vulnerability in Contec	Yes	No	No	False

			Health CMS8000 Patient Monitor via hard-coded public IP address				
CVE-2025-21333	Microsoft	Windows Hyper-V	An Elevation of Privilege Vulnerability in Microsoft Windows Hyper-V NT Kernel Integration VSP	Yes	No	Yes	False
CVE-2025-21334	Microsoft	Windows Hyper-V	An Elevation of Privilege Vulnerability in Microsoft Windows Hyper-V NT Kernel Integration VSP	Yes	No	Yes	False
CVE-2025-21335	Microsoft	Windows Hyper-V	An Elevation of Privilege Vulnerability in Microsoft Windows Hyper-V NT Kernel Integration VSP	Yes	No	Yes	False
CVE-2025-23006	SonicWall	SMA1000 Appliance Management Console (AMC) and Central Management Console (CMC)	A Deserialization of Untrusted Data Vulnerability in the SonicWall SMA1000 AMC and CMC allows remote, unauthenticated attackers to execute arbitrary OS commands	Yes	No	Yes	False
CVE-2025-24085	Apple	Multiple Products	A Use-after-free Vulnerability in Apple's Core Media Component could allow a malicious application already installed on a device to escalate its privileges.	Yes	No	Yes	False
CVE-2024-8190	Ivanti	Cloud Service Appliance (CSA)	An OS Command Injection Vulnerability in Ivanti CSA that enables a remote authenticated attacker to achieve remote code execution	Yes	No	Yes	False
CVE-2024-8963	Ivanti	Cloud Service Appliance (CSA)	A Path Traversal Vulnerability in Ivanti CSA that can enable an attacker to bypass admin authentication and execute arbitrary commands on the appliance	Yes	No	Yes	False
CVE-2024-9379	Ivanti	Cloud Service Appliance (CSA)	A SQL Injection Vulnerability in the Ivanti CSA allows a remote, authenticated attacker with administrator	Yes	No	Yes	False

			privileges to execute arbitrary SQL commands				
CVE-2024-9380	Ivanti	Cloud Service Appliance (CSA)	A Command Injection Vulnerability in the Ivanti CSA enables a remote, authenticated attacker with administrator privileges to execute arbitrary commands on the system	Yes	No	Yes	False
CVE-2024-12248	Contec Health	CMS8000 patient monitor	A Remote Code Execution Vulnerability in the Contec Health CMS8000 patient monitor	Yes	No	No	False
CVE-2024-12686	BeyondTrust	• Privileged Remote Access (PRA) • Remote Support (RS)	An OS Command Injection Vulnerability in the BeyondTrust Privileged Remote Access (PRA) and Remote Support (RS) solutions that can be exploited by attackers with existing administrative privileges to upload and execute malicious files	Yes	Yes	Yes	False
CVE-2024-12847	NETGEAR	• DGN1000 • DGN2200 v1	An Authentication Bypass Vulnerability in the NETGEAR routers enables remote attackers to gain unauthorized access and take control of the affected devices.	Yes	No	No	False
CVE-2024-40891	Zyxel	CPE series devices	A Command Injection Vulnerability in Zyxel CPE devices allows attackers to execute arbitrary commands on affected systems, potentially resulting in full system compromise, data exfiltration, or network infiltration	Yes	Yes	No	False
CVE-2024-41710	Mitel	• Mitel 6800 Series • Mitel 6900 Series • Mitel 6900w Series	A Command Injection Vulnerability in Mitel 6800, 6900, and 6900w series SIP phones, including the 6970 Conference Unit, could allow attackers to execute arbitrary commands within the phone's context.	Yes	No	No	False

		• Mitel 6970 Conference Unit					
CVE-2024-41713	Mitel	MiCollab	A Path Traversal Vulnerability in the NuPoint Unified Messaging (NPM) component of Mitel MiCollab that arises due to insufficient input validation	No	No	Yes	False
CVE-2024-50603	Aviatrix	Network Controller	An Unauthenticated Command Injection Vulnerability in the Aviatrix Network Controller allows remote attackers to execute arbitrary code	No	Yes	Yes	False
CVE-2024-52875	GFI Software	Kerio Control Firewall	A HTTP Response Splitting Vulnerability in Kerio Control firewalls leads to remote code execution	No	No	No	False
CVE-2024-55550	Mitel	MiCollab	A Path Traversal Vulnerability that allows attackers with administrative privileges to read local files on the MiCollab server	No	No	Yes	False
CVE-2024-55591	Fortinet	FortiOS and FortiProxy	An Authentication Bypass Vulnerability in Fortinet FortiOS and FortiProxy could enable remote attackers to gain super-admin privileges	Yes	No	Yes	False
CVE-2023-48365	Qlik	Sense Enterprise	A HTTP Tunneling Vulnerability in the Qlik Sense Enterprise that enables an attacker to escalate privileges and send HTTP requests to the backend server hosting the software	No	Yes	Yes	False
CVE-2022-40684	Fortinet	FortiOS, FortiProxy, and FortiSwitch Manager	An Authentication Bypass Vulnerability in Fortinet FortiOS, FortiProxy, and FortiSwitchManager allows an unauthenticated attacker to execute administrative operations by sending specially crafted HTTP or HTTPS request on the interface.	No	Yes	Yes	False

CVE-2020-2883	Oracle	WebLogic Server	A Deserialization of Untrusted Data Vulnerability in the Oracle WebLogic Server, that can result in remote code execution	No	No	Yes	False
CVE-2020-11023	jQuery	jQuery	A Cross-Site Scripting (XSS) Vulnerability exists in jQuery, where maliciously crafted, untrusted input enclosed in HTML tags can be passed to jQuery's DOM manipulators	No	Yes	Yes	True

Ransomware Insights for January

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 January - 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-	64	• Healthcare • Finance • Manufacturing • Energy • Government • Retail • Legal	• Unknown

	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.			
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 vulnerabilities, or leveraging compromised credentials.	60	• Healthcare • Bank • Education • Gaming • Transportation	• CVE-2024-55956 • CVE-2023-0669 • CVE-2023-27350 • CVE-2023-27351 • CVE-2023-34362 • CVE-2023-47246
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	36	• Finance • Retail • Real Estate • Manufacture • Construction • Logistic	• Unknown

	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.			
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, showcasing its technical sophistication. The group's first	33	• Healthcare • Finance • Government • Information technology • Education	• Unknown

	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.			
Ransomhub	Ransomhub is a self-described Ransomware-as-a-Service 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	32	• Education • Construction • Government	CVE-2020-1472

	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			
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.	31	• Education • Manufacture • Finance	• CVE-2020-1472 • CVE-2020-3259
Inc Ransom	The Inc Ransom group is a sophisticated ransomware operation targeting large-scale organizations and enterprises. Known for its diverse attack methods, the group employs a combination of vulnerability exploitation, spear-phishing campaigns, and tailored ransomware deployment to compromise victims. Once inside a network, Inc Ransom uses advanced techniques to encrypt files, including partial encryption to optimize speed, targeting only key portions of large files.	23	• Education • Healthcare • Government Sectors	CVE-2023-3519
8Base	Despite a significant surge in activity during the summer of 2023, the 8Base ransomware group has largely operated in obscurity. Employing a combination of encryption and "name-and-shame" tactics, the group coerces victims into	23	• Business service • Finance • Manufacture • Information technology • Construction	• CVE-2023-3519 • CVE-2023-35078

	paying ransoms. Notably, 8Base follows an opportunistic compromise pattern, targeting victims across diverse industries. Despite the extensive compromises, details about the identities, methodology, and motivations behind the group's actions remain elusive. Examination of their ransomware samples indicates the use of a customized Phobos with SmokeLoader.			
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.	18	• Healthcare • Finance • Technology • Manufacturing	• CVE-2023-0669 • CVE-2023-27350 • CVE-2023-27351 • CVE-2023-34362 • CVE-2023-47246 • CVE-2022-2295
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	16	• Education • Healthcare	• Unknown

	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.			
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 increasingly prioritizes industries where operational disruption could drive substantial ransom demands.	11	• Education • Recreation	• CVE-2024-40711 • CVE-2024-40766
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,	10	• Healthcare • Media • Technology • Telecommunication	• CVE-2022-41040 • CVE-2022-41080 • CVE-2022-41082 • CVE-2021-34523 • CVE-2020-12812 • CVE-2018-13379

	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.			
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.	9	• Healthcare • Education • Research	• Unknown
ElDorado	The Eldorado ransomware is a sophisticated Ransomware-as-a-Service (RaaS) operation that targets both Windows and Linux environments, specifically aiming at VMware ESXi systems and virtual machines (VMs). Developed using the Golang programming language, this ransomware is designed for cross-platform functionality, enabling attacks across multiple operating	6	• Healthcare • Financial • Government Agencies • Manufacturing • Industrial Sectors • Telecommunications	• Unknown

	systems and broadening its reach. Eldorado operates through dedicated leak sites (DLS) on the dark web, where it advertises stolen data and threatens to release it publicly if ransoms are not paid.			
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.	11	• 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

Conclusion

As cyber threats grow in sophistication and scale, organizations must take decisive action to mitigate risks. The active exploitation of vulnerabilities and the continued rise of ransomware highlight the need for continuous threat intelligence, robust security measures, and timely patching. Loginsoft Vulnerability Intelligence (LOVI) provides critical insights to help businesses stay ahead of cyber adversaries. Strengthening cybersecurity defenses now will be crucial in preventing future attacks and ensuring a secure online environment.

Reference Links:

- https://www.cisa.gov/news-events/alerts/2025/01/08/cisa-adds-one-vulnerability-kev-catalog
- https://www.cisa.gov/news-events/alerts/2025/01/14/cisa-adds-four-known-exploited-vulnerabilities-catalog
- https://www.cisa.gov/news-events/alerts/2024/09/13/cisa-adds-one-known-exploited-vulnerability-catalog
- https://www.cisa.gov/news-events/alerts/2024/09/19/cisa-adds-one-known-exploited-vulnerability-catalog
- https://www.cisa.gov/news-events/alerts/2024/10/09/cisa-adds-three-known-exploited-vulnerabilities-catalog
- https://www.cisa.gov/news-events/alerts/2025/01/13/cisa-adds-two-known-exploited-vulnerabilities-catalog
- https://www.cisa.gov/news-events/alerts/2025/01/07/cisa-adds-three-known-exploited-vulnerabilities-catalog
- https://www.cisa.gov/news-events/alerts/2025/01/23/cisa-adds-one-known-exploited-vulnerability-catalog
- https://www.cisa.gov/news-events/alerts/2025/01/07/cisa-adds-three-known-exploited-vulnerabilities-catalog
- https://www.greynoise.io/blog/active-exploitation-of-zero-day-zyxel-cpe-vulnerability-cve-2024-40891
- https://www.cisa.gov/news-events/alerts/2025/01/30/cisa-releases-fact-sheet-detailing-embedded-backdoor-function-contec-cms8000-firmware
- https://cloud.google.com/blog/topics/threat-intelligence/ivanti-connect-secure-vpn-zero-day/

- https://www.bloomberg.com/news/articles/2025-01-08/white-house-rushes-to-finish-cyber-order-after-china-hacks
- https://www.wiz.io/blog/wiz-research-identifies-exploitation-in-the-wild-of-aviatrix-cve-2024-50603
- https://arcticwolf.com/resources/blog/qlik-sense-exploited-in-cactus-ransomware-campaign/
- https://www.rewterz.com/rewterz-news/rewterz-threat-alert-chinese-apt-earth-lusca-adopts-sprysocks-linux-malware-to-bolster-its-cyber-arsenal-active-iocs

loginsoft

Connect with us

linkedin.com/loginsoft

x.com/loginsoft_inc

www.loginsoft.com