LevelBlue

Incident Response & Digital Forensics

Monthly Threat Review – May 2025

Agenda

New Vulnerabilities

- Microsoft Security Update Overview
- Recent security updates from:
  - Adobe
  - Apple
  - Google
  - Cisco
  - SAP
  - Vmware
- Known Exploited Vulnerabilities Catalog

Prevalent Threats

- Update on the top 5 ransomware groups

New Vulnerabilities

Microsoft Security Update: May 2025

Total CVE's: 77 **Critical: 8** **Actively Exploited 5**

Actively Exploited

CVE	Title	Severity
CVE-2025-30397	Microsoft Scripting Engine Memory Corruption Vulnerability	High (CVSS 7.5)
CVE-2025-30400	Windows Desktop Window Manager (DWM) Core Library Elevation of Privilege Vulnerability	High (CVSS 7.8)
CVE-2025-32701	Windows Common Log File System (CLFS) Driver Elevation of Privilege Vulnerability	High (CVSS 7.8)
CVE-2025-32706	Windows Common Log File System (CLFS) Driver Elevation of Privilege Vulnerability	High (CVSS 7.8)
CVE-2025-32709	Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability	High (CVSS 7.8)

Critical Rated CVEs

CVE	Title	Severity
CVE-2025-29972	Azure Storage Resource Provider Spoofing Vulnerability	Critical (CVSS 9.9)
CVE-2025-29813	Azure DevOps Server Elevation of Privilege Vulnerability	Critical (CVSS 10.0)
CVE-2025-29827	Azure Automation Elevation of Privilege Vulnerability	Critical (CVSS 9.8)
CVE-2025-29966	Microsoft Windows Remote Desktop Services RCE Vulnerability	Critical (CVSS 8.8)
CVE-2025-29967	Microsoft Windows Remote Desktop Services RCE Vulnerability	Critical (CVSS 8.8)
CVE-2025-30377	Microsoft Office RCE Vulnerability	Critical (CVSS 8.4)
CVE-2025-30386	Microsoft Office RCE Vulnerability	Critical (CVSS 8.4)
CVE-2025-29833	Windows Virtual Machine Bus RCE Vulnerability	Critical (CVSS 7.1)

Microsoft Security Update: May 2025

Total CVE's: 77 **Critical: 8** **Actively Exploited 5**

High Interest CVEs

CVE	Title	Severity	Likelihood of Exploit
CVE-2025-24063	Kernel Streaming Service Driver Elevation of Privilege Vulnerability	Important (CVSS 7.8)	Exploitation More Likely
CVE-2025-29841	Universal Print Management Service Elevation of Privilege Vulnerability	Important (CVSS 7.8)	Exploitation More Likely
CVE-2025-29971	Web Threat Defense (WTD.sys) Denial of Service Vulnerability	Important (CVSS 7.5)	Exploitation More Likely
CVE-2025-29976	Microsoft SharePoint Server Elevation of Privilege Vulnerability	Important (CVSS 7.8)	Exploitation More Likely
CVE-2025-30382	Microsoft SharePoint Server Remote Code Execution Vulnerability	Important (CVSS 7.8)	Exploitation More Likely
CVE-2025-30383	Microsoft Office Visio Remote Code Execution Vulnerability	Important (CVSS 7.8)	Exploitation More Likely
CVE-2025-30385	Windows Common Log File System Driver Elevation of Privilege Vulnerability	Important (CVSS 7.8)	Exploitation More Likely
CVE-2025-30386	Microsoft Office Remote Code Execution Vulnerability	Critical (CVSS 8.4)	Exploitation More Likely
CVE-2025-24063	Kernel Streaming Service Driver Elevation of Privilege Vulnerability	Important (CVSS 7.8)	Exploitation More Likely
CVE-2025-29841	Universal Print Management Service Elevation of Privilege Vulnerability	Important (CVSS 7.8)	Exploitation More Likely

Additional Vendor Security Disclosures - May 2025

Adobe

- Forty (40) vulnerabilities identified
- Three (3) critical in Photoshop 2024/2025 affecting Windows and MacOS
- No active exploits reported.

Apple

- Thirty (30) vulnerabilities patched including a baseband firmware bug in Apples newly released in-house modem (named C1).
- Apple has acknowledged that the most recent software update corrects a significant security gap that could potentially allow hackers to get into personal data such as photos, messages and app information.
- Updates also to StoreKit, Notifications and Bluetooth components
- No active exploits reported by Apple
- iOS 18.5 iPadOS 18.5 and macOS Sequoia 15.5 released.

Google

- Forty-seven (47) vulnerabilities patched in Android.
- Active exploits in Android and Chrome
- A high-severity out-of-bounds write flaw in the Android FreeType font rendering library first identified in March 2025.
- Insufficient Policy enforcement in Chromium browser can lead to theft of login session information and account compromise.
- Patch to latest Chrome release 136.0.7103

Cisco

- Thirty-five (35) vulnerabilities patched in IOS and IOS XE.
- CVE-2025-20188 - Cisco IOS XE Wireless Controller Software Arbitrary File Upload Vulnerability (CVSS 10.0)
    - Catalyst 9800-CL Wireless Controllers for Cloud
    - Catalyst 9800 Embedded Wireless Controller for Catalyst 9300, 9400, and 9500 Series Switches
    - Catalyst 9800 Series Wireless Controllers
    - Embedded Wireless Controller on Catalyst APs
- Exploit expected after public release of details on June 2, 2025
- Also patched were bugs in RADIUS message processing in Cisco Identity Services Engine (ISE) and the Unified Intelligence Center application.

SAP

- Sixteen (16) vulnerabilities addressed, including two (2) critical in SAP NetWeaver visual composer.
- Active exploit of CVE-2025-31324 Missing Authorization Check In SAP NetWeaver (CVSS 10.0)
- Exploit activity has been attributed to Chinese espionage and Russian Ransomware groups

Vmware

- Five (5) security advisories addressing high severity issues in AVI Load Balancer, Cloud Foundation, Ari Suite, and Cloud Foundation
- No Active Exploits

U.S. Cybersecurity Infrastructure Security Agency

Known Exploited Vulnerabilities Catalog

CVE	Vendor	Product	Description	Date
CVE-2024-38475	Apache	HTTP Server	Apache HTTP Server Improper Escaping of Output Vulnerability	5/1/25
CVE-2023-44221	SonicWall	SMA100 Appliances	SonicWall SMA100 Appliances OS Command Injection Vulnerability	5/1/25
CVE-2025-34028	Commvault	Command Center	Commvault Command Center Path Traversal Vulnerability	5/2/25
CVE-2024-58136	Yiiframework	Yii	Yiiframework Yii Improper Protection of Alternate Path Vulnerability	5/2/25
CVE-2025-3248	Langflow	Langflow	Langflow Missing Authentication Vulnerability	5/5/25
CVE-2025-27363	FreeType	FreeType	FreeType Out-of-Bounds Write Vulnerability	5/6/25
CVE-2024-11120	GeoVision	Multiple Devices	GeoVision Devices OS Command Injection Vulnerability	5/7/25
CVE-2024-6047	GeoVision	Multiple Devices	GeoVision Devices OS Command Injection Vulnerability	5/7/25
CVE-2025-47729	TeleMessage	TM SGNL	TeleMessage TM SGNL Hidden Functionality Vulnerability	5/12/25

U.S. Cybersecurity Infrastructure Security Agency

Known Exploited Vulnerabilities Catalog

CVE	Vendor	Product	Description	Date
CVE-2025-32756	Fortinet	Multiple Products	Fortinet Multiple Products Stack-Based Buffer Overflow Vulnerability	5/14/25
CVE-2024-12987	DrayTek	Vigor Routers	DrayTek Vigor Routers OS Command Injection Vulnerability	5/15/25
CVE-2023-38950	ZKTeco	BioTime	ZKTeco BioTime Path Traversal Vulnerability	5/19/25
CVE-2024-27443	Synacor	Zimbra Collaboration Suite (ZCS)	Synacor Zimbra Collaboration Suite (ZCS) Cross-Site Scripting (XSS) Vulnerability	5/19/25
CVE-2025-27920	Srimax	Output Messenger	Srimax Output Messenger Directory Traversal Vulnerability	5/19/25
CVE-2024-11182	MDaemon	Email Server	MDaemon Email Server Cross-Site Scripting (XSS) Vulnerability	5/19/25
CVE-2025-4428	Ivanti	Endpoint Manager Mobile (EPMM)	Ivanti Endpoint Manager Mobile (EPMM) Code Injection Vulnerability	5/19/25
CVE-2025-4427	Ivanti	Endpoint Manager Mobile (EPMM)	Ivanti Endpoint Manager Mobile (EPMM) Authentication Bypass Vulnerability	5/19/25
CVE-2025-4632	Samsung	MagicINFO 9 Server	Samsung MagicINFO 9 Server Path Traversal Vulnerability	5/22/25

General Recommendations

- Apply patches provided by product vendors to vulnerable systems immediately after thorough testing.
- Run all software with non-administrative privileges to reduce the impact of a successful attack.
- Advise users to avoid visiting untrusted websites or clicking links from unknown or untrusted sources. Consider setting up email filtering to block HTTP links, minimizing the risk of users accidentally accessing malicious content.
- If blocking URL links isn't feasible, educate users about the dangers of hypertext links in emails or attachments, particularly from untrusted sources.
- Implement the principle of Least Privilege across all systems and services.

Prevalent Threats

Prevalent Threats

Top threat groups

- safepay
- qilin
- play
- akira
- devman

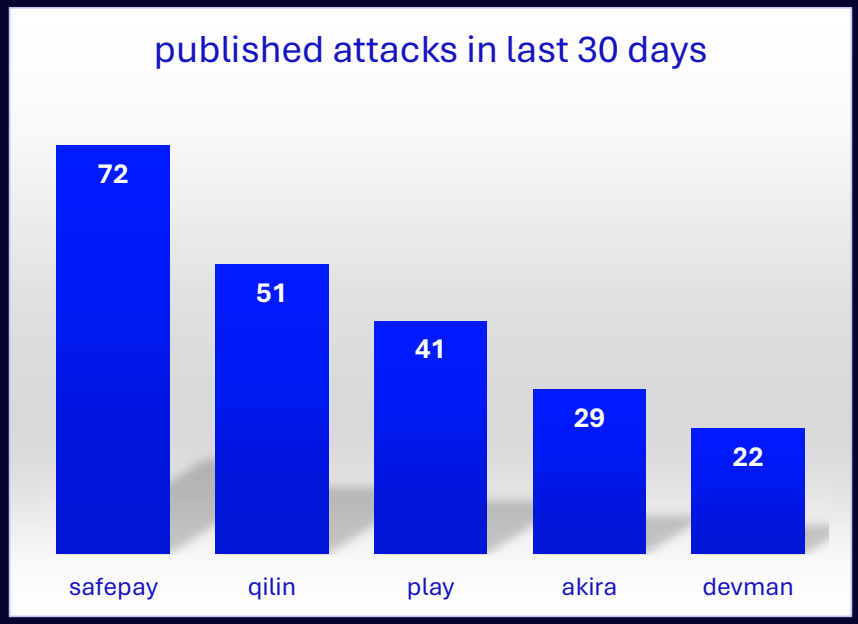
Threat Group Highlight

safepay

- First appeared in Sep 2024
- Analysis of ransomware binaries show similarities to LockBit. Other tooling includes the use of a backdoor previously identified with the Blacksuit threat group. Ransomware also includes check to avoid encrypting Russian speaking countries.

devman

- First appeared in April 2025
- Initial analysis of binary tooling suggests the group may be a former Qilian affiliate.



data from information published on threat group leak sites

LevelBlue

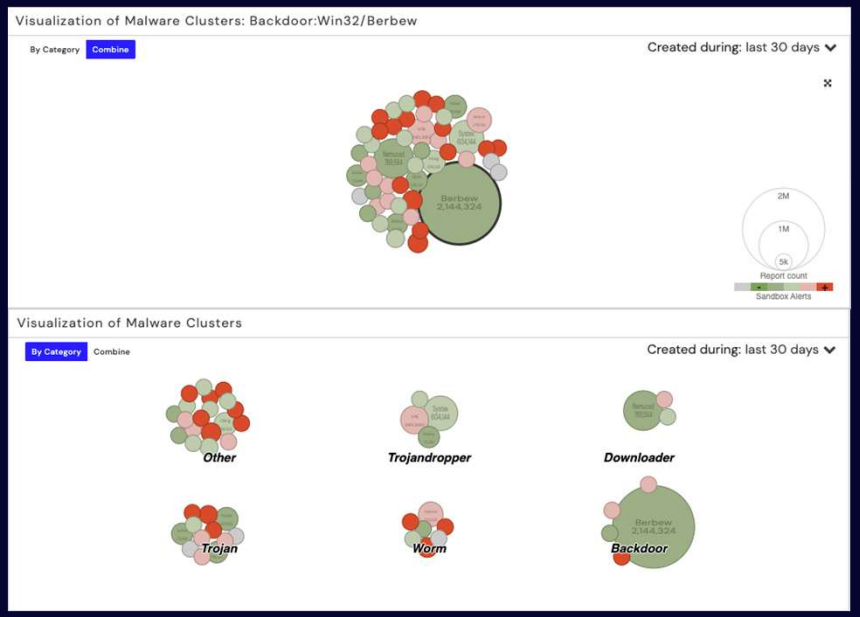
OTX Threat Exchange

Malware Sandbox Submissions

- Berbew (backdoor)
- Nimzod (downloader)
- Systex (trojandropper)
- VB (trojandropper)
- Autoruns (worm)

BerBew Backdoor

- Berbew backdoor is a family of Trojan malware designed to compromise Windows-based systems.
- Provides unauthorized remote access to an infected system
- Malware's primary goal stealing sensitive information (account logins)



Data provided by otx.alienvault.com

LevelBlue

Thank you