SCC | DIGITAL

THREAT PULSE

Amateurs hack systems;
professionals hack people
- Bruce Schneier

THREATS

NEWS

PHISHING

February 2025 - VOL.2

The News

IN THE NEWS THIS WEEK

Microsoft's Patch Tuesday Fixes 63 Flaws, Including Two Under Active Exploitation

Microsoft released updates fixing 63 security flaws, including two actively exploited vulnerabilities: CVE-2025-21391 and CVE-2025-21418. These flaws could allow attackers to delete files and achieve SYSTEM privileges. Additionally, a similar flaw (CVE-2024-38193) was linked to the Lazarus Group. The updates also addressed a critical RCE vulnerability (CVE-2025-21198) in the High Performance Compute Pack and another RCE flaw (CVE-2025-21376) in Windows LDAP. The U.S. CISA has added these vulnerabilities to its Known Exploited Vulnerabilities catalog.

READ MORE

Apple Patches Actively Exploited iOS Zero-Day CVE-2025-24200 in Emergency Update

Apple released out-of-band security updates to fix a flaw (CVE-2025-24200) in iOS and iPadOS that has been exploited in the wild. The vulnerability allows disabling USB Restricted Mode on locked devices, requiring physical access to exploit. Introduced in iOS 11.4.1, USB Restricted Mode blocks communication with accessories if the device hasn't been unlocked within an hour. The update was credited to Bill Marczak of The Citizen Lab. It follows a recent fix for a use-after-free bug (CVE-2025-24085) in Core Media exploited against iOS versions before 17.2.

READ MORE

OTHER NEWS HIGHLIGHTS

Gcore DDoS Radar Reveals 56% YoY Increase in DDoS Attacks

DeepSeek App Transmits Sensitive User and Device Data Without Encryption

FBI, Europol, and NCA Take Down 8Base Ransomware Data Leak and Negotiation Sites

Multiple Vulnerabilities in Fortinet Products Could Allow for Remote Code Execution

The News

TOP OF THE NEWS THIS WEEK

Microsoft Patch Tuesday for February 2025 — Snort rules and prominent vulnerabilities

Microsoft's February 2025 security update addresses 63 vulnerabilities, with four marked as "critical" and one as "moderate." Notable critical flaws include:

- CVE-2025-21376 (CVSS 8.1): RCE in Windows LDAP due to an out-of-bounds write caused by a race condition, potentially leading to arbitrary code execution.
- CVE-2025-21379 (CVSS 7.1): RCE in the DHCP Client Service, allowing attackers to modify network communications and execute arbitrary code.
- CVE-2025-21177: Privilege escalation in Microsoft Dynamics 365 Sales via SSRF.
- CVE-2025-21381: RCE in Microsoft Excel, triggered via the preview pane.
-

Vulnerabilities CVE-2025-21391 and CVE-2025-21418 are actively exploited in the wild, involving privilege elevation and SYSTEM privileges exploitation. The update also addresses important RCE flaws in various Windows services. Talos has released new Snort rules to detect exploit attempts.

READ MORE

TOP RELATED ARTICLES

Apple Confirms 'Extremely Sophisticated' Exploit Threatening iOS Security

Massive 1.17TB Data Leak Exposes Billions of IoT Grow Light Records

Microsoft Uncovers 'BadPilot' Campaign as Seashell Blizzard Targets US and UK

Geo-Politics

NEWS FROM AROUND THE WORLD

The Rise of Cyber Espionage: UAV and C-UAV Technologies as Targets

Resecurity detected a rise in cyberattacks targeting UAV and counter-UAV technologies, especially during conflicts like the Russia-Ukraine war and the Israel-Hamas confrontation. The trend increased in Q3-Q4 2024 and continued into Q1 2025. Cybercriminals, mercenaries, and nation-state actors are targeting these technologies for intelligence and espionage.

Resecurity found Dark Web postings seeking sensitive military documents related to drones. Actors are more interested in buyers of UAV and counter-UAV technologies, likely for reconnaissance and future cyber threats. This includes Human Intelligence (HUMINT) efforts focused on the defense industrial base (DIB) workflow.

READ MORE ›

UK Secret Order Demands That Apple Give Access to Users' Encrypted Data

The Washington Post reported that the UK government secretly ordered Apple to create a backdoor to iCloud, allowing access to encrypted user data globally. This unprecedented demand, issued under the Investigatory Powers Act (IPA), aims to help law enforcement tackle criminal activities but raises significant privacy concerns.

Apple has not publicly commented on the order but previously stated it would rather withdraw encrypted services than compromise user privacy.

US lawmakers have criticized the order, calling it a "foreign cyberattack" and are considering measures to counter it.

READ MORE ›

HIGHLIGHTS FROM AROUND THE WORLD

China-linked Espionage Tools Used in Ransomware Attacks

UK Government Reportedly Demands Access to Encrypted iCloud Files Worldwide

Australians Hit With One Cyber Attack Every Second in 2024

US, UK and Australia Sanction Russian Bulletproof Hoster Zservers

Breaches

SECURITY BREACHES THIS WEEK

Doxbin Data Breach: Hackers Leak 136K User Records and Blacklist File

Doxbin, a platform known for doxxing, was breached by the hacker group Tooda, resulting in the deletion of user accounts and exposure of 136,814 user records, including emails and usernames.

Tooda also leaked a "blacklist" of individuals who paid to keep their information off the platform.

This breach raises significant risks for affected users, as their personal information could be cross-referenced with other data leaks, potentially exposing their real-world identities. The incident highlights the vulnerability of even malicious platforms to cyberattacks.

READ MORE

Massive 1.17TB Data Leak Exposes Billions of IoT Grow Light Records

A massive 1.17 TB data leak from Mars Hydro, an IoT grow light company, exposed 2.7 billion records, including Wi-Fi passwords, IP addresses, and device IDs. The unprotected database also contained email addresses, API details, and error logs with sensitive information like tokens and app versions. The breach was linked to LG-LED Solutions and Spider Farmer, both involved in agricultural technology. The exposed data connects to control devices, such as smartphones, revealing operating system details. This leak presents significant risks of unauthorized network access and potential cyberattacks on the affected systems.

READ MORE

OTHER SECURITY BREACHES

Secret Taliban records published online after hackers breach computer systems

Sarcoma ransomware gang claims the theft of sensitive data from PCB maker Unimicron

Vulnerabilities

VULNERABILITIES & EXPLOITS

CVE-2025-21177- Windows Remote Desktop Services Remote Code Execution Vulnerability

CVSS SCORE 8.1

CVE-2025-21376 - Windows Remote Desktop Services Remote Code Execution Vulnerability

CVSS SCORE 8.1

LAST WEEKS RECAP

CVE-2024-40591- FortiOS Security Fabric privilege escalation

CVSS Score: (8.0)

CCVE-2024-21413 Microsoft Outlook Remote Code Execution Vulnerability

CVSS Score: (9.8)

Ransomware

WEEKLY RANSOMWARE ROUNDUPS

OVERVIEW

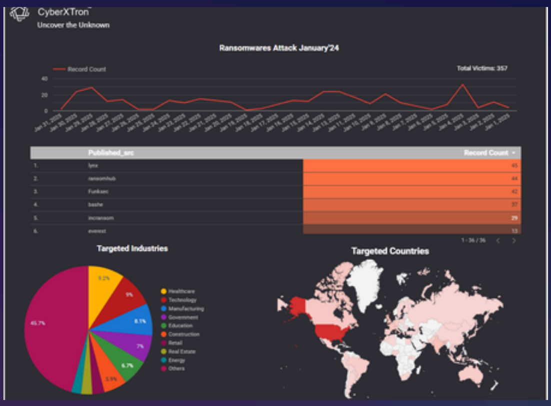
Top Group: The Lynx Group was the most active, claiming 45 victims on January. Across all ransomware groups, 357 new victims being published across various groups

TARGET INDUSTRIES

The Healthcare sectors accounted for 9.2% of the total victims, making it the most targeted industry in January 2025.

TARGET COUNTRY

With 162 victims in total, the USA was the most targeted country in January 2025.



	Published_src	Record Count
1.	lynx	45
2.	ransomhub	44
3.	Funksec	42
4.	bashe	37
5.	incransom	29
6.	everest	13

Dive into this interactive report to uncover hidden trends HERE!

Published Ransomware Attacks - Source: CyberXTron ThreatBolt

TOP THREAT ACTORS

RansomHub

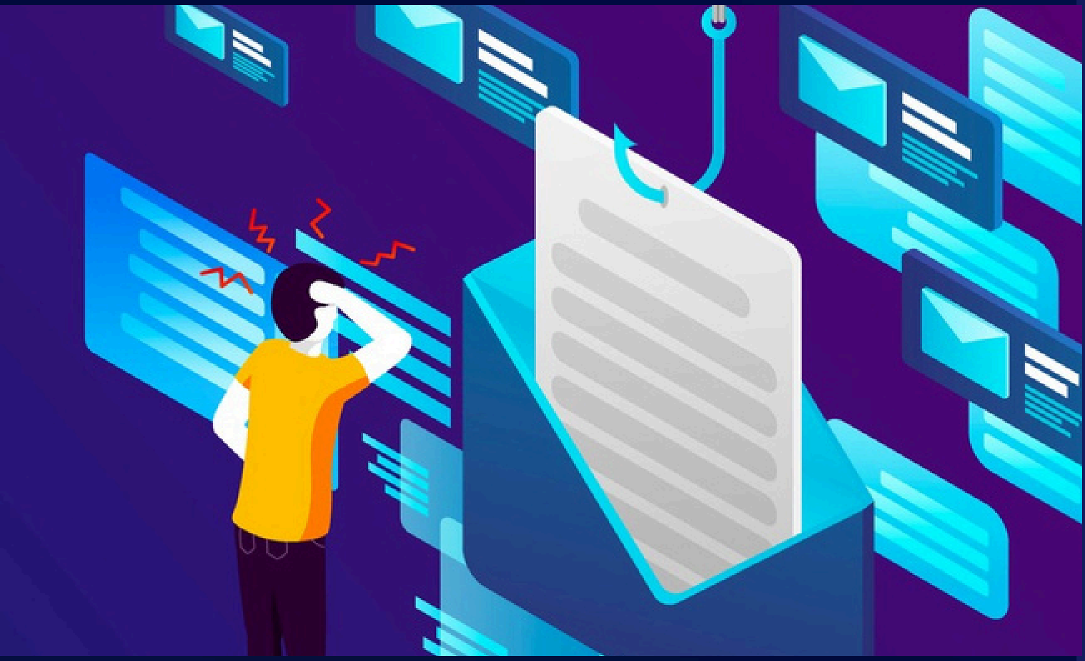
The RansomHub ransomware group has been observed targeting various sectors, including critical infrastructure, financial and government services, and the healthcare sector. They use ransomware variants rewritten in GoLang to target both Windows and Linux systems. RansomHub is known for employing double extortion attacks, encrypting data using “Curve25519” encryption

Lynx

The Lynx Ransomware-as-a-Service (RaaS) group has been found operating a highly organized platform, complete with a structured affiliate program and robust encryption methods. Researchers at Group-IB gained access to the group’s affiliate panel, revealing the inner workings of this sophisticated cyber-threat.

Phishing

PHISHING NEWS THIS WEEK



How AI was used in an advanced phishing campaign targeting Gmail users

FBI warned about the increasing use of AI in cyber scams. Cybercriminals are leveraging AI to craft convincing emails, voice, and video messages, often making phishing campaigns more effective. These AI tools are relatively low cost, with sophisticated email attacks starting at just $5. The FBI cautions against unsolicited emails or messages, as AI-powered tools can bypass security filters and trick users into providing sensitive information.

A recent campaign targeting Gmail users demonstrates this threat. Attackers made calls claiming Gmail accounts were compromised, followed by emails from fake Google domains to obtain recovery codes. With these codes, criminals could access multiple services, leading to potential identity theft. The FBI warns about links to fake websites designed to steal credentials or session cookies, allowing cybercriminals to hijack accounts.

To protect against AI-driven phishing attacks, the FBI advises:

- Avoiding clicks on links or downloads from unexpected emails or messages.
- Not entering personal information on uncertain websites.
- Using a password manager to autofill credentials on trusted sites.
- Monitoring accounts for unauthorized access.
- Verifying security alerts directly on the Google Account page.
- Using multi-factor authentication (MFA) for all accounts.
- Protecting devices with up-to-date security software.

READ MORE >

OTHER PHISHING ARTICLES

Astaroth Phishing Kit Bypasses 2FA to Hijack Gmail and Microsoft Accounts

Phishing evolves beyond email to become latest Android app threat

Astaroth is an advanced phishing kit using real-time credential and session cookie capture to compromise Gmail, Yahoo and Office 365 accounts