Cyber News Journal

vol. 6

birbank

Introduction

Dear Readers,

As we move into the second half of 2025, cybersecurity incidents continue to rise globally. Artificial intelligence plays a significant role in this evolving landscape. In this edition, we bring you the latest cybersecurity trends and key updates shaping the year ahead.

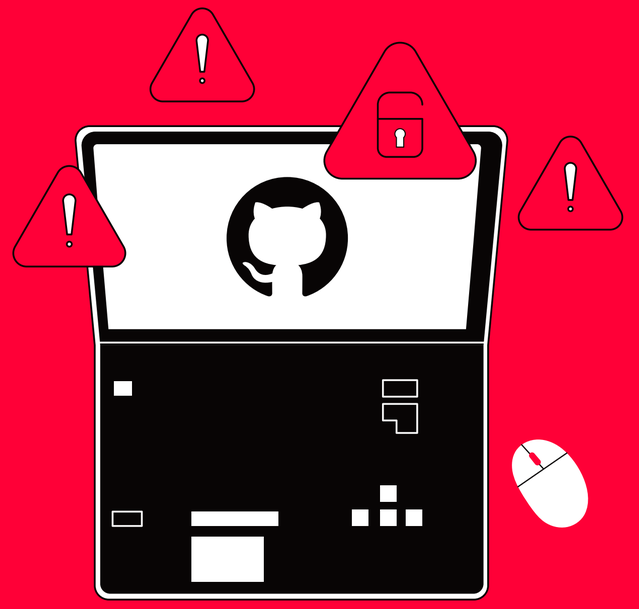
With cyber threats constantly evolving, staying informed and vigilant remains the best defense.

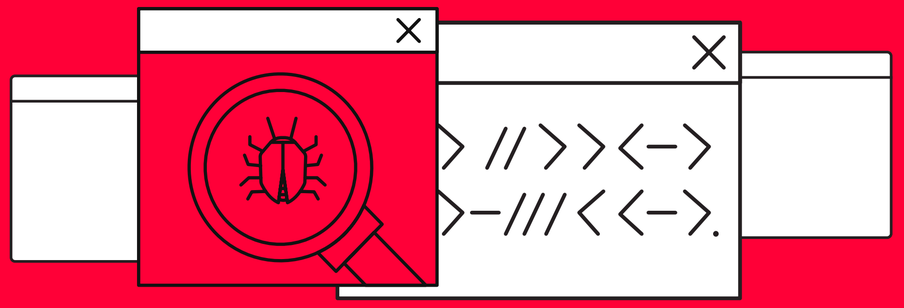
Let’s explore the cybersecurity dynamics of 2025 together!

Microsoft warns of malvertising campaign impacting over **1M devices**

Microsoft recently shared details about a widespread malvertising campaign that has affected more than 1 million devices globally.
This attack, first identified in December 2024, seems to be a calculated move to steal personal and sensitive data from users.

Tracked by Microsoft under the name Storm-0408, this campaign is tied to a group known for using methods like phishing, malvertising, and search engine manipulation to spread malware. Their goal is to gain unauthorized access to devices and collect valuable information.

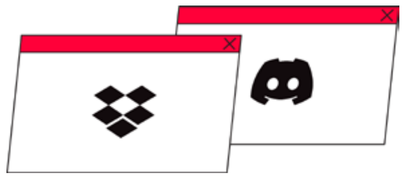




The campaign originated from shady streaming websites, which contained malicious ads. These ads redirected users to an intermediary site, and from there, they were directed to GitHub and other platforms, where the malware was delivered. The attack targeted both personal users and businesses, making it a far-reaching threat.

A notable aspect of the attack was the use of GitHub to deliver the initial malware payload. In a few separate instances, the malicious files were also hosted on platforms like Discord and Dropbox.

Microsoft took action by removing the compromised repositories, though the exact number hasn't been disclosed.



The attack unfolds in multiple stages:

Stage 1:
Online Platform

Stage 2:
Malicious adware

Stage 3:
Malicious website

Stage 4:
User infected

This campaign underscores the risks of malvertising and how cybercriminals constantly evolve their tactics.

It serves as a reminder for both individuals and businesses to stay vigilant and improve their cybersecurity defenses.

https://thehackernews.com/2025/03/microsoft-warns-of-malvertising.html

Microsoft February 2025 Security Updates: **Critical Vulnerabilities Fixed**

Microsoft announced that it has resolved 63 security vulnerabilities in February. While this update is smaller compared to last month's major security fixes, it appears that critical security issues still remain.

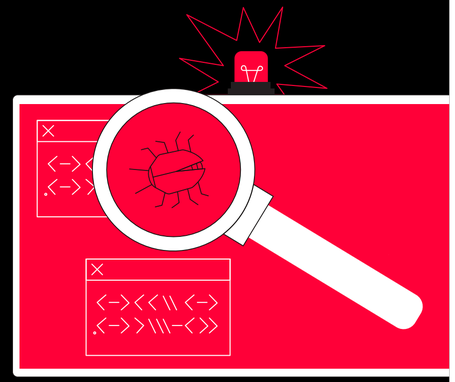
Two particularly significant vulnerabilities continue to be actively exploitable, meaning hackers could use them to attack systems.

The two most critical vulnerabilities are:

- One allows cybercriminals to delete files. While data leakage may not be likely, the deletion of critical files could make the service unavailable.

- The other enables attackers to gain full system-level privileges, potentially giving them complete control over the entire system.

Microsoft
Patch Tuesday



Microsoft
Active Directory

Active Directory (AD) Vulnerability: A Critical Risk

Active Directory (AD) is the backbone of user and device management in organizations. Cybercriminals can exploit weaknesses in the LDAP protocol to compromise this system, leading to severe security risks.

What Are the Risks?

- Remote Code Execution: Attackers can gain unauthorized access by running malicious code.
- Privilege Escalation: They can elevate their access from a regular user to an administrator.
- Lateral Movement: Once inside, they can spread across the network, compromising multiple systems.

Why Does It Matter?

AD manages user authentication and access controls across the corporate network. A breach could give attackers unrestricted access to sensitive company data.

While AD is crucial for identity and access management, it is not a data storage system. Data is typically housed in dedicated servers and databases, but an AD compromise can still be a gateway to widespread security breaches.

This month's security patches cover **a broad spectrum of vulnerability types:**

- **25 Remote Code Execution (RCE) Vulnerabilities**
- **20 Elevation of Privilege (EoP) Vulnerabilities**
- **9 Denial of Service (DoS) Vulnerabilities**
- **5 Spoofing Vulnerabilities**
- **2 Security Feature Bypass Vulnerabilities**
- **1 Information Disclosure Vulnerability**
- **1 Tampering Vulnerability**

In conclusion, while Microsoft's February update addressed critical vulnerabilities, the active exploitation of these weaknesses poses a significant threat. This serves as a reminder for companies not to delay security updates and to take immediate action to protect their systems.

https://thehackernews.com/2025/02/microsofts-patch-tuesday-fixes-63-flaws.html

Lazarus Group's LinkedIn Attack:
Fake Job Offers as a Trap

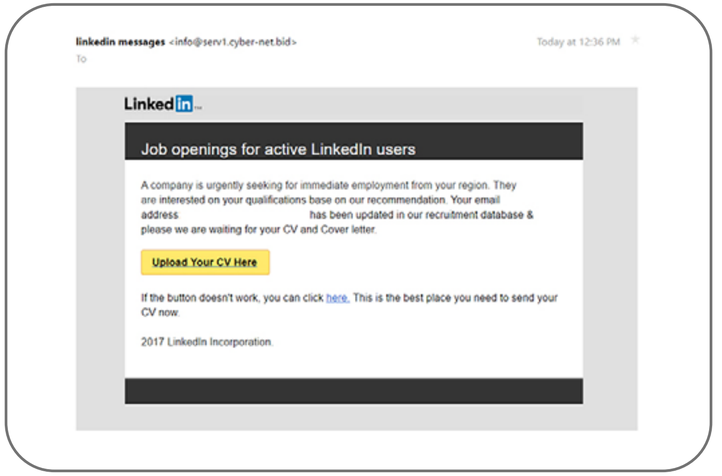
A cybercriminal group, Lazarus, has recently increased its cyber espionage activities using the LinkedIn platform. The aim of this new attack is to target employees working in the finance and tourism sectors. The group attempts to deceive individuals with fake job offers, thereby downloading malware onto their mobile devices.

The attack begins on LinkedIn, with a message designed to attract attention and interest by offering collaboration on decentralized cryptocurrency exchange projects. The message proposes remote work with part-time hours and high salaries. Interested individuals are asked to send their CVs or GitHub profiles, which serves the dual purpose of collecting personal information and convincing the targets.

Such attacks aim to steal users' personal information and compromise their systems. Therefore, it is crucial to avoid suspicious job offers and always remain vigilant.

After the initial contact, the targeted individuals are sent a project through GitHub or Bitbucket. These files contain hidden code that installs malware onto the computers. This malware operates on Windows, macOS, and Linux systems. The primary goal is to steal information from cryptocurrency accounts in the victim's browser. The malware creates a backdoor on the computer, allowing cybercriminals to gain remote control.

https://socradar.io/lazarus-groups-cyber-espionage-involving-linkedin/



Hundreds of Fake Reddit Sites Spread **Lumma Stealer Malware**

The cybercriminal has published nearly 1,000 fake websites impersonating popular sites like Reddit and WeTransfer, luring users into downloading the Lumma Stealer malware.

These fake websites exploit the Reddit brand by initiating a fake discussion on a specific topic. The person starting the discussion requests help to download a special tool, another shares a link by uploading it to WeTransfer, and a third person expresses gratitude, making everything appear legitimate. When unsuspecting users click on the link, they are redirected to a fake WeTransfer site, where the “Download” button triggers the download of the Lumma Stealer malware.

Lumma Stealer Malware Threat

Lumma Stealer is sold to cybercriminals, who distribute it through various means such as GitHub, fake websites, and advertisements. This type of malware steals session tokens to capture passwords and accounts stored in users’ browsers. The stolen data is then used in network attacks or social engineering to acquire sensitive information from companies and individuals.

https://www.bleepingcomputer.com/news/security/hundreds-of-fake-reddit-sites-push-lumma-stealer-malware/

All these fake websites appear legitimate at first glance by imitating the brand name and adding random numbers and symbols. According to investigations, a complete list of pages involved in this social engineering attack has been shared. Within this campaign, 529 fake Reddit sites and 407 fake WeTransfer sites have been found.

Ransomware attack: Medusa group demands up to $15M from victim

Since its first appearance in January 2023, the Medusa ransomware group has been linked to almost 400 attacks, with incidents rising by 42% between 2023 and 2024. In just the first two months of 2025, more than 40 new attacks have been attributed to the group.

Medusa follows a double-extortion model, first stealing data from victims before encrypting their systems. This tactic increases pressure on organizations to meet ransom demands, as refusal often leads to the stolen data being published on the group's leak site.

With the recent disruption of major Ransomware-as-a-Service (RaaS) groups like LockBit and BlackCat, Medusa has emerged as a key player in the cyber extortion landscape. Other ransomware groups, including RansomHub (also known as Greenbottle and Cyclops), Play (Balloonfly), and Qilin (Agenda, Stinkbug, Water Galura), have also expanded their operations.

Ransom demands from Medusa vary widely, ranging from $100,000 to $15 million. The group primarily targets large entities, including financial institutions, government agencies, non-profits, and healthcare providers. Their attacks frequently exploit vulnerabilities in public-facing applications, such as Microsoft Exchange Server, to gain initial access.

Like most ransomware groups, Medusa is financially motivated, with no ideological or political agenda, focusing solely on extorting money from high-value targets across various industries.

https://www.linkedin.com/pulse/medusa-ransomware-hits-40-victims-2025-demands-100k15m-ransom-mafic/

https://thehackernews.com/2025/03/medusa-ransomware-hits-40-victims-in.html

16 Chrome extensions compromised putting over **600,000 users at risk**

A recent cyberattack has compromised 16 Chrome extensions, putting over 600,000 users at risk of having their personal information stolen.

The attackers used a clever phishing scheme to target developers who create extensions for the Chrome Web Store. Once they gained access, the hackers injected malicious code into legitimate extensions, allowing them to steal sensitive data like cookies and login tokens from users.

cyberhaven

On December 27, a company called Cyberhaven revealed that one of their own extensions was affected by the attack. The hackers used the extension to communicate with an external server, download more malicious files, and collect user data.

Threat Overview

The phishing emails were designed to look like they were coming from Google Chrome Web Store Developer Support. They falsely warned developers that their extensions were at risk of being removed for policy violations and asked them to click a link to resolve the issue. This link led to a malicious page that gave the attackers access to a harmful app called “Privacy Policy Extension.”
Experts are now warning that browser extensions, while often overlooked, can access a lot of sensitive user information. “Many organizations don’t even realize which extensions are installed on their systems, and that leaves them wide open to attacks like this,” said Or Eshed, CEO of LayerX Security. This serves as an important reminder to stay vigilant about the security of browser extensions and keep a close eye on what’s being installed.

To stay protected, we recommend reviewing your browser extensions and removing any you don’t recognize or no longer use. Always install extensions from trusted sources, and be cautious of unexpected pop-ups or emails asking you to take action on your browser.

https://www.linkedin.com/pulse/16-chrome-extensions-hacked-exposing-over-600000-users-data-6urvc/

birbank

Should you have any suggestions or feedback, please contact cyberjournal@kapitalbank.az