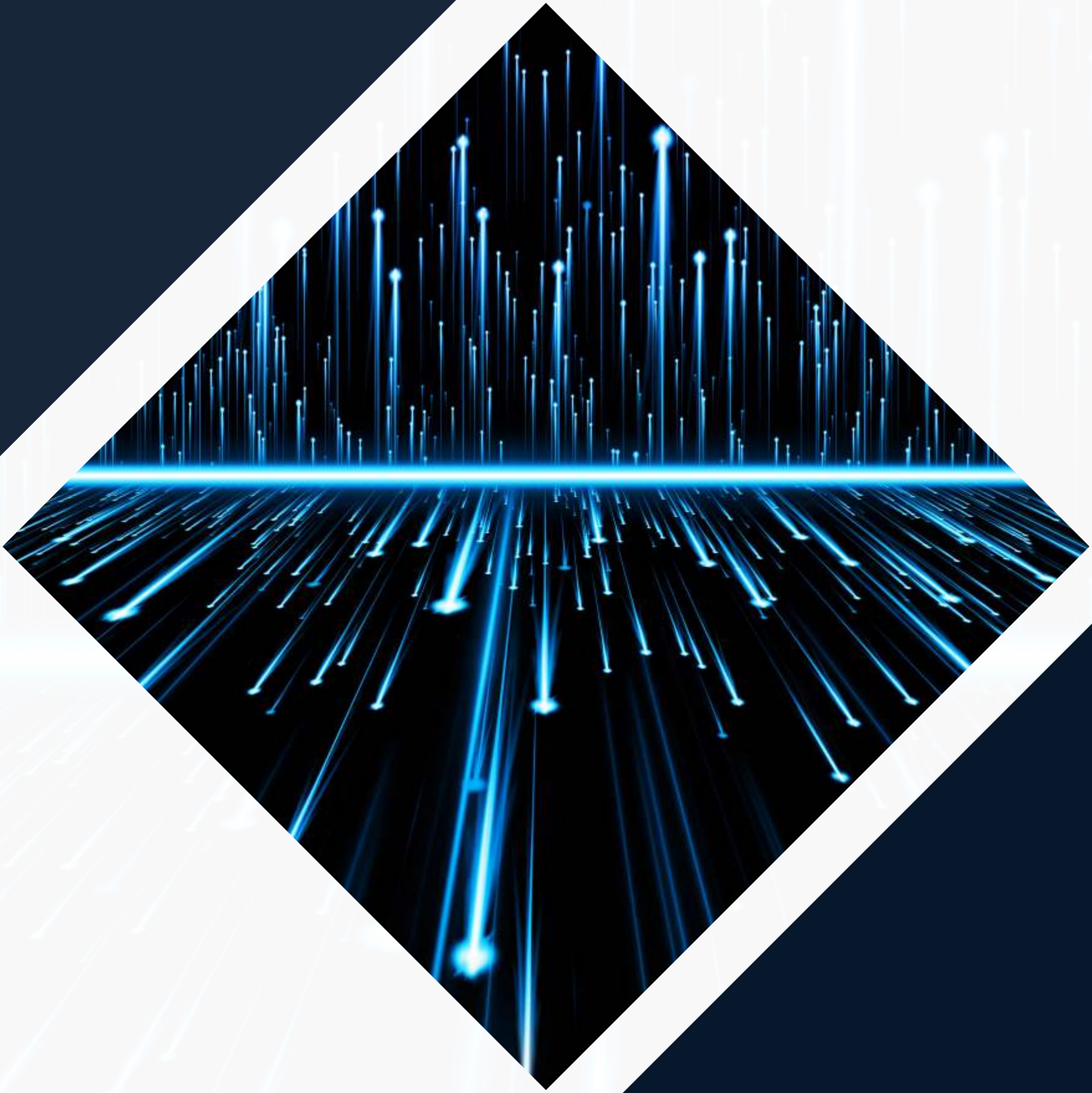

FEBRUARY

THREAT PULSE

THREAT PULSE

PROTECTING THE DIGITAL FRONTIER

TOP OF THE NEWS THIS MONTH

LockBit ransomware returns, restores servers after police disruption

The LockBit gang is restarting its ransomware activities on a different infrastructure shortly after law enforcement breached their servers. They are now targeting more attacks towards the government sector.

On February 19, authorities took down LockBit's infrastructure, which included 34 servers hosting the data leak website and its mirrors, data stolen from the victims, cryptocurrency addresses, decryption keys, and the affiliate panel.

Five days later, LockBit is back and provides details about the breach and how they're going to run the business to make their infrastructure more difficult to hack. Immediately after the takedown, the gang confirmed the breach saying that they lost only the servers running PHP and that backup systems without PHP were untouched.

"Due to my personal negligence and irresponsibility, I failed to update PHP on time." The threat actor mentioned that the victim's admin and chat panels server, as well as the blog server, were operating on PHP 8.1.2 and were likely compromised through a critical vulnerability identified as CVE-2023-3824.

Regarding the alleged hacking by "the FBI" on their system, the cybercriminal suggested it was in response to the ransomware attack on Fulton County in January. This attack potentially risked leaking sensitive information, including details on Donald Trump's legal cases that could impact the upcoming US election. As a result, LockBit aimed to provoke "the FBI" into demonstrating their capability to combat the gang by targeting the .gov sector more frequently.

READ MORE →

TOP OF THE NEWS THIS MONTH

Ongoing Microsoft Azure account hijacking campaign targets executives

A phishing campaign in late November 2023 targeted Microsoft Azure environments, compromising hundreds of user accounts, including senior executives'.

The attacks employ documents sent to targets that embed links masqueraded as "View document" buttons that take victims to phishing pages.

The messages target employees who are more likely to hold higher privileges within their employing organisation, which elevates the value of a successful account compromise.

This user agent has been associated with various post compromise activities, such as MFA manipulation, data exfiltration, internal and external phishing, financial fraud, and creating obfuscation rules in mailboxes.

READ MORE →

Kasseika ransomware uses antivirus driver to kill other antiviruses

The recently discovered ransomware operation 'Kasseika' uses Bring Your Own Vulnerable Driver (BYOVD) tactics, exploiting the Martini driver to disable antivirus software. This tactic allows attackers to escalate privileges to kernel-level, gaining extensive control over system resources.

Because the drivers are legitimately signed, hence trusted by security software, they are neither flagged nor blocked.

Successful exploitation allows attackers to achieve kernel-level privilege escalation, which grants them the highest level of access and control over system resources on a target.

READ MORE →

IN THE NEWS THIS MONTH

New IDAT Loader Attacks Using Steganography to Deploy Remcos RAT

Ukrainian entities in Finland targeted by a malicious campaign distributing Remcos RAT using IDAT Loader.

The attack has been attributed to a threat actor tracked by the Computer Emergency Response Team of Ukraine (CERT-UA) under the moniker UAC-0184.

READ MORE →

New 'Gold Pickaxe' Android, iOS malware steals your face for fraud

A new trojan called 'GoldPickaxe' on iOS and Android uses social engineering to deceive users into scanning their faces and ID documents.

This data might be used to create deepfakes for unauthorized banking access. The malware is linked to the Chinese threat group 'GoldFactory.'

READ MORE →

US says it blocked China cyber-threat but warns hackers can 'wreak havoc'

A China-backed hacking operation targeting civilian infrastructure was disrupted by US officials. The group Volt Typhoon aimed at public sector facilities for China.

Chinese hackers had hijacked a hundreds of US-based small office owned by private citizens and companies, intent on covering their tracks as they sowed the malware, according to the FBI.

READ MORE →

VULNERABILITIES AND EXPLOITS

The Common Vulnerability Scoring System (CVSS) is a free and open industry standard for assessing the severity of computer system security vulnerabilities.

Notable Vulnerabilities and exploits for this month:

CVSS SCORE 9.8

CVSS SCORE 9.6

CVE-2024-20252 & **CVE-2024-20254**
Cisco Expressway Series Cross-Site Request Forgery Vulnerabilities

CVSS SCORE 9.6

CVE-2024-1071
SQL Injection Vulnerability in WordPress

CVSS SCORE 9.8

CVE-2023-40547
Critical Boot Loader Vulnerability in Shim impacting Linux Distros

CVSS SCORE 9.6

PHISHING NEWS

Bumblebee Malware Returns with New Tricks, Targeting U.S. Businesses

The malware Bumblebee reappeared in a phishing campaign targeting US organisations in February 2024. Emails with OneDrive links led to Word documents impersonating Humane.

The dropped temporary file contained a PowerShell command to download and execute the next stage from a remote server stored in the file "update_ver." The subsequent stage involved another PowerShell command to download and run the Bumblebee DLL.

READ MORE

LabHost cybercrime service enables phishing attacks on Canadian bank customers.

The PhaaS platform 'LabHost' aids cybercriminals in targeting North American banks, leading to increased activity. PhaaS platforms offer phishing kits, hosting infrastructure, email content generation, and campaign services for a monthly fee.

Phishing-as-a-Service platforms increase cybercrime accessibility for unskilled hackers, expanding the pool of threat actors and impacting cybersecurity broadly.

READ MORE

Open Redirects Used to Disguise Phishing Links

Phishing attacks are using open redirects hosted on trusted domains to lead users to potentially malicious sites, as noted by Trustwave researchers.

Open redirects are URLs hosted on trusted domains that take users to separate, potentially malicious domains. Trustwave has observed a “significant rise” in phishing attacks using open redirects over the past several months.

READ MORE

Patch Tuesday - February Updates

Microsoft updates:

Microsoft addressed 73 vulnerabilities this February 2024 Patch Tuesday, including two zero-day / exploited-in-the-wild vulnerabilities.

Of the new patches released today, five are rated Critical, 65 are rated Important, and two are rated Moderate in severity.

Critical and Important Vulnerabilities:

CVE-2024-21413 - Microsoft Outlook Remote Code Execution Vulnerability – 9.8 (Critical)

An attacker can exploit this vulnerability via the preview pane in Outlook, allowing them to circumvent Office Protected View and force files to open in edit mode, rather than in the safer protected mode.

CVE-2024-21410 - Microsoft Exchange Server Elevation of Privilege Vulnerability - 9.8 (Critical)

A remote, unauthenticated attacker could use this bug to relay NTLM credentials and impersonate other users on the Exchange server.

CVE-2024-21357 - Windows Pragmatic General Multicast (PGM) Remote Code Execution Vulnerability - 7.5 (Critical)

Enables remote code execution but is confined to adjacent attack scenarios—meaning the attacker must be on the same network segment or connected to the same switch or virtual network as the target.

A full list of Vulnerabilities disclosed by Microsoft can be found here

Patch Tuesday - February Updates

Fortinet updates:

CVE-2024-21762 - FortiOS - Out-of-bound Write in sslvpnd - CVSS 9.6 (Critical)

A out-of-bounds write vulnerability (CWE-787) in FortiOS may allow a remote unauthenticated attacker to execute arbitrary code or command via specially crafted HTTP requests.

READ MORE

CISCO updates:

CVE-2024-20253 - Cisco Unified Communications Products Remote Code Execution Vulnerability – 9.9 (Critical)

Improper access control in Zoom Desktop Client for Windows, Zoom VDI Client for Windows, and Zoom SDKs for Windows before version 5.16.10 may allow an authenticated user to conduct an escalation of privilege via local access.

READ MORE

Other vendors who released updates for February:

ExpressVPN - released a new version to remove the split-tunnelling feature after it leaked DNS queries.

Google - released the Android February 2024 security updates.

Ivanti - released security updates for a new Connect Secure authentication bypass flaw.

Linux -distros release patches for new Shim bootloader code execution flaw.

JetBrains - released security updates for a new critical authentication bypass vulnerability in TeamCity On-Premises.

Mastodon - released a security update to fix a vulnerability that allows attackers to take over any remote account.

SAP - has released its February 2024 Patch Day updates.