# TOP ATTACKS AND BREACHES

- Romanian hospital patients' data management system, Hipocrate IT Platform, was hit by a ransomware attack, leading to data encryption of over 20 Bucharest hospitals. The attack rendered the hospital staff resorting to manual logging and tracking of critical patient data and progress. Another 79 Romanian hospitals using Hipocrate went offline following the attack, which was first detected on February 10. The attackers used Backmydata ransomware, a variant of Phobos.

  *Check Point Harmony Endpoint and Threat Emulation provide protection against this threat.*

- Ransomware gang ALPHV claimed responsibility for the recently disclosed breach of Fortune 500 company Prudential Financial. The company admitted that employees' and contractors' data was compromised, and ALPHV claim that after failed negotiations, the data will be leaked for free on their website.

  *Check Point Harmony Endpoint and Threat Emulation provide protection against this threat*
  *(Ransomware.Wins.BlackCat.ta.*; Ransomware.Win.BlackCat)*

- 200,000 records of Facebook marketplace users' data were leaked on a cyber-crime forum. The data includes phone numbers, emails, and other personal information. The leaker claimed the database was obtained by the Discord user 'algoaston', who hacked a third-party provider of Meta's system.

- Hacker group LulzSec claimed to have compromised 600,000 French social security accounts (CAF) and shared data from 4 accounts as evidence on X (formerly Twitter). The social security agency refuted claims of a breach and advised users to update passwords to avoid future credential-stuffing attacks.

- The FBI initiated a takedown of the Moobot botnet used by APT28, which is affiliated with the Russian military intelligence (GRU). A known cybercrime group first established the network of Moobot-malware infected SOHO routers. It was then repurposed by the GRU to be a global cyber-espionage platform and used to conceal and enable attacks against the U.S. and its allies, including Ukraine, predominantly in spear-phishing and credential harvesting campaigns.

- Researchers have detected a cyber-espionage campaign, orchestrated by Russia-affiliated group TAG-70 (aka Winter Vivern). The threat actor targeted over 80 organizations, including government, military, and national infrastructure entities primarily in Georgia, Poland and Ukraine, as well as central-Asia and Europe. The operation, likely conducted on behalf of Russia and Belarus, has been ongoing since at least December 2020. The group utilized cross-site scripting (XSS) vulnerabilities in webmail servers, similarly to other Russia-linked APTs.

# VULNERABILITIES AND PATCHES

- Check Point Research discovered critical Remote Code Execution (RCE) Microsoft Outlook vulnerability dubbed #MonikerLink (CVE-2024-21413). Microsoft have addressed this flaw in their February's Patch Tuesday. The flaw allows a remote attacker to deploy a malicious link that bypasses the Protected View Protocol, which could lead to credentials leakage and RCE capabilities.

  *Check Point IPS blade provides protection against this threat* *(Microsoft Outlook Malicious Moniker Link Remote Code Execution (CVE-2024-21413))*

- Microsoft's Patch Tuesday also contained security updates for 73 vulnerabilities, including two actively exploited zero-day security feature bypass flaws in Windows SmartScreen and Internet Shortcut File ( CVE-2024-21412 and CVE-2024-21351). Five of the flaws were critical, including denial-of-service, Remote Code Execution, information disclosure and elevation of privileges vulnerabilities.

- Adobe released security updates for multiple products, including Adobe Commerce and Magento, Acrobat and Reader, 3D Painter, FrameMaker and more. Multiple vulnerabilities in these products were given critical scores, and they include Arbitrary Code Execution and security feature bypass flaws, which can allow threat actors to take control of an affected system.

# THREAT INTELLIGENCE REPORTS

- Check Point Research reports on increase in targeting related to Valentine's Day. January saw a 39% increase from the previous month and a 17% increase from the year before in new domains containing 'Valentine' or 'love'. While 1 out of every 8 of these domains was found to be malicious or risky. Moreover, on a weekly basis, 1 out of every 27 organizations faced attempts to access these perilous websites.

- Researchers have analyzed the Hamas-linked wiper malware campaign dubbed as SameCoin. The wiper affects Windows and Android devices and is distributed via phishing emails impersonating the Israeli National Cyber Directorate, luring victims to download supposed "security updates". The campaign employs a sophisticated infection chain, including a loader, wiper, and tasks spreader for Windows, alongside an APK wiper for Android. As well as damaging and wiping files, the campaign also aims to spread propaganda. Researchers attribute the operation to the Hamas-linked Arid Viper APT group (aka APT-C-23, Desert Falcon), based on the low-grade malware quality and elaborate social engineering.

- Financially motivated advanced group Water Hydra (aka DarkCasino) has been actively exploiting the Microsoft Defender SmartScreen bypass vulnerability (CVE-2024-21412) in its campaigns against financial market traders. The group deployed a spear-phishing campaign on forex trading forums and stock trading Telegram channels, and then leveraged the flaw to execute a malicious MSI file.