TOP ATTACKS AND BREACHES

- The fast food brand 'Yum! Brands', operator of leading fast food restaurants including KFC, Pizza Hut and Taco Bell, has been targeted by a ransomware attack. The attack lead to the temporary closure of almost 300 breaches in the United Kingdom. No group has taken claim at this point.

- Vice Society ransomware gang has claimed an attack on the University of Duisburg-Essen, one of Germany's largest universities. The breach took place in November 2022 and the ransomware group has since leaked alleged data from the institution's network.

  Check Point Threat Emulation provides protection against this threat *(Trojan.Wins.ViceSociety.*)*

- Vice Society ransomware gang appears to be behind the attack on Los Angeles Unified School District (LAUSD), the second-largest school district in the United States. The group has reportedly taken files with contractors' personal information, including Social Security Numbers, after two months of activity inside the network between July and September of 2022.

- PayPal has disclosed a data breach which concerns close to 35,000 users. The breach was spotted after accounts were accessed through automated credential stuffing orchestrated by hackers, which exposed some of the users' personal data during December 2022.

- Researchers have published a report on a suspected China-nexus espionage campaign exploiting FortiOS SSL-VPN vulnerability (CVE-2022-42475), as early as October 2022. The threat actors have been using a novel malware dubbed 'BOLDMOVE' with variants for Windows and Linux, to target a European government entity and a Managed Service Provider located in Africa.

- Email marketing firm MailChimp was hacked, marking their second data breach this year. The threat actors behind the attack accessed the data of 133 customers, after conducting a social engineering attack on the company's employees and contractors. Few days after the breach was disclosed, FanDuel sportsbook and betting site issued a warning to its customers as their names and email addresses were exposed in this latest MailChimp breach, which can expose them to phishing attacks.

- A recent report reveals the Russian state-sponsored Gamaredon APT has continued to actively target the Ukrainian government using a new infection technique, with recent attacks leveraging Telegram messaging app.

  Check Point Threat Emulation and Anti-Bot provide protection against this threat *(Technique.Win.LinkRemote.Ia.I; InfoStealer.Win.Gamaredon; Trojan.Win32.Gamaredon.A)*

VULNERABILITIES AND PATCHES

- A critical flaw (tracked CVE-2022-47966) allowing remote code execution without authentication in several Zoho ManageEngine products has been disclosed, with an available proof-of-concept.

  Check Point IPS provides protection against this threat *(Zoho ManageEngine Remote Code Execution (CVE-2022-47966)*

- Git has patched two critical vulnerabilities (tracked as CVE-2022-23521 and CVE-2022-41903), which could be exploited by a malicious actor to achieve remote code execution. An additional Windows-specific flaw impacting the Git GUI (tracked as CVE-2022-41953) was shared and is yet to be remediated.

- CISA has released four Industrial Control Systems advisories, marking several security flaws affecting products from Siemens, GE Digital, Mitsubishi and Contec. The two most critical vulnerabilities are RCE and command injection flaws in Siemens SINEC INS (tracked CVE-2022-45092 and CVE-2022-2068).

- Two vulnerabilities have been published in Netcomm and TP-Link routers (tracked as CVE-2022-4873 and CVE-2022-4874), and when chained together could be weaponized for remote code execution.

- Two flaws in Samsung's official Galaxy App Store were found and fixed (tracked as CVE-2023-21433 and CVE-2023-21434); a PoC is available. The vulnerabilities could enable attackers to install any app in the Galaxy Store without the user's knowledge or to direct victims to a malicious web location.

THREAT INTELLIGENCE REPORTS

- Check Point Research shares recent insights on the latest actions of NoName057(16) against the Czech Republic during the 2023 Czech Presidential Election, marking the first successful attempt by Russian-affiliated hacktivist groups to disrupt key websites during democratic western elections.

- Check Point Research examined Cloud-based networks and found a significant growth of 48% in the number of attacks per organization, experienced in 2022 compared to 2021.

- Researchers have uncovered and took down a massive ad fraud operation dubbed 'Vastflux' that managed to spoof over 1,700 mobile applications from 120 publishers, mostly for iOS. The operators abused VAST (Digital Video Ad Serving Template) and used the "fast flux" evasion technique, leading to the scheme running inside apps on nearly 11 million devices.

- Data gathered throughout 2022 shows a major decline in ransomware profits, with a drop of 40% compared to the two years prior. The drop was driven from victims refusing to pay attackers, and not from fewer attacks, as 2022 was one of the most active years in ransomware activity.