TOP ATTACKS AND BREACHES

- The California cities of Oakland and Modesto have been targeted by ransomware attacks, disrupting services in the former and the police network in the latter. Also in California, healthcare company 'Heritage Provider Network' has confirmed that medical and personal information of more than 3 million patients had been disclosed in a ransomware attack against the company in December.

- A British member of Parliament has disclosed that his email account had been hacked in a spear-phishing attack. According to reports, the threat actor behind the attack is the Russian-government APT group Seaborgium, which has lately been targeting UK politicians, journalists and activists.

- The group behind the massive 'ESXiArgs' ransomware campaign, which affected thousands of VMware ESXi hosts, has updated their malware's encryption process. The updated version of the malware prevents the potential recovery method that was recommended by researchers, as it now also encrypts the files that could have been used to trigger the recovery process.

  Check Point IPS provides protection against this threat *(VMWare OpenSLP Heap Buffer Overflow (CVE-2019-5544; CVE-2021-21974))*

- Social media platform Reddit suffered a security breach, after an employee fell victim to a phishing attack. According to the company's statement, while internal documents and source code were stolen, user information and credentials have not been impacted.

- One of Israel's leading universities, 'The Israel Institute of Technology' (Technion), has been targeted by a ransomware attack, forcing it to shut down its network and postpone final exams to the upcoming semester. Suspicions were raised that the attack might be politically or personally motivated, as the perpetrators are a previously unknown group and the ransom note included nonstandard messaging.

- American grocery delivery company 'Weee!' has confirmed that a security breach had caused disclosure of customer information, after a database including more than a million of the company's customers' accounts had been leaked on online forums.

- US and South Korean agencies warn of recent ransomware efforts originating from North Korea. According to the report, North Korean government-sponsored ransomware attacks, specifically targeting the healthcare industry, are used to generate funds for further malicious activity.

- Canada's largest book retailer, Indigo, has been forced to shut down its website and all online operations due to a cyberattack. It is still unknown whether customer information has been compromised.

VULNERABILITIES AND PATCHES

- 'GoAnywhere' Managed File Transfer platform has released version 7.1.2 to address CVE-2023-0669, a zero-day remote code execution vulnerability which has recently been widely exploited in the wild. The 'Cl0p' ransomware gang has assumed responsibility for exploiting the vulnerability, and claims to have abused it to exfiltrate data from more than 130 organizations.

  Check Point IPS provides protection against this threat *(GoAnywhere MFT Insecure Deserialization)*

- The OpenSSL project has published a security advisory which contains fixes for 8 vulnerabilities across multiple versions of OpenSSL. One of the vulnerabilities is considered to be of High severity, as it allows a remote attacker to read memory content and cause denial of service.

- Android has released its February security patch. More than 20 vulnerabilities were fixed in the patch, some of which could lead to remote code execution.

THREAT INTELLIGENCE REPORTS

- Check Point has published its 2023 Security Report, which reviews significant developments in the cyber landscape during the past year. Among the trends analyzed by Check Point are the shift of ransomware groups to data exfiltration and extortion, the increasing threat of nation-state backed hacktivism, and the observed rise in attacks targeting cloud-based networks in 2022.

- Check Point's researchers found that threat actors are working their way around ChatGPT's restrictions to create malicious content and to improve the code of a basic Infostealer malware from 2019.

- Researchers have analyzed multiple campaigns using malicious packages in attempted supply-chain attacks. One Pypi (Python) campaign created over 450 crypto-related packages that would replace cryptocurrency wallet addresses, while another registered 5 packages that deliver credential-stealing malware. Also observed was an npm (Java) campaign, which delivered a remote-access Trojan.

- New information-stealer malware used by the Russian-affiliated Nodaria APT group has been detected. The malware, which was observed in a campaign targeting Ukraine, has sophisticated information gathering capabilities as well as multiple evasion techniques.

- Researchers have analyzed a new campaign by mercenary APT group Dark Caracal. The campaign affected more than a dozen countries in Latin America, successfully infecting more than 700 hosts. The payload is a remote access Trojan with various spyware and remote control capabilities.

- A new APT group dubbed 'NewsPenguin' has been discovered. The group has been targeting organizations in Pakistan using a sophisticated spyware tool. The payload was delivered using spear-phishing emails related to an expo in Pakistan, targeting the expo's visitors.