Check Point Research
WEEKLY INTELLIGENCE REPORT

## TOP ATTACKS AND BREACHES

- The Portuguese airline company TAP Air Portugal was the victim of an alleged ransomware attack launched by the Ragnar Locker ransomware gang. The airline company reported that the attack was blocked and that no unauthorized access was made to customer data, yet certain functionalities of the app and the website were impacted.

- Hive ransomware gang has launched an attack against Damart, a French clothing company with a revenue of $390 million and over 130 stores worldwide. The attack impacted some of the company's systems and disrupted normal operations in over 90 of its stores.

  *Check Point Harmony Endpoint, Anti-Bot and Threat Emulation provide protection against this threat*
  *(Ransomware.Hive.A; Ransomware.Wins.Hive.ta.B )*

- A traffic jam was generated in Moscow in a kind of physical DDoS attack, as attackers hacked Russian taxi service Yandex, and ordered dozens of cars to a specific location. The Anonymous collective claims to be behind this attack.

- Chile has been the victim of a ransomware attack that targeted a government agency's Microsoft and VMware ESXi servers. Chile's cybersecurity incident response team has not provided a response on which ransomware group was behind the attack, or which government agency was targeted.

- Security researchers have revealed a new Instagram phishing campaign in which threat actors have targeted thousands of unsuspecting Instagram users with a fake email that lured them to fill out a form and claim their alleged verification badge (blue-badge).

- The ALPHV ransomware group has launched an attack against Italy's energy agency *Gestore dei Servizi Energetici SpA* (GSE) over the weekend. GSE has reported that it has taken down its website and IT systems in order to keep the threat actors from gaining access to data. The company's website is still offline a week after the cyberattack was launched.

- Samsung disclosed a data breach and reported that the threat actors stole personal information belonging to customers, including names, contracts, dates of birth, etc. The company mentioned that no financial information was stolen and they are notifying customers of the incident.

# VULNERABILITIES AND PATCHES

- Google has released a patch for a zero-day high-severity security vulnerability tracked as CVE-2022-3075. The vulnerability was the result of insufficient data validation in Mojo runtime libraries.
- Apple has released security updates to a remote code execution zero-day vulnerability that was discovered earlier this month in WebKit, the browser engine used by Safari and other apps, tracked as CVE-2022-3289.
- Microsoft has discovered a high severity vulnerability in the TikTok app for Android (CVE-2022-28799) that could have allowed attackers to take over accounts. The vulnerability has been patched.

# THREAT INTELLIGENCE REPORTS

- Security Researchers have conducted an analysis of Raspberry Robin infection to reveal what may be the objectives of the threat actors behind the malware. Following the investigation, the researchers have found similarities between the Raspberry Robin infection and the Dridex malware and as such, concluded that there may be a link between Raspberry Robin infections and the Russian cybercriminal group – 'Evil Corp'.
- Security Researchers have discovered a new Remote Access Trojan (RAT) dubbed CodeRAT which specifically targets Farsi-speaking software developers using a Microsoft Word document that contains a Microsoft Dynamic Data Exchange (DDE) exploit. The researchers have been able to identify the malware creator, who then published the RAT's source code in his public GitHub account.
- The National Security Agency (NSA) and the Cybersecurity and Infrastructure Security Agency (CISA) have released a page designed to provide guidance for developers to ensure stronger security practices in the face of supply chain attacks.
- Security researchers have highlighted a risky feature in one third of Python packages - when a Python package is downloaded, automatic code is being executed, which exposes developers to a higher risk of a supply chain attack.
- Microsoft has announced that it plans to disable basic authentication in Exchange Online tenants worldwide in order to improve security and make it more difficult for threat actors to steal sensitive information using man-in-the-middle attacks. Basic authentication will be replaced permanently by modern authentication methods on the first week of January 2023.