December 23 – 29, 2019

YOUR CHECK POINT

THREAT INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- Check Point researchers have detected a phishing campaign impersonating the royal bank of Canada and other Canadian banks. The attack contained emails sent to targeted customers that use look-alike domains to appear genuine. The emails included pdf attachments, with links to phishing websites that asked for the victim's bank account credentials.
- The U.S. Coast Guard Marine (USCG) has reported that a Maritime Transportation Security Act (MTSA) regulated facility has been hit by Ryuk ransomware, entering the system via an email phishing campaign allowing the attackers to access and encrypt significant IT files, preventing the facility's access to them. The attack took down the facility for over 30 hours.

  Check Point SandBlast provides protection against this threat
- Alaskan airline carrier RavnAir Group has experienced an undisclosed cyber-attack on their company's IT network forcing them to ground flights and disconnect their entire Dash 8 aircraft maintenance system. The company had to cancel 6 flights, affecting 260 passengers during the holiday season.
- IoT equipment provider Wyze has suffered a server leak exposing online details of 2.4 million users. The leak occurred from an exposed online Elasticsearch database system.
- UAE-based company "ToTok", a mobile messaging and voice call app, has been used by the government as a surveillance tool. Authorities were using it to spy on its users, tracking their conversations and movements due to lack of end-to-end encryption security. The app, used in UAE and most of the Middle East, has been removed from Apple and Google's online stores.
- A new Trojan called "lampion", a banking Trojan that aims to hijack sensitive information, has been spreading via a phishing campaign impersonating the Portuguese government finance and tax authorities.

  Check Point Anti-Virus blade provides protection against this threat (lampion.TC.x)

VULNERABILITIES AND PATCHES

- Google chrome browser has been affected by Magellan 2.0 vulnerabilities. The latest update to Chrome (version 79.0.3945.79) has patched 5 vulnerabilities that steam from SQLite cloud enabling RCE. These vulnerabilities can be exploited remotely via a crafted HTML page to run an array of malicious attacks.
- NVIDIA released a new version of Geforce Experience 3.20.2, to patch a vulnerability that allowed an attacker with local system access to corrupt a system file when GameStream is enabled. Successful exploit may lead to denial of service or escalation of privileges.
- A critical vulnerability in Citrix Application Delivery Controller (NetScaler ADC) and Citrix Gateway (NetScaler Gateway), tracked as CVE-2019-19781, could be exploited to access companies' networks. 80,000 companies are at risk worldwide. Citrix has published a guide to mitigate the threat.
- A zero-day vulnerability in Dropbox for Windows allows attackers to perform privilege escalation and escalate from a user to system authority. The vulnerability resides in the DropBoxUpdater service, which is responsible for keeping the client application up to date. A patch has not been released yet.

THREAT INTELLIGENCE REPORTS

- A new P2P Botnet named "Mozi" is targeting Netgear, D-Link, and Huawei routers using weak telnet passwords. The botnet is related to the Gafgyt malware as it reuses some of its code. The botnet's main purpose is to conduct DDoS attacks.

  Check Point Anti-bot blades provide protection against these threats (Botnet.Win32.Mozi-P2P.TC.a)
- Researchers have reported that the Chinese state-sponsored group ATP20 has been bypassing the RSA secure ID two-factor authentication (2FA) in a recent wave of attacks targeting government entities and managed service providers (MSPs). Analysts claimed the attack was conducted using stolen software token, although the attack details remain unclear.
- Russia's national internet infrastructure, RuNet, has been tested and successfully disconnected from the internet, and Internet traffic was re-routed internally. In addition, the government tested several disconnection scenarios, including a scenario that simulated a hostile cyber-attack from a foreign country.

For comments, please contact: TI-bulletin@checkpoint.com