December 16 - 22, 2019

YOUR CHECK POINT
THREAT INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- An Emotet infection has caused Frankfurt to shut down its IT network, to refrain from the malware being used to launch a ransomware attack. Also in Germany, the federal cybersecurity agency has issued a warning about Emotet, following a campaign that included emails supposedly sent from the German federal authorities.

  Check Point SandBlast and Anti-Bot blades provide protection against this threat (Trojan.Win32.Emotet)

- Personal data of about 100,000 Singapore defense personnel may have been compromised after attack on two security force vendors – ST Logistics and HMI Institute of Health Sciences.

- CoyBot (aka BasBanke) mobile banking Trojan has resurfaced after a year of dormancy, targeting 9 different banking apps in Brazil.

  Check Point SandBlast Mobile provides protection against this threat

- The gaming company Zynga has been breached, and login credentials of 170 million users were compromised. This includes players of Draw Something and Words With Friends. The hackers are suspected to be of Pakistani origins.

- Twitter has warned its users in India about a threat in the Twitter app for Android, and asked to install the latest update. Threat actors injected malicious code into the app, which might have allowed them to access to non-public account information and the option to take control over the account.

- Canadian largest healthcare lab provider, LifeLabs, has suffered a data breach that compromised private health information of nearly 15 million Canadians that could include name, address, email, login, passwords, date of birth, health card number and lab test results. The company paid an undisclosed amount in ransom to retrieve the stolen data.

VULNERABILITIES AND PATCHES

- Cisco Security Appliances in risk after resurrection of old vulnerability (CVE-2018-0296), according to a warning issued by Cisco. The attack can cause the appliance to reload by simply sending it a crafted HTTP request, making it highly susceptible to a DoS attack. The attack can also be leveraged to view sensitive system information. The vulnerability has a patch available.

  Check Point IPS blade provides protection against this threat (Cisco Adaptive Security Appliance Web Services Denial of Service)

- Microsoft has released a patch to a SharePoint Server vulnerability (CVE-2019-1491) that allowed an attacker to obtain sensitive information using a specially crafted request to a susceptible server.

- TP-Link has patched a critical zero-day vulnerability (CVE-2017-7405) that could be used to allow attackers to login to Archer routers without passwords, and spread laterally through the network.

- Drupal has released a critical security update for its open-source content management software, for a vulnerability involving .tar and similarly packed files, which would have allowed attackers to overwrite sensitive files on a targeted server. Several other moderately critical issues were patched as well.

THREAT INTELLIGENCE REPORTS

- Check Point researchers have found a way to crash WhatsApp on multiple phones in a shared group, causing the app to enter a crash loop as long as the group is still active, forcing the user to delete it and lose their data if they wish to continue using WhatsApp.

- A new RAT (Remote Access Trojan) by the North Korean based Lazarus APT group (WannaCry, Sony Pictures attack) has been discovered. The new RAT, named Dacls, is unique in targeting Linux as well as Windows OS. Its main functions include command execution, file management, process management, test network access, C2 connection agent, and a network scanning module.

  Check Point Anti-Bot blade provides protection against this threat (RAT.Win32.Dacls.TC)

- A Lithuanian scammer who successfully conducted business email compromise attacks against Google and Facebook, stealing $120 million, has been sentences to 5 years in prison. In his 2013-2015 phishing attacks, he sent requests for payment, allegedly from a Taiwanese hardware manufacturer who works with both companies. He pleaded guilty of fraud, identity theft and money laundering.

- A new phishing campaign is spreading Emotet and other malware using the premise of invites to demonstrations of Greta Thunberg, the Swedish environmental activist.

  Check Point SandBlast and Anti-Bot blades provide protection against this threat (Trojan.Win32.Emotet)