November 6-11, 2018

Check Point SOFTWARE TECHNOLOGIES LTD.

YOUR CHECK POINT

THREAT INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- Personal details of nearly 700,000 American Express India customers have been exposed online via an unsecured MongoDB server. The exposed data includes phone numbers, full names, email addresses, card type description fields, as well as accounts' details to americanexpressindia.co.in.
- Several Italian ministries and institutions have suffered major data breaches and defacements, attributed to Anonymous-affiliated groups celebrating 'Guy Fawkes Day'. The victims included Italy's National Research Center, the Institute for Education Technologies, and State Police Association.
- A new IRC botnet has been spotted in the wild, targeting mostly IoT devices and Linux servers, but also Android and Windows systems. The botnet, dubbed 'Shellbot' is able of performing port scanning, distributed denial of service (DDoS) and SSH brute force attacks against large organizations.

  Check Point Anti-Bot and Anti-Virus blades provide protection against this threat (Trojan.Linux.Shellbot)
- Security researches have revealed a new spam Botnet dubbed "BCMPUPnP_Hunter", which may have already infected 400,000 machines. The botnet targets mainly routers with the BroadCom Universal Plug and Play (UPnP) feature enabled, including router models from, D-Link, Linksys/Cisco, ZyXEL and others.

  Check Point Anti-Bot and Anti-Virus blades provide protection against this threat (Trojan.Linux.BCMPUPnP_Hunter)
- Threat actors have created a .com version of the voter information website "vote411.org" in order to conduct a technical support scam. The threat actors redirected visitors from macOS and iOS platforms to pages showing fake infection alerts, in purpose to trick the victims into paying for fake services.
- HSBC Bank USA has suffered a major data breach as unauthorized attackers managed to access online accounts of the financial institution. The exposed data includes personal customers' personal information as well as account balances, transaction history, payee account information, and more.

©2018 Check Point Software Technologies Ltd. All rights reserved. [Protected] Non-confidential content

VULNERABILITIES AND PATCHES

- Check Point researchers have discovered a critical vulnerability in DJI Drones in which the same login cookie can be used to connect to several DJI users. The vulnerability may allow attackers to access various user platforms, as well as photos, videos, flight map and logs, live camera feed and more.
- Nginx open source web server software has released a security update addressing several denial-of-service (DoS) vulnerabilities affecting more than million unpatched nginx web servers.
- Remote code execution vulnerability has been found affecting Icecast open-source streaming media server, and allowing potential attackers to take off the broadcast of online radio stations.
- A zero-day vulnerability in the popular open source virtualization software VirtualBox has been spotted. The vulnerability may allow an attacker or a malicious program with root or administrator rights to escape virtual machine, and execute code on the operating system of the host machine.
- Zero-day arbitrary file deletion vulnerability has been discovered in the popular WooCommerce WordPress plugin. The vulnerability may allow a malicious or compromised privileged user to reset administrator accounts' password and gain full control over the unpatched websites.
- Security researchers have discovered multiple critical vulnerabilities in the popular self-encrypting solid state drives (SSD) that may allow an attacker to decrypt disk encryption and recover protected data by bypassing password-based authentication.

THREAT INTELLIGENCE REPORTS

- Security researchers have uncovered 'FastCash' Trojan used by the Lazarus North Korean APT Group to conduct fraudulent ATM attacks. The attackers compromise the switch application servers handling ATM transactions using credentials stolen from banks' networks, and process the ATM withdrawal requests.

  Check Point Anti-Virus blade provides protection against this threat *(Trojan.Win32.FASTcash)*

- Security researchers have discovered a new Emotet campaign using malicious macros embedded inside Word and PDF mail attachments. The new campaign contains new and improved attack modules, including an email exfiltration module designated to harvest email messages from infected computers.

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

- A new Crypto-miner variant has been discovered targeting Linux and capable of hiding its malicious process's presence from monitoring tools by utilizing a rootkit. The infected systems could only indicate the high CPU utilization, without detecting the source process causing it.