March 19 - 25, 2018

Check Point
SOFTWARE TECHNOLOGIES LTD.

YOUR CHECK POINT THREAT INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- The City of Atlanta computer network has fallen victim to a ransomware attack that has encrypted computers of the City Hall and other municipal services, and affected various online services in the city. The ransom note presented on affected machines demand 0.8 Bitcoin ($6,750) to unlock a single computer, or 6 Bitcoins ($50,700) to unlock the entire network.

  Check Point SandBlast and IPS blades provide protection against this threat (Suspicious Executable Containing Ransomware)

- Orbitz, an Expedia-owned travel site has said it may have experienced a breach leading to the disclosure of 880K payment cards used for online purchasing, along with other personal information belonging to customers. The incident took place somewhere between October 2016 and December 2017.

- A new crypto-mining campaign has been discovered to be targeting Linux servers, by exploiting vulnerability in Cacti's Network Weathermap log-in. The campaign is focused on Japan, Taiwan, China, the US and India, and seems to have earned the attackers at least $75K in Monero cryptocurrency.

  Check Point IPS and Anti-Bot blades provide protection against this threat (Command Injection Over HTTP; Jenkins CI Unauthenticated Remote Code Execution; Operator.Jenkinsminer; Jenkinsminer.; Trojan.WIN32.XMRig.A)*

- A new crypto-miner dubbed GhostMiner has been spotted in the wild as a part of a mining campaign. GhostMiner is a fileless crypto-miner harvesting Monero. While being very evasive and undetected by many security vendors, it seems to have only limited monetary success, as the Monero wallet used in the campaign has earned a mere $200 worth of Monero within three weeks of activity.

  Check Point IPS and Anti-Bot blades provide protection against this threat (Oracle WebLogic WLS Security Component Remote Code Execution; Trojan.WIN32.XMRig.A)

- The UK National Lottery, Camelot, has stated on a potential security incident. Camelot had monitored some suspicious activity on 150 players' online lottery accounts, which included unauthorized log-ins and in 10 accounts even some abusive activity using the compromised accounts. Camelot assures that its core systems weren't affected in the incident, and that no victim suffered any financial damage.

VULNERABILITIES AND PATCHES

- A critical vulnerability has been discovered and patched in Windows Remote Assistance feature, affecting all Windows versions. Attackers may obtain sensitive information from target machines.

  Check Point IPS blade provides protection against this threat (Microsoft Windows Remote Assistance XXE Injection Information Disclosure (CVE-2018-0878))

- A buffer overflow vulnerability has been exposed in MikroTik RouterOS SMB service, which might allow remote code execution on attacked routers.

  Check Point IPS blade provides protection against this threat (MikroTik RouterOS SMB Remote Code Execution (CVE 2018 7445))

- Citrix has released security updates for several XenServers versions. The updates address 3 vulnerabilities, which if exploited, may allow a malicious administrator of a guest VM to crash the host, and in some cases even allow compromising the host.
- Drupal has released a security advisory on a coming security update for a highly critical vulnerability in several Drupal versions. The update will also be released for no-longer supported Drupal versions.
- Check Point's researchers have published a review on the recent reveal of flaws in AMD processor chips, verifying the existence of the vulnerabilities in RYZENFALL-1 and RYZENFALL-3. The AMD flaws are 13 critical vulnerabilities suspected by researchers to exist in AMD processors. AMD confirmed their existence, and committed to issue security updates in the coming weeks.
- A major security flaw has been discovered in cryptocurrency hardware wallets made by Ledger, a French producer of physical keys safeguard. The flaw, an insecure microcontroller, was discovered by a 15-year-old security researcher from the UK.

THREAT INTELLIGENCE REPORTS

- A new report describes recent changes in the Trickbot banking Trojan, which include the development of screen-locking capabilities and the implementation of lateral movement methods.

  Check Point Anti-Bot and Anti-Virus blades provide protection against this threat (Operator.Trickbot; Trojan.Win32.Trickbot)

- According to researchers, crypto-mining malware have recently started to target cloud infrastructure by attacking Docker and Kubernetes systems.
- A new report on search-autocomplete manipulations finds that the malicious use of it for threat activity is widespread. Hundreds of thousands of manipulated terms are used to distribute scams, phishing and malware in common search engines, with one in every 200 Google search suggestions abused this way.