October 22 – 28, 2018

YOUR CHECK POINT

THREAT INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- Some 9 million customers of the Hong Kong-based airline Cathay Pacific were affected by a data breach, in which passport numbers, identity cards and personal information was collected.
- British Airways has announced that last September's data breach had a greater impact than previously believed, as further 185,000 customers may have had their banking information stolen.
- The website of the Saudi summit "Future Investment Initiative (FII)" has been defaced with messages against Saudi Arabia's government, and with protest against murder of the journalist Jamal Khashoggi. The threat actors have also leaked sensitive information of government employees.
- New findings reveal that the UK GCHQ intelligence agency was behind the attack against the Belgian telecommunications company "Belgacom". Apparently the motive to target Belgacom International Carrier Services is the large amount of Middle Eastern roaming traffic handled by the company.
- Personal data of 10,000 Raley's pharmacy customers has been compromised, as an unprotected company laptop was stolen. Data includes medical condition and prescription drugs.
- FilesLocker is a new Ransomware offered for sale on a Chinese underground forum, sold as ransomware-as-a-service in an affiliate program mode. At this point, its targets include mainly Chinese targets.

  Check Point SandBlast provides protection against this threat

- A new massive Denial of Service botnet dubbed DemonBot has been leveraging servers with vulnerable Hadoop installation to increase its power in preparation for a massive DDoS attack.

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

- Triton, a malware designed to attack industrial control systems and cause physical damage, is now estimated to be orchestrated by a Russian state-sponsored research institute.

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

VULNERABILITIES AND PATCHES

- A critical privilege escalation flaw has been found in X.Org Server package, impacting multiple Linux distributors such as Debian, Red Hat and Ubuntu..
- Researchers have discovered a unique vulnerability in the Cisco WebEx video software. The bug allows remote execution of commands via a component of the WebEx client, even when the software does not listen for remote connections.
- A proof-of-concept has been published for a new zero-day exploit for Windows operating system. The exploit resides in Microsoft Data Sharing service and allows privilege escalation.

THREAT INTELLIGENCE REPORTS

- In response to the growing appearance of mobile banking Trojans on Google Play Store, researchers have analyzed 29 sophisticated mobile bankers which feature tailor-made phishing forms delivery and stealth functionalities.

  Check Point SandBlast Mobile customers are protected from this threat

- New malware targeting Mac OS has been spotted in the wild, capable of injecting ads into encrypted web traffic. The malware installs additional components on the infected device, allowing it to modify the network configuration and to intercept and replay web traffic using man-in-the-middle techniques.
- Security researchers have discovered a new DDoS-for-hire service dubbed "0x-booter". The service is powered by the Bushido IoT botnet and allows users to conduct attacks in a cost ranging from $20 to $150, depending on the number and duration of the attack and on "customer support" level.

  Check Point IPS and Anti-Virus blades provide protection against this threat (Dasan GPON Router Authentication Bypass; Huawei HG532 Router Remote Code Execution; Realtek SDK Miniigd AddPortMapping SOAP Action Command Injection; Eir D1000 Routers Remote Code Execution; Botnet.Win32.Mirai; Botnet.Win32. bushido)

- Security researches have published a report describing a new sophisticated downloader dubbed "sLoad", which delivers Ramnit banking Trojan. sLoad fingerprints the infected systems using geofencing, allowing the attackers to choose targets of interest for the payloads of their choice.

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

- Researchers have investigated a new North Korean cryptocurrency scam called Marine Chain, run by a North Korean network based in Singapore. Victims are lured into purchasing a coin allegedly backed by real-world assets, and once enough purchases are made the shop is closed.
- The potential vulnerabilities of voting machines and infrastructure are reviewed in an article which covers attack vectors such as politically-oriented phishing scams and voting machines hacking.