June 15 – 21, 2020

YOUR CHECK POINT
THREAT INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- Check Point Research has exposed an ongoing phishing campaign designed to collect Office365 credentials. To evade detection, threat actors exploited an Oxford University mail server to send malicious emails, abused an Adobe campaign redirection tool, and then used a Samsung domain to take users to a Microsoft Office 365-themed phishing website.

- New Android spyware dubbed ActionSpy targets users in Tibet, Turkey, and Taiwan, with a specific focus on Uyghur Muslims. The campaign is attributed to the Earth Empusa threat group (aka POISON CARP/Evil Eye) which had previously targeted Tibetan and Uyghurs groups. The malware is spread through watering hole attacks from pages distributed via phishing emails.

  Check Point SandBlast Mobile provides protection against this threat

- Patient records of more than 230K Indonesian COVID-19 patients have been leaked, including patients' names, addresses, telephone numbers, citizenship, diagnosis date, result, and more.

- "Operation In(ter)ception", a cyber-espionage and BEC campaign targeting employees of aerospace and military organizations in Europe and the Middle East, has been reported by researchers. The operation, attributed to the North Korean linked Lazarus APT group, used LinkedIn to approach victims with job proposals, posing as HR managers of well-known companies in the aerospace and defense industries.

- US chipmaker MaxLinear had been breached and systems encrypted by the Maze ransomware operators who later leaked 10GB of the company's accounting and financial information out of the alleged 1TB of data stolen in a double-extortion attack.

  Check Point SandBlast and Anti-Bot blades provide protection against this threat *(Ransomware.Win32.Maze)*

- Operations of the Australian beverage company, Lion, have been shut down due to ransomware attack. The attack is the latest in a series of ransomware attacks to hit Australian companies, such as Toll logistics and BlueScope Steel Limited.

- Nearly 270 GB of sensitive files from police departments across the US have been leaked online on the Distributed Denial of Secrets (DDoSecrets) leak site in a collection dubbed "BlueLeaks". The files contain highly sensitive information from 24 years of police work including financial data, PII, operational information regarding suspects and more. The source of the compromise is a web service company, Netsential, used by multiple law enforcement and other government agencies across the United States.

VULNERABILITIES AND PATCHES

- Nineteen newly discovered vulnerabilities in a low-level TCP/IP software library, designed in the 1990s, affect billions of IoT devices. Four of the vulnerabilities, dubbed Ripple20, are ranked critical and some may result in remote code execution. Affected devices range from home devices to health care, industrial gear, aircraft devices and more.

  Check Point IPS blade provides protection against this threat *(customers need to turn on "Packet Sanity" under Inspection Settings)*

- Adobe has addressed 18 critical code execution flaws in After Effects, Illustrator, Premiere Pro, Premiere Rush, and Audition products.

- Drupal has released security updates to address multiple security vulnerabilities, including a critical flaw tracked as CVE-2020-13664 that could be exploited by an attacker to execute arbitrary PHP code.

- Oracle has addressed two critical flaws in its E-Business Suite (EBS) that could allow a remote and unauthenticated attacker alter financial reports without leaving a trace. An estimated 50 percent of Oracle EBS customers have not deployed the patches to date.

  Check Point IPS blade provides protection against this threat *(Oracle E-Business Suite SQL Injection (CVE-2020-2586))*

THREAT INTELLIGENCE REPORTS

- Security assessment performed on behalf of 28 telecom operators in Europe, Asia, Africa and South America has found vulnerabilities in the GPRS Tunneling Protocol (GPT) for cellular communication. Reported flaws could be exploited to intercept user data and carry out impersonation, fraud, and denial of service (DoS) attacks affecting 2G-5G mobile network generations.

- Australia's Prime Minister has stated that Australia is being targeted by a sophisticated, state-sponsored cyber actor "across a range of sectors, including all levels of government, industry, political organizations…and operators of other critical infrastructure". The Australian Cyber Security Center (ACSC) published a detailed advisory describing related TTPs and IoCs. Previous report by Australia's Intelligence agency determined China was behind a cyber-attack on its parliament, but recommended keeping the findings secret in order to maintain trade relations with Beijing.