August 12 - 18, 2019

Check Point
SOFTWARE TECHNOLOGIES LTD.

YOUR CHECK POINT THREAT INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- Researchers have discovered an online unsecured 23-GB ElasticSearch archive containing fingerprints, facial recognition information and unencrypted usernames and passwords of one million people. The database belongs to Suprema Security Company responsible for biometric locking systems used by the UK police, defense contractors, banks and more.

- A phishing campaign targeting Chinese government officials and state owned enterprises has been detected. The campaign uses spoofed login pages to steal users' credentials and has been attributed to the BITTER APT group previously linked to India.

  Check Point Zero-Phishing protects against this threat

- Czech Republic parliamentary committee blames foreign state for a recent cyberattack on Czech foreign ministry. Previous attack on 150 email accounts of the foreign ministry in 2016 was attributed by the Czech spy agency to Russia.

- 700,000 Choice Hotels customer records have been stolen; hackers left a ransom note but failed to delete the data. The company's MongoDB had been left open for four days to allow a partner vendor to work on a proposal, which was enough time for security researchers to locate and alert the company but also for the attackers to copy it.

- European Central Bank has shut down its BIRD website (Banks' Integrated Reporting Dictionary) after detecting a cyberattack dating back to December 2018, which allowed attackers to access users' contact information.

- Huawei technicians in Uganda and Zambia have helped local governments spy on political opponents, and collected information leading to their arrest. Employees reportedly assisted government officials to break into WhatsApp apps and groups, access phones and Facebook pages belonging to opposition activists and bloggers and retrieve locations and other data.

VULNERABILITIES AND PATCHES

- Microsoft has released patches for a new family of vulnerabilities called “DejaBlue”, affecting RDP (Remote Desktop Protocol) protocol in Windows version 7 and newer, two of which are “wormable”. Microsoft August patch Tuesday addressed over 90 vulnerabilities, 29 of which rated critical.

  Check Point IPS blade protects against this threat (Microsoft Edge Chakra Scripting Engine Memory Corruption (CVE-2019-1139); Microsoft Outlook Memory Corruption (CVE-2019-1199); Microsoft Code Remote Code Execution (CVE-2019-1201); Microsoft Windows Kernel Elevation of Privilege (CVE-2019-1159); Microsoft Graphics Component Information Disclosure (CVE-2019-1078) and more)

- New Bluetooth vulnerability, dubbed KNOB, which affects more than a billion Bluetooth enabled devices allows remote attackers in close proximity to targeted devices to intercept, monitor or manipulate encrypted Bluetooth traffic between two paired devices.

- Adobe Patch Tuesday security updates for August 2019 addressed a total of 119 vulnerabilities affecting multiple products.

  Check Point IPS blade will provide protection against this threat in its next online package (Adobe Acrobat and Reader Out-of-Bounds Write (APSB19-41: CVE-2019-7965); Adobe Acrobat and Reader Use After Free (CVE-2019-8003); Adobe Acrobat and Reader Out-of-Bounds Read (CVE-2019-8005); Adobe Acrobat and Reader Heap Overflow (CVE-2019-8015); Adobe Acrobat and Reader Untrusted Pointer Dereference (CVE-2019-8017))

- Vulnerability in Kaspersky Antivirus exposed a unique user associated identifier to visited websites allowing cross-site tracking of user actions. The vulnerability allows user tracking to bypasses cookies disabling and incognito mode, and provides continuous tracking even when switching between browsers.

THREAT INTELLIGENCE REPORTS

- North Korea has illegally acquired as much as $2 billion in at least 35 cyberattacks targeting 17 countries – so states a UN expert report submitted to the Security Council committee last week. The report cites three main modes of operation: Attacks on SWIFT systems, theft of cryptocurrencies and unpermitted use of resources for cryptocurrency mining. Most attacks targeted South Korea, but India, Bangladesh, Chile and other countries were also attacked.

- Cerberus, a new RAT for Android mobile devices has been detected and is marketed as “Banking Malware for Rent”. The malware grants operators full functionality and control of the infected device but does not implement vulnerability exploitation and requires direct installation on target devices.

  Check Point SandBlast Mobile provides protection against this threat