July 29 - August 4, 2019

Check Point
SOFTWARE TECHNOLOGIES LTD.

YOUR CHECK POINT THREAT INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- Capital One, one of the largest banking institutions in the United States has suffered a massive data breach, exposing personal information of over 106 million credit card applicants between 2005 and 2019. The hacker allegedly exploited a misconfigured firewall on one of Capital One’s cloud servers and stole over 700 folders of data.

- An unprotected ElasticSearch database belonging to the automotive giant Honda has been found online, containing around 134 documents with information on 300,000 Honda employees. Other than personal employee details, the exposed data included internal network information such as machine hostnames, MAC and internal IP addresses, OS version and endpoint security status. The database also contained information on computers used by high-ranking personnel, including Honda’s CEO.

- Details of over one million credit cards from South Korea have been offered for sale on the dark web, many of them belonging to US citizens that purchased services in South Korea. It is estimated that criminals obtained the data by infecting Point-of-Sale systems with malware in restaurants and stores.

- Several computer networks of schools in Louisiana, US, have been infected with ransomware after a wave of cybersecurity breaches had hit 4 school districts in the country. The attacks hit the districts a week before the school year starts, and caused shutdown of different systems and data loss.

- The Los Angeles Police Department (LAPD) has suffered a data breach that exposed personal information of 2,500 LAPD officers along with 17,500 applicants. The exposed data included names, email addresses, passwords and birth dates and it is still unknown how the attacker gained access to it.

- Hackers have found a publicly accessible MongoDB database and replaced nearly 1.2 million records with a ransom note. The database belongs to a bookseller in Mexico and included sensitive customer information such as full names, phone numbers, hashed payment card details and invoices.

VULNERABILITIES AND PATCHES

- 11 critical vulnerabilities have been found in VxWorks, one of the most widely-used real-time operating systems installed in over 2 billion systems and devices, including SCADA, trains, MRI machines and more. Among the discovered vulnerabilities are critical remote code execution, Denial-of-Service and information leak flaws.

  Check Point IPS blade provides protection against this threat (Packet Sanity; TCP Urgent Data Enforcement)

- Critical vulnerabilities have been discovered in OXID eShop e-commerce software that may allow unauthenticated attackers to take full control over websites running older versions of it. The vulnerabilities include an unauthenticated takeover through SQL injection and a remote PHP object injection to the administration panel of the website.

- Researchers have disclosed PoC exploits for 4 remotely exploitable flaws in iOS that could allow attackers to gain access to Apple iOS devices by sending a maliciously-crafted message over iMessage. All 4 vulnerabilities, which include memory corruption issues and use-after-free flaws, were patched in the latest iOS update.

THREAT INTELLIGENCE REPORTS

- Check Point Research has uncovered a recent campaign conducted by the Cobalt Group against a bank in Kazakhstan, using a weaponized decoy document that was planted on the bank's official website. The malicious document dropped various banking Trojans such as Dridex, IcedID and Ursnif.

  Check Point Anti-Bot blade provides protection against this threat (Backdoor.Win32.CobaltGroup)

- A new wave of fraudulent marketing campaigns has been revealed, targeting Italian and Spanish-speaking customers. The campaigns, carried out by a threat group dubbed "Lotsy", involve dozens of well-known brands such as Target, Carrefour, Alitalia and more. The group used fake ads for coupons and free gifts containing links to third-party marketing resources and paid services.

- Experts have discovered LookBack malware, a remote access Trojan (RAT) that has a proxy mechanism used for C&C communication. The malware was observed targeting the United States Utilities sector through phishing emails impersonating a US-based engineering licensing board.

  Check Point Anti-Virus and Anti-Bot blades provide protection against this threat (RAT.Win32.LookBack)

- A new variant of the TrickBot banking Trojan is targeting Windows Defender in attempt to evade detection and removal. The new variant revealed 12 new methods to disable and modify Windows Defender settings.

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