Check Point
SOFTWARE TECHNOLOGIES LTD.

October 29 - November 4, 2018

YOUR CHECK POINT
THREAT INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- Check Point security researchers have published a report describing the elections threat landscape throughout the stages of the elections process - voter registration, election management systems storing voter data, digital campaign arena, and voting machines.
- Toward the upcoming 2018 US midterm elections, 20 different state voter databases were found available for purchase on the dark web. The offered information belongs to about 82 million voters and includes voter IDs, full names, current and previous addresses, phone numbers and citizenship status.
- Chinese government intelligence officers are accused of recruiting hackers and insiders for stealing confidential information from US and French companies involved in aerospace and turbine manufacturing and technology services.
- Austal, a leading Australian defense firm, has fallen victim to a major data breach. Threat actors have gained access to personnel email addresses and mobile phone numbers, and attempted to extort the company by demanding payment in return to the stolen information.
- Private messages related to over 81,000 Facebook accounts have been offered for sale in the dark web. Facebook claims that the information offered by attackers has been harvested through malicious browser extensions.
- The Girl Scouts of Orange County has suffered a data breach exposing data of 2,800 members, including names, birth dates, home addresses, insurance policy numbers and health history. The threat actor gained access to an email account operated by the organization and used it to send messages.
- Iran's infrastructure and strategic networks has allegedly been hit by a new destructive and sophisticated version of Stuxnet. Iran's Passive Defense Organization claims to have neutralized the threat.

VULNERABILITIES AND PATCHES

- High rated zero-day vulnerability has been found actively exploited in the wild, affecting Cisco System's SIP inspection engine. The vulnerability may allow unauthenticated remote attacker to trigger a DoS condition on the vulnerable device.

  Check Point IPS blade provides protection against this threat *(Cisco Multiple Products Denial of Service (CVE-2018-15454))*

- A new iPhone passcode bypass flaw has been found in the latest version of iOS mobile operating system, iOS 12.1. The bypass flaw resides in the new feature Group FaceTime, and may allow an attacker to access all contacts' private information on a locked iPhone.

- Two critical vulnerabilities dubbed 'BleedingBit' have been spotted in Bluetooth Low Energy (BLE) chips, embedded in millions of access points and networking devices used by enterprises around the world. The vulnerabilities could allow remote attackers to execute arbitrary code and take full control of vulnerable devices without authentication.

- Microsoft has released a security patch addressing a bug in Windows 10 operating system. The bug allowed UWP (Universal Windows Platform) apps to access all files on victim's computer without the user's knowledge or permission, by declaring required permissions called "broadFileSystemAccess" in their package configuration file.

THREAT INTELLIGENCE REPORTS

- Security researches claim that the SamSam Ransomware was involved in fresh targeted attacks against 67 different targets, most of them in the U.S. SamSam was also described as "targeted Ransomware" performing extensive reconnaissance before launching the attacks.

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

- New version of Kraken Ransomware has been spotted in the wild, being promoted in a ransomware-as-a-service (RaaS) model on the Dark Web together with a unique affiliation program.

  Check Point SandBlast, Anti-Bot and Anti-Virus blades provide protection against this threat *(Trojan-Ransom.Win32.Kraken)*

- Security report focusing on the Energy and Utilities industries claims that most of the cyberattacks against these sectors occurred inside the enterprise IT networks rather than critical infrastructure itself.

- Some ongoing sextortion scam campaigns leverage the Necurs botnet infrastructure. The attackers used compromised email addresses to send emails to victims, pretending to be in possession of videos showing them while watching porn, and including a payment demand in cryptocurrency.

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