October 2 – October 7, 2018

YOUR CHECK POINT

THREAT INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- Chinese hackers have carried out the most significant supply chain attack recorded against the US, and implanted tiny microchips in servers destined to be placed in the data centers of some of the world's biggest companies, including Apple and Amazon. Some 30 major companies, including banks and government contractors, were affected. Following the publication, Apple and Amazon denied that their servers had been affected by the attack.

- A joint report written by several US agencies warns against an ATM scheme conducted by the infamous North Korean APT Lazarus. The group attacked Switch servers, a key component of ATMs, of banks in over 30 countries to facilitate fraudulent transactions. Researchers revealed that access to some 3,000 breached websites has been offered for sale on a Russian-speaking underground marketplace.

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

- The sales intelligence company Apollo has fallen victim to a major data breach, exposing more than 200 million contact records. The company allows sales people to connect with potential buyers by using its database, which contains information collected by the company and includes names, email addresses, and company contact information.

- Security researchers have discovered that the infamous Russian state-sponsored group, APT28, is now actively conducting cyber espionage campaigns against government and military organizations in Europe and South America.

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

- The recent activities of Turla, a Russian APT group best known for its attacks against NATO-related entities, has been reviewed in-depth by researchers. At least six campaigns were observed during the past two years, including the known IcedCoffee JS backdoor campaign, spread via RTF documents.

  Check Point Anti-Bot and Anti-Virus blades provide protection against this threat (Backdoor.Win32.Turla; Turla)

VULNERABILITIES AND PATCHES

- New vulnerability has been announced by the Git Project. The vulnerability, assigned the ID CVE-2018-17456, could allow a malicious repository to remotely execute commands on a vulnerable machine.
- Following the discovery of a critical flaw in the Windows 10 October 2018 update, Microsoft has paused the release of the update. The flaw causes an unexpected removal of files during the upgrade process, such documents and pictures.
- Mozilla released a patch to resolve seven vulnerabilities in Thunderbird, its email service. One of them was rated critical, a memory corruption flaw that could enable an attacker to run arbitrary code.
- Some 150 vulnerabilities were discovered on the US Marine Corps websites and related services in a designated bug bounty challenge.
- Passcode bypass vulnerability in Apple's new iOS version 12 has been spotted, allowing a potential attacker to gain access to photos and contacts; including phone numbers and emails on a locked iPhone XS and other recent iPhone models.

THREAT INTELLIGENCE REPORTS

- Google Chrome has blocked the feature of inline installs of browser extensions, now only allowing extensions to be downloaded from the official Google Web Store. To bypass this security mechanism, threat actors have developed a new method to trick users into installing the extension – by opening a new window and reducing its size so that only the installation button is revealed, the software's true Google Wed Store description and rating is invisible.
- Following the rise in Business Email Compromise schemes, used to lure financial departments into performing massive transactions to accounts owned by malicious actors, actors in dark web forums are offering corporate email hacking services for as little as 150 USD.
- Researchers have investigated Roaming Mantis, a group that began its way targeting vulnerable routers to spread malicious Android malware. Recently, the groups shifted its iOS campaign from credential theft to crypto mining.

  Check Point SandBlast Mobile customers are protected from this threat
- Data breaches in the Healthcare sector increased by 70 percent between 2010 and 2017, according to a research of the Center for Quantitative Health. Since 2010, there have been over 2100 breaches which affected some 176 million medical records.