September 10 – September 16, 2018

Check Point
SOFTWARE TECHNOLOGIES LTD.

YOUR CHECK POINT THREAT INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- Recent attacks have been targeting the Japanese Media Sector. Conducted by the Chinese APT group "Stone Panda", or APT 10, the attack used target-specific email messages with titles related to maritime, diplomatic, and North Korean issues. The body of the messages included a password for the "password-protected" document, luring victims to open the document and run the group's "UPPERCUT" backdoor.

- A new campaign by the Iranian APT OilRig has been targeting an undisclosed Middle-Eastern governmental organization. The campaign included target-specific emails with attached Microsoft Word document that contained a macro responsible for installing a new variant of the APT's malware "BONDUPDATER".

- Security researchers have concluded that the data breach at British Airways was probably the work of "MageCart", the hacking team behind the TicketMaster breach earlier this year, as it fits the group's modus operandi. Researchers reported that the attacker weaponized a genuine file on the company's website, adding to it a piece of code that extracts any data entered in the checkout page payment form, and sends it to a remote server located in Romania.

- In yet another operation by "MageCart", the group weaponized the code distributed to the customers of the web analytics firm "Feedify", who declares servicing over 4,000 customers. The attackers injected their malicious code into a library the Feedify script served to customers' websites, thus compromising hundreds of e-commerce sites.

- The Bristol Airport has reportedly been hit by a ransomware, causing problems to the flight display screens for two days, forcing the staff to resort to "manual processes", namely - whiteboards and marker pens.

- The gambling app EOSBet has been hacked, and the attackers took off with $200,000 worth of game tokens. According to the company, the attackers exploited a bug in one of their games, using a fake hash to hijack the EOSBet's transfer funds.

VULNERABILITIES AND PATCHES

- Security researchers have uncovered a zero-day vulnerability in Tor browsers. The flaw resides in the NoScript browser plugin pre-installed in the Mozilla Firefox bundled in the Tor software, and effectively allows a website to execute malicious JavaScript on victims' browsers to identify their real IP address.
- Microsoft has issued 17 critical patches in a bundle of 61 new patches overall, addressing issues in Microsoft Windows, Edge, Internet Explorer, MS Office, ChakraCore, .NET Framework and others.

  Check Point IPS blade provides protection against these threats (Microsoft Windows Remote Code Execution (CVE-2018-8475); Microsoft Windows ALPC Elevation of Privilege (CVE-2018-8440); Adobe Flash Player Memory Corruption (APSB14-26: CVE-2014-8439))
- Adobe has released 10 new patches for Flash Player and ColdFusion, six of which are rated as critical.
- Security researchers have revealed that Safari browsers remain vulnerable to a serious vulnerability that could allow attackers to spoof website addresses. Microsoft, of which Edge browser had also been found vulnerable, has patched the issue.

THREAT INTELLIGENCE REPORTS

- Check Point researchers have revealed a new Malware as a Service (MaaS) product, “Black Rose Lucy”, currently targeting Android-based phones in Russia. The product, apparently developed by a Russian-speaking team, includes a remote control dashboard for monitoring the botnet of victim devices, and a payload that collects the victim’s data and can install extra malware on infected devices.

  Check Point SandBlast Mobile customers are protected from this threat
- A new variant of the Kraken Cryptor ransomware has been discovered. This version is masquerading as the legitimate SuperAntiSpyware anti-malware program in order to trick users into installing it. Attackers gained access to that software’s official website, and distribute the ransomware from there.

  Check Point Anti-Bot and Anti-Virus blades provide protection against this threat (Trojan-Ransom.MSIL.Kraken.A)
- A new ransomware has been discovered, pretending to be Locky and written in Python, aptly named “Pylocky”. The malware is distributed via spam emails targeting European countries, mostly France.
- Security researchers have found a way for an attacker to manually tamper with the firmware of a stolen laptop in order to acquire the encryption keys of the encrypted hard drives and other personal information that hadn’t been known to be vulnerable to hard reboot attacks. The Researchers stated all modern laptops are vulnerable to this attack method.
- Security researchers have highlighted the re-emergence of targeted ransomware, where an attacker infects an already compromised victim, rather than relying on large scale spam campaigns.