October 16 - 22, 2017

Check Point
SOFTWARE TECHNOLOGIES LTD.

YOUR CHECK POINT

THREAT INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- Check Point researchers have identified a new IoT botnet, "IOTroop", assessed to have been hitting 60% of corporate networks. The botnet, of which ultimate purpose is yet unknown, impacts a large array of IoT devices, mostly routers and cameras, including GoAhead, D-Link, TP-Link, AVTECH, NETGEAR, MikroTik, Linksys and others. The researchers assess the potential damage by this bot could dwarf that caused last by the Mirai, which had brought down internet traffic of several major corporations.

  Check Point IPS and Anti-Bot blades provide protection against this threat *(Wireless IP Camera (P2P) WIFICAM Cameras Information Disclosure; Wireless IP Camera (P2P) WIFICAM Cameras Remote Code Execution; D-Link 850L Router Remote Code Execution; D-Link DIR800 Series Router Remote Code Execution; D-Link 850L Router Remote Unauthenticated Information Disclosure; D-Link 850L Router Cookie Overflow Remote Code Execution; Dlink IP Camera Video Stream Authentication Bypass – Ver2; Dlink IP Camera Luminance Information Disclosure – Ver2` D-Link DIR-600/300 Router Unauthenticated Remote Command Execution; Netgear DGN Unauthenticated Command Execution; Netgear ReadyNAS Remote Command Execution; AVTECH Devices Multiple Vulnerabilities; Belkin Linksys E1500/E2500 Remote Command Execution; Linux System Files Information Disclosure; Technicolor TD5336 Router Remote Code Execution; Botnet.Linux.IOTroops.*)*

- Researchers have revealed that the Elmedia Media Player has been infected with Proton Malware, with two infected versions of the software uploaded to the manufacturer's official website affecting hundreds of machines. The malware is Mac-specific and could lead to the leak of sensitive information.

  Check Point Anti-Bot blade provides protection against this threat *(Trojan.OSX.Proton.A)*

- Security researchers have reported that two large-scale campaigns are attempting to exploit a new zero-day vulnerability in Abobe Flash exposed last week, that had since and been patched. One spam-based campaign by hacking group BlackOasis attempted to use the vulnerability to install Finspy malware. The other attempt was made by the allegedly state-backed Russian hacking group APT28 set out on several malware campaigns via focused phishing attempts, to install the DealersChoice malware.

  Check Point IPS blade provides protection against this threat *(Adobe Flash Player Type Confusion (APSB17-32: CVE-2017-11292))*

VULNERABILITIES AND PATCHES

- Security researchers have revealed that the zero-day vulnerability in Microsoft Office DDE which could enable attackers to run code in documents without using macros, can also be utilized in Outlook, using emails and calendar invites formatted using Microsoft Outlook Rich Text Format (RTF).

  Check Point IPS blade provides protection against this threat *(Microsoft Office DDE Remote Code Execution; Microsoft Office Memory Corruption (CVE-2017-11826)*

- Researchers have identified "Kracked" - a vulnerability in the Wi-Fi Protected Access II (WPA2) protocol that secures all modern protected Wi-Fi networks. The weakness could enable an attacker to enforce a reinstallation of the encryption key. However, this attack requires the attacker to be connected to the victim's Wi-Fi range, and cannot be carried remotely.

THREAT INTELLIGENCE REPORTS

- Researchers have announced that the Necurs botnet is now using the recently discovered Microsoft Office DDE vulnerability to spread the Locky ransomware. As before, the attack is propagated by a spam email containing malicious file.

  Check Point SandBlast, IPS and Anti-Bot blades provide protection against this threat *(Suspicious Metadata Mail Phishing Containing Attachment; Microsoft Office DDE Remote Code Execution; Microsoft Office Memory Corruption (CVE-2017-11826), Trojan-ransom.Win32.Locky*, Trojan.Win32.Necurs.B)*

- Researchers have identified a new ransomware dubbed "Magniber" which is being distributed through malvertisements displayed by Magnitude exploit kit, the last known distributor of Cerber, and specifically targeting users from South Korea.

  Check Point IPS and Anti-Bot blades provide protection against this threat *(Magnitude Exploit Kit Landing Page; Magnitude Exploit Kit Redirection; Operator.Magniber*)*

- Researchers have warned of a new malware campaign leveraging the Ursnif banking Trojan. The malware spreads by spam email containing a fake invoice.

  Check Point Anti-Bot blade provides protection against this threat *(Trojan.Win32.Ursnif.*, Trojan-Spy.Win32.Ursnif.*)*

- Security analysts have warned against the cyber-capabilities of North Korea, which they defined as expansive and carried out by well-trained experts. Most recently, a group dubbed "Lazarus" operating from North Korea hacked the Far Eastern International Bank, leading the U.S Department of Homeland Security and FBI to issue a warning regarding the malware used in the attack.

  Check Point IPS and Anti-Bot blades provides protection against this threat *(Hangul Word Processor Type Confusion (CVE-2015-6585); Adobe Flash Player Integer Overflow Remote Code Execution (APSB16-01: CVE-2015-8651); Microsoft Silverlight Runtime Remote Code Execution (MS16-006: CVE-2016-0034); Adobe Flash Player Remote Code Execution (APSA16-01: CVE-2016-1019); Adobe Flash Out of Bounds Access Code Corruption; Botnet.Win32.HiddenCobra.A; Trojan-DDoS.Win32.HiddenCobra.A)*