November 6 - 12, 2017

Check Point
SOFTWARE TECHNOLOGIES LTD.

YOUR CHECK POINT

THREAT INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- Researchers revealed a new malware dubbed Ordinypt, which currently targets business users in Germany. The malware pretends to be a ransomware, presenting to the user what appear to be encrypted files, but it is in fact a wiper; the original files were deleted and replaced by randomly generated content. The malware spreads via bogus emails in flawless German with a malicious attachment that pretends to be a CV.

  Check Point IPS blade provides protection against this threat *(Suspicious Executable Mail Attachment)*

- Wikileaks have published the first of what they claim to be a new string of publications dedicated to the CIA cyberwarfare tools. The publication is dedicated to "Hive", the means by which CIA malware communicates with its C&C.

- Security researchers have warned against a potential new malware campaign targeting users in Japan. The potential malware involves a .jtd file, used by the popular JustSystems Ichitaro word processor, spread by spam mail. As of now, the embedded macros are harmless and were patched by the company in the most recent version of the program, but may be used in the future with a malicious payload.

  Check Point IPS blade will provide protection against this threat in its next online package

- Security researchers have warned that hackers targeting banks in Brazil are vastly using AutoIt, a Windows scripting tool, to load a banking Trojan. This mechanism allows the Trojan to evade simple Anti-Virus mechanisms.

- OilRig, suspected to be an Iranian threat group, has been using a new crafted Trojan called "ALMA Communicator", presumably to target "an individual at a public utilities company in the Middle East".

  Check Point IPS blade provides protection against this threat *(Microsoft Office Files Containing Malicious VBScript Downloader; Microsoft Office Files Containing Malicious Downloader)*

VULNERABILITIES AND PATCHES

- A vulnerability in Brother printers that can allow a remote attacker to cause denial of service to the printer has been disclosed, but not yet patched by the vendor.

  Check Point IPS blade provides protection against this threat *(Brother Debut Embedded Httpd Unauthenticated Denial Of Service (CVE 2017 16249))*

- Google has patched the KRACK vulnerability in WPA2 for its Andorid OS. Apple has also patched the issue in its latest security bulletin. This vulnerability could allow attackers to reveal encrypted data sent over Wi-Fi network, when in physical proximity to their target machine.

- Security researchers have revealed an encryption weakness in the standard used to secure intellectual property, P1735 IEEE which could reveal the underlying encrypted information to an attacker.

THREAT INTELLIGENCE REPORTS

- Researchers have found 685 Android and iOS apps that are vulnerable to a new potential leakage of information. The vulnerability is due to hardcoded credentials left in the apps by the developers, which could be used by attackers to access conversations and SMS messages made by these apps.

- Researchers have identified a new Android malware called TOASTAMIGO which exploits a newly discovered vulnerability in Toast pop-ups – Android's mechanism to display notifications over another running application. This vulnerability has been fixed in the latest Android OS version.

- Security Researchers have reported on a new malware dubbed "Gibon". The ransomware, possibly originating from Russia, spreads itself via spam mail. However, a decryptor is already available.

  Check Point IPS and Anti-Bot blades provide protection against this threat *(Suspicious Executable Containing Ransomware; Trojan-Ransom.Win32.Gibon.*)*

- Researchers have revealed that stolen digital certificates are available for sale over the dark net for $1,200. The research team also showed 58.2% of signed malware carry valid digital signatures, which could enable malware to bypass security measures, as most famously done by the Stuxnet malware.

- Security researchers have analyzed 2017's "Summer of Ransomware", throughout which the most popular ransomware used were Cerber and WannaCry, followed by a great gap by Locky, Petya and Jaff.

  Check Point SandBlast, IPS, Anti-Bot and Anti-Virus blades provide protection against this threat *(Suspicious Microsoft Office File Archive Mail Attachment; Microsoft Windows SMBTouch Scanner; Microsoft Windows ArchiTouch SMB Scanner; Microsoft Windows SMB Remote Code Execution (MS17-010: CVE-2017-014*); Microsoft Windows Eternal*; Microsoft Windows DoublePulsar SMB Remote Code Execution; Petya Ransomware Lateral Movement Remote Code Execution; Suspicious SMB Ransomware Propagation Attempt; Trojan-Ransom.Win32.Jaff.*; Trojan-ransom.Win32.Locky.*; Trojan-Ransom.Win32.Petya.*; Trojan-Ransom.Win32.Cerber.*; Trojan-Ransom.Win32.WannaCry.*)*