March 14 - 20, 2016

Check Point SOFTWARE TECHNOLOGIES LTD.

YOUR CHECK POINT

THREAT INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- NSHC hackers group hacked an archive of the conservative Swiss People's Party (SVP), Switzerland's largest party, and stole the personal data of over 50,000 of their supporters.
- Approximately six million non-jailbroken iOS mobile devices were infected by a new malware dubbed 'AceDeceiver', which leverages design flaws in Apple's DRM software.
- A massive Malvertising campaign has recently been observed, distributed via high profile publishers such as bbc.com and msn.com, leveraging Angler exploit kit.

  Check Point IPS blade provides protection against all known variants of this threat *(Angler Exploit Kit Redirection; Angler Exploit Kit Landing Page; Angler Exploit Kit Landing Page Patterns; Angler Exploit Kit Landing Page URL)*

- Visitors to Korean news websites have been redirected to the GongDa exploit kit, a relatively old kit which uses exploits to vulnerabilities from 2010-2014 and delivers various payloads.

  Check Point IPS blade provides protection against all known exploits of these vulnerabilities *(Oracle Java Applet Rhino script engine policy Bypass; Adobe Flash Player External MP4 Buffer Overflow (APSB11-21); Oracle Java MBeanInstantiator.findClass Remote Code Execution; Microsoft Windows OLE Automation Array Remote Code Execution (MS14-064))*

- A new phishing-based Torrentlocker campaign is targeting Swedish and Italian users, by imitating PostNord, a Nordic logistics company, and Enel, an Italian gas and electricity manufacturer.

  Check Point Anti-Virus and Anti-Bot blades provide protection against all known variants of this threat *(Trojan.Win32.TorrentLocker; Operator.Torrentlocker; Torrentlocker)*

- A new phishing-based Torrentlocker campaign is targeting Swedish and Italian users, by imitating PostNord, a Nordic logistics company, and Enel, an Italian gas and electricity manufacturer.
- Researchers issued a warning against a new spam campaign which lures victims into downloading JS.downloader by claiming to have information about the Zika virus. Once a victim is infected with the Downloader, it will try to fetch an additional payload.

VULNERABILITIES AND PATCHES

- A new Android exploit based on Stagefright multimedia playback library has been disclosed; the exploit, dubbed Metaphor, allows an attacker to hack Android smartphones in just a few seconds by tricking users into visiting a hacker's webpage which contains a malicious multimedia file.
- Researchers from John Hopkins University exposed a security flaw in Apple's iMessage application, which might enable an attacker to intercept images, videos and other files sent via the service. However, the flaw does not enable decryption and interception of the text messages.

THREAT INTELLIGENCE REPORTS

- Researchers revealed that Chinese hackers are using tools and techniques previously associated with Chinese government-supported espionage campaigns in order to install ransomware, and has already managed to infect machines in a transportation company and a technology firm, both located in the U.S.
- A new variant of TeslaCrypt ransomware has been observed in the wild. TeslaCrypt 4.0 features include improved data leakage techniques, a new encryption algorithm (RSA 4096) and some additional new functionalities. At least currently, the designated recovery tool 'TeslaDecoder' does not work with Teslacrypt this version.

  Check Point Anti-Virus and Anti-Bot blades provide protection against this threat *(Trojan-Ransom.Win32.TeslaCrypt; Operator.Teslacrypt; Teslacrypt)*

- A new Trojan dubbed Thanatos is being offered as a service these days. Dropped by the Nuclear exploit kit, The Trojan features an AV module which scans and removes additional malicious files found on the victim's computer. In addition to the Trojan, the operators offer a custom written ransomware and bulletproof hosting.

  Check Point IPS and Anti-Virus blades provide protection against this threat *(Nuclear Exploit Kit Lading Page; Nuclear Exploit Kit Redirection; Trojan.Win32.Alphabot)*

For comments, please contact: TI-bulletin@checkpoint.com