October 23 - 29, 2017

YOUR CHECK POINT

THREAT INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- A new ransomware dubbed BadRabbit has hit worldwide in an outbreak focused on Russia and Ukraine. The ransomware was being spread via a fake Flash software installer, which seems to have arrived as a pop-up from several compromised sites, mostly legitimate Russian news sites. Once run, the pop-up leads to a malicious site, which in turn downloads an executable file. Once infecting a target machine, the malware encrypts it and asks for a ransom payment of 0.05 BTC (~$280).

  Check Point SandBlast, IPS and Anti-Virus blades provide protection against this threat *(Suspicious SMB Ransomware Propagation Attempt; Suspicious JavaScript Web Evasions; Suspicious Executable Containing Ransomware; Suspected Ransomware Dropzone; Trojan-Ransom.Win32.Badrabbit)*

- Check Point's researchers have released the full investigation of the IoTroops botnet, which includes an in depth technical analysis of the malware and the botnet. According to the investigation, the botnet includes two different infrastructures. The main set of servers and samples is focused on infection and propagation, while a smaller and different set is used for second stage payloads. In addition, the attackers behind the network have quick and flexible control of infected device via LUA scripting.

- *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.*)*

- Basetools.ws, an underground forum and marketplace used by threat actors, seems to have been breached and face a ransom demand, after an unknown threat actor had published samples of the site's databases with a ransom note demanding $50K or else he will share information regarding the site's

administrator with the US security services. Basetools.ws has over 150K users and offers illegal goods such as stolen credit card data and cyber-tools.

- Kaspersky cyber-security vendor has rejected the accusations of a role in the NSA cyber-tools' leak. According to the accusations, Kaspersky had gained access to the NSA tools and delivered them to the Russian regime. According to The Company's announcement, back in 2014, it had scanned a home-computer belonging to an Equation Group worker, where its software detected malware developed by Equation Group that the worker may have took home without permission. The company added that the malware was deleted from its servers, and therefore couldn't have been exposed.
- The Department of Homeland Security (DHS) and the Federal Bureau of Investigation (FBI) have issued an alert, warning companies from the energy, aviation and water industries from advanced persistent threat (APT) groups' threat activity.

  Check Point IPS blade will provide protection against this threat in its next online package
- jQuery's official blog was compromised by an unknown threat actor. The attack appears to be a simple defacement attack, and seems to not have harmed jQuery's libraries.

VULNERABILITIES AND PATCHES

- Check Point researchers have discovered a vulnerability, dubbed HomeHack, in LG's smart home infrastructure, exposing it to critical user account takeover. If attackers would have exploited this vulnerability, they would have been able to log into LG users' SmartThinQ® home appliance accounts and take remote control of the devices connected to the account.
- Two critical vulnerabilities were found in AmosConnect 8, a communication platform using the maritime sector. The vulnerabilities may allow pre-authenticated attackers to fully compromise an AmosConnect server, thus expose sensitive data linked to the server.

  Check Point IPS blade provides protection against this threat (SQL Servers Blind SQL Injection)
- Google has released security updates for Chrome browser, addressing 10 vulnerabilities, 9 of which are KRACK (Key Reinstallation Attack) vulnerabilities, and the tenth is a high severity stack overflow vulnerability.

THREAT INTELLIGENCE REPORTS

- A recent Terror exploit kit campaign distributing the Smoke Load downloader was spotted by researchers. The campaign is being delivered via a Propeller Ads' advertising domain. In this new campaign, Terror exploit kit has demonstrated improved obfuscation capabilities and new exploits.

Check Point Anti-Virus and Anti-Bot blades provide protection against this threat *(Terror Exploit Kit; Terror Exploit Kit URL Pattern; Microsoft Internet Explorer Memory Corruption (MS16-051: CVE-2016-0189); Microsoft Windows OLE Automation Array Remote Code Execution (MS14-064); Trojan.Win32.Smokeloader; Operator.Terror ek)*

- A new two-part research by Check Point researchers describes the world of web-based crypto-currency miners. The research describes the new trend of deploying web-based crypto-miners within websites. The miners abuse visitors' CPU to generate profits without users' approval or knowing. The research describes the activity of CoinHive Monero miner, and suggests various implementation methods. On a related issue, CoinHive's CloudFlare server was hijacked by a threat actor that was able abused its DNS servers for six hours and steal the mined Monero crypto-coins from CoinHive's users.

  Check Point IPS blade provides protection against this threat *(Multiple Websites Mine Cryptocurrencies CPU Hijacking)*

- Researchers have discovered that Lokibot android mobile banking Trojan has adopted ransomware capabilities, and thus become a hybrid mobile malware. The malware functions as a mobile banking Trojan, and whenever a victim tries to uninstall it, it performs a ransom attack remanding $70-100 in order to retrieve the infected device. Lokibot is being sold on underground forums for $2K.

  Check Point Sandblast Mobile customers are protected from this threat

- According to a research conducted in the UK, youngsters under 25 are now twice more likely to fall victims to phishing scams than baby boomers (over 55). In addition, their average damage is estimated at £613.22 compared with £214.70 for the older generation.

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