November 20 - 26, 2017

Check Point SOFTWARE TECHNOLOGIES LTD.

YOUR CHECK POINT

THREAT INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- Uber has revealed that in 2016 it suffered a data breach which compromised 57 million accounts, leaking email addresses, mobile phones and names associated with the accounts. Further Reports claim the breached data was stored on Amazon Web Services accounts, that the attackers used Uber software engineer credentials found on GitHub to gain access, and that the company paid the attackers to guarantee the data is destroyed and the hack silenced.

- Security researchers have identified a spike in the activity of Mirai botnet. The new campaign, based on spam emails, utilizes recently resurfaced credentials-vulnerability in old ZyXEL PK5001Z routers to infect them with Mirai. Researches reported around 100,000 infected IP addresses, most of them in Argentina.

  Check Point IPS and Anti-bot blades provide protection against this threat *(ZyXEL PK5001Z Modem Authentication Bypass (CVE-2016-10401); Botnet.Win32.Mirai.*)*

- Security researchers have announced a new Necrus-based spam campaign spreading the Scarab Ransomware. The spam email pretends to be from HP, Lexmark, Canon or Epson, and includes a malicious .vbs attachment compressed in 7zip.

  Check Point SandBlast, IPS and Anti-Virus blades provide protection against this threat *(Suspicious Executable Mail Attachment; Trojan-ransom.Win32.Scarab.*)*

- Researchers have reported a new Android-based campaign targeting Samsung users in South Korea, initiated by the North-Korean hacking group Lazarus APT. The malicious code is embedded in APK file designed to mimic a Korean bible app. The app wasn't available in the Google Play store, so its means of propagation are still unclear.

  Check Point Sandblast Mobile customers are protected from this threat

- Newly discovered vulnerabilities in two WordPress plugins are now being exploited in the wild.

  Check Point IPS blade provides protection against this threat *(WordPress Formidable Forms Plugin Remote Code Execution)*

VULNERABILITIES AND PATCHES

- Researchers at Check Point have exposed a new vulnerability in AliExperss shopping website, which could theoretically be used via phishing campaigns to infect site users. The vulnerability allows criminals to target AliExpress users by sending them a link to an AliExpress web page containing malicious Javascript code. The vulnerability has been fixed by the website.

  Check Point IPS blade provides protection against this threat *(Cross-Site Scripting Scanning Attempt)*

- Intel has published its new security bulletin, patching newly discovered vulnerabilities in its Management Engine, Trusted Execution Engine and Server Platform Services that could allow local attackers elevate privileges, run arbitrary code, crash systems and eavesdrop on communications.

- HP has announced it patched a newly discovered remote code execution vulnerability in its printers' firmware, revealed by security researchers. The vulnerability could, for example, enable a remote attacker to gain access to the content of any print job, even protected ones.

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

- Security researchers have devised a new way to forge the SAML secured communication protocol. The "Golden SAML" could enable attackers to gain any level of privileges to cloud-based services that uses SAML (e.g. Azure, AWS, vSphre) and pretend to be any user they desire. However, this technique can only be used after already getting access to the target's domain.

THREAT INTELLIGENCE REPORTS

- Security researchers have discovered a new ransomware dubbed "QyG". The ransomware, identified while still in development, is embedded in the macros of a Word document. Once opened and enabled, the malware encrypts only the user's Word documents.

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

- A new version of OWSAP top 10 security threats has been published. The report includes several new categories, but injection attacks and cross-site scripting still top the list.

  Check Point IPS blade provides protection against these threats *(e.g: Microsoft Windows System Information Console XXE Injection Information Disclosure; Microsoft Windows Performance Monitor XXE Injection Information Disclosure (CVE-2017-0170); Microsoft Windows XXE Information Disclosure (CVE-2017-8710); Adobe ColdFusion OOXML XXE Information Disclosure; Adobe Digital Editions Epub XXE Information Disclosure; Red Hat JBoss RESTEasy PARAMETER ENTITY XXE Information Disclosure; Red Hat JBoss Seam Framework XXE information disclosure; Apache Struts REST Plugin XStream Deserialization Remote Code Execution (CVE-2017-9805); HPE Intelligent Management Center RMI Registry Insecure Deserialization; HPE Operations Orchestration Insecure Deserialization)*