Check Point
SOFTWARE TECHNOLOGIES LTD.

May 27 – June 2, 2019

YOUR CHECK POINT
THREAT INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- Around 855 million of insurance-related documents have been leaked online after the US real-estate insurance company First American Financial Corp. accidentally left the documents unsecured on their website. The leaked data, dated back to 2003, included bank account numbers, mortgage and tax records, social security numbers and more.

- Nansh0u, a new cryptojacking campaign targeting Windows MS-SQL and phpMyAdmin servers worldwide, has already infected nearly 50K servers and is being carried out by an APT-grade Chinese group. The group uses brute-forcing techniques to login to the servers, and then uses exploits to escalate privileges and install malicious payloads. Payloads are a cryptominer and a kernel-mode rootkit to prevent the malware from being terminated.

  Check Point Anti-Virus blade provides protection against this threat (Cryptominer.Win32.Nansh0u)

- Flipboard, the social sharing and news aggregator service, has suffered a data breach after hackers gained access to one of its user databases for nearly 10 months. The database contained details such as full names, usernames and hashes password, email addresses and some digital tokens.

- A new hacking campaign is injecting a malicious code into hypertext access (.htaccess) files on websites running Joomla and WordPress. The malicious code was observed redirecting visitors to an advertisement website.

- The Pyramid Hotel Group, the brand manager of Marriott, Hilton and Sheraton Plaza hotel chains, suffered a data leak after 85GB of security audit logs and some personal employee information were found on an unprotected server online.

- Checkers and Rally's drive-through restaurant chain has revealed a data breach impacting their point-of-sale system that affected an unknown number the restaurants' customers in 20 US states. The malware implanted collected payment information from the credit cards used in these PoS devices.

VULNERABILITIES AND PATCHES

- A remote code execution vulnerability has been discovered in Microsoft's Notepad text editor. Successful exploitation of the flaw, a memory corruption bug, may allow launching a Command Prompt from the Notepad.
- The WordPress plugin Convert Plus is affected by a critical flaw that may allow an unauthenticated user to create new accounts with administrator privileges. The flaw resides in an improper validation of the user role field in the subscription form filled by new subscribers.

  Check Point IPS blade will provide protection against this threat in its next online package
- Several Siemens Healthineers software products, providing digitalized healthcare solutions, have been found vulnerable to the recently-patched Windows RDP vulnerability dubbed BlueKeep (CVE-2019-0708).

  Check Point IPS and SandBlast Agent provide protection against this threat (Microsoft Remote Desktop Services Remote Code Execution (CVE-2019-0708))

THREAT INTELLIGENCE REPORTS

- The recent activity of the cyber-espionage Chinese APT group Emissary Panda has been uncovered, exposing their recent campaign targeting government organizations in the Middle East in which the group compromised SharePoint servers for information collection and lateral movement purposes.

  Check Point IPS and Anti-Virus blades provide protection against this threat (Microsoft SharePoint Remote Code Execution (CVE-2019-0604), Trojan.Win32.Emissary Panda)
- A new sophisticated Linux malware has been discovered, dubbed HiddenWasp. HiddenWasp was observed in targeted attacks of victims that were already under the attacker's control, and is using code parts and algorithms borrowed from open source malware such as Mirai and Azazel.

  Check Point Anti-Virus blade provides protection against this threat (Trojan.Linux.HiddenWasp)
- GandCrab, the infamous ransomware-as-a-service, will shut down its operations and terminate its activity. The operators have published posts in several popular hacking forums announcing their decision to shut down the operation, stating that the operation earned more than $2 billion in ransom payment as well as revealing their personal revenue of nearly $150 million.

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