Check Point
SOFTWARE TECHNOLOGIES LTD.

Nov 15 – 21, 2021

YOUR CHECK POINT

THREAT INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- Emotet, the most popular and notorious botnet before its takedown ten months ago, is back. Emotet is currently distributed via TrickBot and already launched a worldwide email spam campaign delivering malicious documents. Researchers believe that Conti ransomware gang is behind the botnet's return.

  Check Point Threat Emulation and Anti-Bot provide protection against these threats (HEUR:Trojan Banker.Win32.Emotet; Trojan-Banker.Win32.Trickbot)

- US, UK and Australia warn of state-sponsored Iranian hackers actively exploiting Fortinet and Microsoft Exchange ProxyShell vulnerabilities to gain initial access to compromised systems for data exfiltration or ransomware attacks. Targeted sectors include transportation and healthcare.

  Check Point IPS provides protection against these threats (VERS_Fortinet FortiOS Directory Traversal (CVE-2018-13379); Microsoft Exchange Server Remote Code Execution (CVE-2021-34473))

- US medical center Utah Imaging Associates has been breached, and data of 582,170 people including names, social security numbers and medical information was exposed.

- 300 WordPress websites have been defaced, displaying fake ransomware notices, trying to trick the website owners into paying 0.1 bitcoin for the recovery. No files were encrypted in the attack, and the page with the ransom note turns out to be an HTML page generated by a bogus WordPress plugin.

- Alleged Chinese threat actors are deploying a new Linux backdoor called linux_avp on e-commerce servers ahead of Black Friday and Holidays shopping season. The malware, written in Golang, is able to intercepts and exfiltrate customer data, including credit card details.

- State-sponsored North Korean cyber espionage group TA406 is targeting diplomats and government officials in the US, Russia, China and South Korea in a credential harvesting campaign using custom made malware and phishing attacks.

- Hackers are targeting Alibaba Cloud Elastic Computing Service instances to mine Monero cryptocurrency.

VULNERABILITIES AND PATCHES

- Microsoft has released out-of-band updates to fix authentication failures associated with Kerberos delegation scenarios impacting Domain Controllers (DC) that are running supported versions of Windows Server.
- Intel has issued a security advisory to confirm the existence of two high-severity vulnerabilities, CVE-2021-0157 and CVE-2021-0158 that could allow privilege escalation attacks in multiple Intel products and processor families.
- npm has fixed several security flaws. One concerned a leak of private npm package names on the npmjs.com's "replica" server, and the other could allow attackers to publish new versions of any existing npm package using an account without proper authorization.
- The FBI has issued a warning concerning an APT group leveraging a zero-day in FatPipe MPVPN router to elevated admin privileges by exploiting a file upload function in the devices firmware to install a WebShell with root access. The flaw was consequently patched.

  Check Point IPS provides protection against this threat *(FatPipe Remote Code Execution)*

THREAT INTELLIGENCE REPORTS

- Popular trading platform Robinhood has suffered a data breach which resulted in millions of customers' information being sold on hacking forums. The company is now being hit by a class-action lawsuit in response to the breach.
- Russian ransomware operators are starting to collaborate with their Chinese counterparts, reaching out to each other on hacking forums.
- Corporate espionage organization RedCurl is resurfacing with upgraded tools, after disappearing last year. The group is mostly interested in obtaining internal documents or staff records using spear-phishing emails.
- Android Banking malware BrazKing makes a comeback with an upgrade including dynamic banking overlays and a new implementation trick that enables it to operate without requesting risky permissions. The malware is likely operated by a Brazilian threat group and is targeting local mobile banking users.
- The Memento ransomware has used password protected WinRar archives as a way to encrypt victims' files, after unsuccessful data encryption that kept being detected by endpoint protections.