Check Point
SOFTWARE TECHNOLOGIES LTD.

April 27 - May 3, 2020

YOUR CHECK POINT
THREAT INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- Check Point Research has discovered a targeted attack on a multinational conglomerate, where the company's Mobile Device Manager (MDM) server has been compromised and used to install Cerberus banking Trojan on employees' mobile devices centrally. This new variant of Cerberus has enhanced RAT capabilities and allows to exfiltrate extensive data including credentials, SMS messages (along with 2FA SMS codes) and more.

  Check Point SandBlast Mobile provides protection against this threat

- Black Rose Lucy, a MaaS botnet and dropper for Android devices first revealed by Check Point in 2018, has acquired ransomware capabilities. In attacks detected by Check Point Research, Lucy utilizes Android's accessibility service to gain administrator privileges, encrypts files and demands ransom and credit-card details from its victims.

  Check Point SandBlast Mobile provides protection against this threat

- Estonian Internal Security Service (KaPo) has reported that state-sponsored hackers exploited a zero-day vulnerability to hack into the Estonian email provider Mail.ee and hijacked a small number of accounts of high-profile users. The KaPo attributed the attack to Russian and Iranian linked APT groups.

- A misconfigured Elasticsearch server of the French newspaper Le Figaro has exposed over 8TB of data containing 7.4 billion records with PII of reporters, employees and at least 42,000 users.

- Maze ransomware operators claim to have stolen 11 million credit card credentials from the state-owned Bank of Costa Rica Banco BCR. The Maze group, infamous for its recent double-extortion routine, explained it did not encrypt the bank's documents due to the world pandemic.

  Check Point SandBlast and Anti-Bot provide protection against this threat *(Ransomware.Win32.Maze)*

- Over 150 companies around the world have been victims of a successful phishing attack leveraging Microsoft file-sharing services including Sway, SharePoint, and OneNote to target high ranking executives.

VULNERABILITIES AND PATCHES

- Check Point Research has reported multiple vulnerabilities in WordPress eLearning platforms, currently in use by thousands of educational institutions and websites. Researchers found vulnerabilities ranging from Privilege Escalation up to full Remote Code Execution, which can allow attackers to gain sensitive information, edit personal records or even take control of the platforms.

  Check Point IPS blade provides protection against these threats (WordPress LearnDash Plugin SQL Injection (CVE-2020-6009); WordPress LearnPress Plugin Privilege Escalation; WordPress LearnPress Plugin SQL Injection; WordPress LifterLMS Plugin Arbitrary File Write (CVE-2020-6008))

- Researchers have discovered a worm-like vulnerability in Microsoft Teams platform that could allow attackers to take over an entire list of an organization's accounts by sending links to image files. The vulnerability, affecting both desktop and web versions of the platform, has been patched by Microsoft.

- Adobe has released emergency updates for three of its widely used products that patch dozens of newly discovered critical vulnerabilities. Affected software includes Adobe Illustrator, Adobe Bridge, and Magento e-commerce platform.

- Sophos has published an emergency security update to fix an SQL injection vulnerability in its firewall product that is being actively exploited in the wild. Following successful exploitation, attackers employed a malware called Asnarok to steal usernames and other data used for remote access to the device.

THREAT INTELLIGENCE REPORTS

- The operators of the Shade ransomware, active since 2014, have announced the termination of their activity and published more than 750K decryption keys to be used by past victims. While the reasons for the termination are unclear, the decryption keys are authentic and functioning and a decryption tool has been published.

- Researchers report of a sharp increase in the number of RDP brute-force attacks since mid-March due to remote working during the COVID-19 pandemic. This aligns with a Shodan report from earlier this month showing a 40% increase in exposed RDP endpoints.

- Researchers have discovered a new Android info stealer dubbed EventBot that targets banks and financial services across Europe. EventBot is designed to read SMS messages and targets over 200 different financial applications mostly in the US and Europe.