Check Point
SOFTWARE TECHNOLOGIES LTD.

Apr 12 - 18, 2021

YOUR CHECK POINT
THREAT INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- The U.S National Security Agency (NSA), the Cybersecurity and infrastructure security agency (CISA), and the Federal Bureau of Investigation (FBI) have published a joint advisory warning that a Russia-linked APT group, APT25, is exploiting five vulnerabilities in an ongoing attack against U.S targets.

  Check Point IPS provides protection against this threat *(Fortinet FortiOS SSL VPN Directory Traversal (CVE-2018-13379); Pulse Connect Secure File Disclosure (CVE-2019-11510); Citrix Multiple Products Directory Traversal (CVE-2019-19781))*

- Codecov, an online platform for hosted code testing, has suffered a breach. The company announced that a threat actor had modified its Bash Uploader script, exposing information in customers' continuous integration (CI) environment.

- Slack and BaseCamp collaboration tools have been abused by the BazarLoader malware in two new campaigns. The malware is using email messages with links to the platforms' cloud services to distribute the malware payload.

  Check Point Threat Emulation and Anti-Bot provide protection against this threat *(Trojan-Downloader.Win64.BazarLoader)*

- After the March breach of the ParkMobile parking app, data stolen in the incident is now offered for sale on a cybercrime forum. The data consists of 21 million user records, including email, phone number, hashed passwords and license plate number, belonging to customers like Donald Trump, Hillary Clinton, security Journalist Brian Krebs, and more.

- The University of Hertfordshire, UK, has suffered an attack that shut down all of its IT systems including Office 365, Teams and Zoom, local network, Wi-Fi, email, data storage, and VPN. Following the attack, all live online teaching has been canceled for 2 days.

- NBA team Houston Rockets has been investigating a cyber-attack against their network by a new ransomware group that claims on their dark web page to have stolen 500 gigabytes of data including contracts, non-disclosure agreements, and financial data.

  Check Point Harmony Endpoint provides protection against this threat

VULNERABILITIES AND PATCHES

- Microsoft's April 2021 Patch Tuesday covers 114 CVEs including Exchange Server remote code execution flaws, SMB information disclosure flaws, and a privilege escalation vulnerability exploited in the wild.

  Check Point IPS blade provides protection against these threats (Microsoft Win32k Elevation of Privilege (CVE-2021-28310); Microsoft Windows SMB Information Disclosure (CVE-021-28324); Microsoft Windows SMB Information Disclosure (CVE-2021-28325))

- Two new Zero-Day vulnerabilities found in Google Chrome and Microsoft Edge have been posted on Twitter as PoC exploits. A fix is expected to be released in the upcoming days.

- Researchers have disclosed "NAME:WRECK", a set of nine DNS vulnerabilities affecting over 100 million devices. The vulnerabilities have the potential to cause either Denial of Service (DoS) allowing attackers to take targeted devices offline or to gain control over them by Remote Code Execution (RCE).

- Jupiter Networks have released fixes for multiple vulnerabilities including Kernel panic upon receipt of specific TCPv6 packet on management interface and critical remote code execution in overdyed services.

THREAT INTELLIGENCE REPORTS

- Check Point Research has reported that Microsoft was the most imitated brand in phishing attempts during Q1 2021, and two banks are also in the top 10 imitated brands.

  Check Point Anti-Phishing provides protection against this threat

- Check Point Research has reported that IcedID has entered the global malware index for the first time, taking second place, after exploiting the Covid-19 pandemic to lure new victims. The Dridex Trojan has taken over the first place.

  Check Point Threat Emulation provides protection against these threats (Trojan-Downloader.Win32.IcedID; Trojan.Win32.Dridex)

- Researches have detected new variants of the Linux-based IoT malware Gafgyt with incorporated code re-used from the infamous Mirai botnet to expand capabilities in conducting DDoS attacks, in addition to new exploits for initial compromise of Huawei, Realtek, and Dasan GPON devices.

  Check Point Threat Emulation and Anti-Bot provide protection against this threat (Botnet.Linux.Gafgyt; Backdoor.Linux.Gafgyt)

- Threat actors are targeting unpatched Microsoft Exchange servers, exploiting the recently exposed ProxyLogon vulnerabilities in a new campaign designed to install cryptocurrency mining malware.

- A major BGP routing leak has been spotted, potentially indicating BGP hijacking activity, in Vodafone's autonomous network (AS55410) based in India. The leak has impacted U.S companies, including Google.

- A new Linux and macOS malware has been found hidden in a malicious package named "web-browserify", imitating the popular Browserify npm component.