Check Point
SOFTWARE TECHNOLOGIES LTD.

May 24-30, 2021

YOUR CHECK POINT
THREAT INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- Check Point Research has conducted a joint investigation into an ongoing and highly targeted campaign against China's Uyghur minority, using messages and sites impersonating UN and human rights groups. The attackers deployed malware capable of exfiltrating information and gaining control of victim PCs.

- The Russian-based hackers behind the SolarWinds attacks, have been conducting an ongoing phishing campaign targeting government agencies, think tanks, and consultants. The campaign started in January 2021 when the group started delivering malicious links while impersonating the US Agency for International Development (USAID). Researchers have linked the threat actors with APT29, AKA Nobelium. In those attacks, the hackers deployed four new malware families.

- Researchers have observed a new wave of the BazarCall phishing campaign that delivers the BazarLoader malware and manages to bypass automated threat detection systems. The hackers impersonate a streaming service, claiming that the user's trial is about to expire and their credit card will be charged.

  Check Point Anti-Bot and Anti-Virus provide protection against this threat (Trojan-Downloader.Win64.BazarLoader; Backdoor.Win32.BazarCall)

- A threat group dubbed CryptoCore has stolen hundreds of millions of dollars from the US, Israel, Europe, and Japan entities over the past three years, by breaching cryptocurrency exchanges and collecting funds. Researchers have linked the campaign to the Korean state-sponsored group Lazarus.

- Since December 2020, Agrius, an Iranian-based threat actor, has targeted Israeli entities in a targeted espionage campaign. The hackers masqueraded their campaign as ransomware attacks while maintaining access to victims' networks for months and deployed the DEADWOOD and Apostle wipers.

- Canada's national mail carrier has suffered a ransomware attack on one of its suppliers that impacted 44 of its largest corporate customers, and compromising the data of more than 950,000 clients. The threat actors managed to steal information dating from July 2016 to March 2019.

VULNERABILITIES AND PATCHES

- Hewlett Packard Enterprise (HPE) has released a fix for a critical vulnerability, CVE-2020-7200, in the HPE SIM (Systems Insight Manager) software. The vulnerability affects the latest versions (7.6.x) for Windows and allows attackers with no privileges to exploit it in low complexity attacks.

  Check Point IPS blade provides protection against this threat *(HPE Insight Manager Insecure Deserialization (CVE-2020-7200))*

- Severe security flaws have been discovered in Visual Studio code extensions, which are in use by millions of users. The vulnerabilities could be utilized to run arbitrary code on a developer's system remotely, in what could ultimately pave the way for supply chain attacks.

- SonicWall has been urging its customers to patch CVE-2021-20026, which impacts the Network Security Manager (NSM) multi-tenant firewall management solution. This post-authentication vulnerability allows an attacker to perform OS command injection without user interaction.

- VMware has warned of a critical vulnerability tracked as CVE-2021-21985 that affects all vCenter Server installs. This remote code execution vulnerability can be used by anyone who can reach the vCenter Server over the network to gain access.

THREAT INTELLIGENCE REPORTS

- Researchers have observed the XCSSET spyware exploiting CVE-2021-30713, a critical vulnerability in macOS, which allows an attacker to take screenshots of the user's desktop without requiring additional permissions. The vulnerability was patched by Apple in the latest version of macOS, Big Sur 11.4.

  Check Point SandBlast and Anti-Virus provide protection against this threat *(Trojan.Mac.XCSSET; XCSSET)*

- Researchers have discovered 50,000 IP addresses compromised by the TeamTNT threat group in a campaign against Kubernetes clusters, which took place between March and May and hit mostly China and the US. The hackers deployed a custom tool and then the XMRig Monero miner on compromised systems.

  Check Point Threat Emulation. Harmony Endpoint and Anti-Virus provide protection against these threats *(Cryptominer.Win32.TeamTNT; TS_Miner.Win32.XMRig)*

- The number of cyberattacks targeting the Asia Pacific region has increased by 168% in the past year, according to Check Point Research. The malware types that were most common in those attacks were ransomware and remote access Trojan (RAT), and Japan and Singapore were the most targeted countries.

- Check Point Research has exposed the IcedID botnet infrastructure and tracked the activity of its C&C servers. The researchers leveraged the botnet's use of self-signed certificates to uncover the servers, and gained access to extensive campaign information.

  Check Point Anti-Bot and Anti-Virus provide protection against this threat *(Banking.Win32.IcedID)*