Check Point
SOFTWARE TECHNOLOGIES LTD.

June 21-27, 2021

YOUR CHECK POINT
THREAT INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- Russian-based threat group Nobelium is using password spraying and brute force attacks to gain access to corporate networks. The group, which was behind the SolarWinds supply-chain attack, deployed an information-stealing Trojan on a Microsoft customer support agent's computer to steal information. Over half of the targets were IT companies.

- The PYSA ransomware gang has been leveraging the remote access Trojan ChaChi to hack into education institutions and healthcare organizations in the United States and the United Kingdom.

  Check Point Harmony Endpoint provides protection against this threat (Ransomware.Win32.Virlock.TC.pysa)

- A new campaign attributed to the North Korean threat group Lazarus has been discovered, in which the group utilized the NukeSped RAT, the Bundlore adware, and the ThreatNeedle Trojan.

  Check Point SandBlast and Anti-Virus provide protection against this threat (Trojan.Win32.NukeSped; Adware.Mac.Bundlore; Trojan.Win32.ThreatNeedle)

- The US Financial Industry Regulatory Authority (FINRA) is warning of an ongoing phishing attack that impersonates FINRA where threat actors are sending emails pretending to be from 'FINRA Support'.

- The City of Tulsa, Oklahoma, has suffered a ransomware attack by the Conti ransomware gang. The attackers stole personal information that belongs to the citizens and published police citations online. The attack also disrupted Tulsa's online bill payment systems, utility billing, and email service.

  Check Point Harmony Endpoint provides protection against this threat (Ransomware.Win32.Conti)

- Mercedes-Benz has disclosed a data breach impacting 1.6 million unique customer records. The stolen data includes credit card information, social security numbers, and driver license numbers. The sensitive data was exposed due to an insufficiently secured cloud storage service.

- Western Digital My Book Live NAS devices have been wiped and their owners were locked outside in a recent attack. This was an exploitation of a remote command execution vulnerability. The affected devices were directly accessible from the Internet, and on some of the devices, the attackers installed a Trojan.

VULNERABILITIES AND PATCHES

- Check Point Research has identified XSS and CSRF security flaws on Atlassian, the team collaboration and productivity platform used by 180,000 customers worldwide. With just one click, an attacker could have used the flaws to take over accounts and control some of Atlassian's applications, including Jira and Confluence.
- Four major vulnerabilities have been discovered in the BIOSConnect feature of Dell SupportAssist. The flaws allow attackers to impersonate Dell.com and to remotely execute code within the BIOS of compromised devices. The issue affects about 30 million devices and has not been fixed yet.
- VMware has published a fix for CVE-2021-21998, a critical vulnerability in Carbon Black App Control, which allows a threat actor to access the server with admin privileges without authentication.
- Researchers have warned that CVE-2020-5135, a critical SonicWall vulnerability disclosed last year, was not fully fixed. The bug allows unauthenticated remote attackers to execute arbitrary code, or cause a denial of service.
- The Tor Project has released a new version of the Tor Browser. The new version fixes numerous bugs, including a bug that allowed a threat actor to collect fingerprints from the applications installed on the compromised device.

THREAT INTELLIGENCE REPORTS

- Microsoft has mistakenly signed a malicious driver called Netfilter, which is in fact a malware. The driver is being distributed within gaming environments and was seen communicating with China-based C&C IPs.

  Check Point Anti-Virus provides protection against this threat (Rootkit.Win32.Netfilter)

- Researchers have observed TA543, a cybercrime group, deploying a new variant of the JSSLoader malware in their recent phishing campaign. The initial infection vector is through malicious phishing emails that impersonate shipping companies such as UPS and ask the victim to insert a correct shipping address.
- A threat actor has begun to utilize Windows imaging format (WIM) attachments to distribute the AgentTesla information stealer. These campaigns start with phishing emails that pretend to be shipping information from DHL or Alpha Trans.

  Check Point SandBlast and Anti-Bot provide protection against this threat (Trojan.Win32.AgentTesla)

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