Check Point
SOFTWARE TECHNOLOGIES LTD.

Aug 30 - Sept 6, 2021

YOUR CHECK POINT
THREAT INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- Following the SolarWinds Orion supply-chain attack, the software firm Autodesk announced they identified a compromised server and realized they were also attacked by the Russian linked group Cozy Bear as part of the espionage campaign.
- The Thai airline Bangkok Airways has announced they were the target of the LockBit ransomware gang. The threat actors announced on their leak website they were holding 200GB of stolen data including passengers' sensitive data, and threatened to leak it if the company refuses to pay the ransom.

  Check Point Harmony Endpoint provides protection against this threat *(Ransomware.Win32.LockBit)*
- US-based DuPage Medical Group has experienced a data breach, potentially affecting sensitive medical and private information of 600,000 patients in 100 locations.
- The Conti ransomware gang has been hacking into Microsoft Exchange servers using the Proxyshell exploits that allow remote code execution on unpatched servers.

  Check Point SandBlast Agent and IPS provide protection against this threat (Ransomware.Win32.Conti; HEUR:Trojan-Ransom.Win32.Conti; Microsoft Exchange Server Remote Code Execution (CVE-2021-34473))
- A researcher has found that over 60,000 parked domains from the domain management company MarkMonitor were left vulnerable to AWS hijacking. The domains were seen pointing to nonexistent Amazon S3 bucket addresses, implying that domain takeovers can be done.
- US officials are warning of potential investment scams associated with the repercussions of Hurricane Ida: victims targeted will likely be among those receiving compensation from insurance companies covering Hurricane damages.
- After being fired from a New York credit union, a former revengeful employee deleted 21 GB of data from the company's file server, including loan applications and highly sensitive information.

VULNERABILITIES AND PATCHES

- Check Point Research has recently exposed a new Out-Of-Bounds read-write vulnerability, tracked as CVE-2020-1910, in the WhatsApp instant messaging app. The issue, which could have allowed a sophisticated attacker to read sensitive information from WhatsApp memory, was subsequently patched.
- Threat actors are currently exploiting the Atlassian Confluence remote code execution vulnerability that was recently unveiled, aiming at installing crypto miners. The vulnerability, tracked as CVE-2021-26084, allows a user to execute arbitrary code on a Confluence Server or Data Center instance.
- Sixteen vulnerabilities dubbed BrakTooth are affecting Bluetooth stacks on system-on-a-chip and could impact billions of varied devices including industrial equipment. The vulnerabilities could allow a threat actor a range of possibilities, including the ability to execute malware on a device.
- Cisco has announced patching a severe authentication bypass vulnerability (CVE-2021-34746) in its Enterprise Network Function Virtualization Infrastructure Software (NFVIS) which could have allowed a remote attacker to circumvent authentication and log into a vulnerable device as an administrator.

THREAT INTELLIGENCE REPORTS

- The Conti ransomware gang playbook that was published by an affiliate of the group last month has been translated to English, and delivers many insights into the attackers' methods.

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

- The entire source code of Babuk Locker (or Babyk) ransomware has been leaked on a Russian speaking hacker forum by a threat actor allegedly tied to the group, claiming to be suffering from a terminal illness.

  Check Point Threat Emulation and Harmony Endpoint provide protection against this threat *(HEUR:Trojan-Ransom.Linux.Babuk; Ransomware.Win.Babuk)*

- The FIN7 cybercrime gang has launched a new campaign using Windows 11 theme lures. The group targeted the point-of-sale provider Clearmind, with malicious Microsoft Word documents that include a VBA macro, and made sure that the targets were not from one of the CIS countries.
- The FBI has released a special warning saying that ransomware gangs are aggressively targeting the food and agricultural sectors that could not only cause financial damage but also impact food supply chains like restaurants, markets, farms, or producers.
- The FBI and CISA jointly warn of the higher risk of ransomware attacks during weekends and holidays, especially when company's offices are closed.