March 29 - April 4, 2021

Check Point SOFTWARE TECHNOLOGIES LTD.

YOUR CHECK POINT

THREAT INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- Personal information of some 553 million Facebook users from 100 countries has been stolen and published online for free in a hacking forum. The records include full name, Facebook ID, phone number, email, location, bio and more.

- Iranian APT group Charming Kitten, linked to the government, has launched a new phishing campaign targeting medical professionals from the fields of genetics, neurology and oncology in the United States and Israel. The campaign relies on emails delivering links to fake Microsoft 365 and OneDrive login pages.

- The Clop ransomware gang has leaked personal and financial information stolen from users in Stanford Medicine, the University of California, and the University of Maryland Baltimore. The actor has leveraged flaws in the Accellion File Transfer Appliance, in use by the universities for knowledge sharing.

  Check Point Harmony Endpoint and Threat Emulation provide protection against this threat *(Ransomware.Win32.Clop)*

- Malware attack has hit Applus Technologies, a global certification sector company, leading to the immediate shut-down of its vehicle inspections activities. The company had to disconnect its IT systems from the internet, and the operational recess has impacted operations in eight US states.

- Asteelflash, a French multinational electronics manufacturing company, has suffered an attack by the REvil ransomware. The company has not released an official statement yet, and the cybercrime gang is demanding a $24 million ransom.

  Check Point Harmony Endpoint and Threat Emulation provide protection against this threat *(Ransomware.Win32.Revil)*

- The hackers behind the SolarWinds Supply-Chain attack, of Russian origin, have gained access to the secretary of the Department of Homeland Security (DHS) in Trump's administration, among other DHS officials. Thousands of emails were stolen.

  Check Point Anti-Bot and Anti-Virus provide protection against this threat *(Backdoor.Win32.SUNBURST; Trojan.Win32.TearDrop)*

VULNERABILITIES AND PATCHES

- VMWare has issued security patches for two critical vulnerabilities in vRealize Operations, its IT operations management AI-based platform. Assigned CVE-2021-21975 and CVE-2021-21983, the flaws might allow an actor to obtain admin credentials and, if chained together, remote code execution.
- OpenSSL has released patches for two high-severity vulnerabilities. The flaw assigned CVE-2021-3450 might lead a client to accept a malicious TLS certificate, whereas the flaw assigned CVE-2021-3449 could lead to a crash or a denial of service.
- Five vulnerabilities have been discovered in the TBox remote terminal units (RTUs) of Ovarro, an asset management company for critical and national infrastructure. The flaws might allow remote code execution and denial-of-service attacks against industrial control systems, without user authentication.

THREAT INTELLIGENCE REPORTS

- Long-lasting espionage campaign that emerged on March 2019 has been targeting Japanese users, most notably from the manufacturing sector, leveraging vulnerabilities in Pulse Connect Secure VPN. Researchers estimate that the Chinese group APT10 is behind the campaign.

  Check Point IPS provides protection against this threat *(Pulse Connect Secure File Disclosure (CVE-2019-11510); Pulse Connect Secure Remote Code Execution (CVE-2019-11539))*

- The FBI and CISA have released a warning against scanning efforts carried out by unknown nation-state actors in order to detect machines vulnerable to three vulnerabilities in Fortinet's operating system, FortiOS. Surge in scanning attempt has been observed as of March.

  Check Point IPS provides protection against this threat *(Fortinet FortiOS SSL VPN Directory Traversal (CVE-2018-13379))*

- GitHub code repository hosting service has been investigating a wave of attacks utilizing the platform's cloud infrastructure in order to mine cryptocurrency, using crafted malicious GitHub Actions.
- Threat actors have been advertising alleged video gaming cheat tools, which in fact install a remote access Trojan dubbed COD-Dropper. Cheat tools typically have high system privileges and require to deactivate security measures, thus facilitating the installation of the malware.
- The North Korean campaign targeting security experts involved in vulnerability research, first published on January, has resumed. The attackers utilize alleged official websites presenting fake security companies in order to lure researchers into accessing a malicious PGP public key download link.

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