January 6 - 12, 2020

Check Point
SOFTWARE TECHNOLOGIES LTD.

YOUR CHECK POINT THREAT INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- Austria’s foreign ministry has suffered a serious cyber-attack, allegedly conducted by a foreign state.
- US government-funded low-cost UMX mobile phones include preinstalled “unremovable” malware. The malware, a variant of HiddenAds, is suspected to be of Chinese origin, as is the UMX phone itself.
- Three malicious apps on Google Store have been exploiting the CVE-2019-2215 vulnerability to compromise Android devices. This is the first published exploit for the vulnerability, exposed in October, claimed to have been used by the NSO group.

  Check Point SandBlast Mobile and IPS provide protection against this threat (Google Android Use-after-free (CVE-2019-2215))
- HappyHotel, a Japanese search engine for booking rooms in “love hotels”, has disclosed a security breach revealing clients’ personal information, including real names, email addresses, login credentials, phone numbers, payment details and more. Similar to the 2015 Ashley Madison hacking, this attack exposes victims to extortion and even suicide.
- Cyber espionage campaign targeting NGOs, political organizations and government agencies in Asia has been uncovered. The operation, attributed to the Chinese APT group Bronze President, has been active since at least mid-2018 and used a verity of tools, both known and custom made, probably gaining initial access using phishing emails with malicious links.
- Following the refusal of Travelex to pay ransom demand of $6M in exchange for decryption keys, the group behind the Sodinokibi ransomware (aka REvil) now threatens to sell 5GB of customer personal information stolen and exfiltrated prior to the encryption, thus exposing the company to GDPR procedures.
- Albany County Airport Authority announced it has been hit by a Sodinokibi ransomware attack encrypting its servers and backup systems. Attack entry point was through the airport’s MSP (Managed Services Provider) LogicalNet and following payment of an undisclosed ransom demand, authorized by the insurance carrier, the authority received decryption keys from the attacker.

  Check Point SandBlast provides protection against this threat

VULNERABILITIES AND PATCHES

- Check Point Research has discovered critical vulnerabilities in the popular TikTok application, utilized by more than 1.3 billion users. Reported vulnerabilities could allow attackers to hijack TikTok accounts, manipulate their content, delete and upload videos and more.
- PoC of exploits utilizing two RCE vulnerabilities in Citrix's ADC and Gateway products have been published, demonstrating how to take full control of the systems. According to Shodan, more than 125K devices are publicly accessible and exploitable, with malicious exploitations already detected for more than a week. Citrix has not released patches but published mitigation directions for system admins.

  Check Point IPS blade protects against this threat (Citrix Multiple Products Directory Traversal (CVE-2019-19781))
- Mozilla has released two Firefox web browser versions to patch a critical zero-day vulnerability (CVE-2019-170260) currently actively exploited in the wild.

THREAT INTELLIGENCE REPORTS

- US CISA (Cybersecurity Agency) is warning organizations of ongoing campaigns by multiple APT and state sponsored groups, exploiting the well-known Pulse Secure VPN vulnerability (CVE-2019-11510) to breach into networks, occasionally delivering the Sodinokibi ransomware. Though patches have been available since April 2019, there are currently more than 3,600 vulnerable servers online.

  Check Point IPS blade provides protection against this threat (Pulse Connect Secure File Disclosure (CVE-2019-11510))
- New ransomware dubbed Snake has been reported to target large organizations designed to encrypt entire networks rather than individual workstations. The new malware, first reported last week, is written in Go programming language.

  Check Point Anti-Virus blade provides protection against this threat (Ransomware.Win32.Snake)
- Researchers report TrickBot operators have developed and used a new PowerShell backdoor for high value targets named PowerTrick. Trickbot has been developed continuously since its initial detection in 2016 and PowerTrick is designed to enhance its ability to bypass restrictions and security controls.

  Check Point Anti-Virus blade provides protection against this threat (Backdoor.Win32.Powertrick)
- New report follows the continuing operations of the North Korean Lazarus APT group targeting cryptocurrency related websites. New findings show the sequel of the 2018 AppleJeus operation using advanced TTPs with new victims in the UK, Poland, Russia and China.

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

©2020 Check Point Software Technologies Ltd. All rights reserved. [Protected] Non-confidential content