December 2 - 8, 2019

Check Point
SOFTWARE TECHNOLOGIES LTD.

# YOUR CHECK POINT THREAT INTELLIGENCE REPORT

## TOP ATTACKS AND BREACHES

- The Vietnam-linked APT group Ocean Lotus has breached networks of the car manufacturers BMW and Hyundai. The group, previously linked to different car vendor attacks, reportedly performed a watering hole attack and deployed the hacking tool Cobalt Strike to access the network of both companies.

  *Check Point IPS and Anti-Bot blades provide protection against this threat (Cobalt Strike Payload Remote Code Execution; Cobalt Strike Beacon Suspicious Communication; Backdoor.Win32.CobaltStrike)*

- CyrusOne, one of the biggest data center providers in the United States, has fallen victim to a targeted ransomware attack. The ransomware strain infecting the company and six of its customers with Sodinokibi (also known as REvil), and the point of entry is currently unknown.

  *Check Point Threat Emulation provides protection against this threat*

- Hackers have injected a malicious skimmer to the website of the American gunmaker Smith & Wesson, allowing them to potentially steal customer payment data. It is speculated that the attackers exploited a vulnerability in Magento web platform to inject the malicious code.

- The state of Ohio has detected and thwarted an SQL injection attempt towards their official website on their election day in early November. The attack was aimed at disrupting their election infrastructure, and forensic investigation traced it back to a Russian-owned company.

- A poorly-secured, plain-text database belonging to TrueDialog, a business SMS provider, has been discovered, affecting over 100 million US citizens. It contained millions of SMS messages sent from businesses to potential customers, and private messages and personal data of TrueDialog users.

- Moscow's CCTV city surveillance footage as well as Facial Recognition data are being offered for sale on underground forums, possibly by local law enforcement and government individuals. The sellers offer 5-day links for live footage access, lookup services in the Facial Recognition systems and permanent login credentials for the video surveillance system.

## VULNERABILITIES AND PATCHES

- A severe vulnerability has been discovered, affecting most Linux and Unix-like operating systems. The vulnerability, tracked as CVE-2019-14899, can be exploited to tamper with and spy on VPN connections by attackers with access to the victim's network.
- Two vulnerabilities in the GoAhead web server software have been uncovered, potentially affecting hundreds of millions of Internet-connected devices. Both vulnerabilities may lead to code execution and could be exploited by attackers sending specially-crafted HTTP requests.
- Strandhogg, an unpatched vulnerability in Android OS that resides in the multitasking feature of Android, is actively exploited in the wild by dozens of malicious apps. Successful exploitation of Strandhogg allows malicious apps to hijack tasks of legitimate apps and display fake interfaces to users.

  *Check Point SandBlast Mobile provides protection against this threat*

## THREAT INTELLIGENCE REPORTS

- Check Point Incident Response has investigated a highly sophisticated and unique Business Email Compromise attack earlier this year. The attacker targeted two companies in the process of a multi-million dollar deal and tracked their email threads. He then purchased domains similar to the victim ones and acted as a man-in-the-middle for their email correspondences, eventually modifying the bank account information that was provided for the transfer and directing the funds to his own account.
- Researchers have uncovered ZeroCleare, a destructive data-wiping malware used by two Iran-linked APT groups - Oilrig and xHunt - to target energy-sector organizations in the Middle East. The attackers used brute-forcing of corporate credentials, web shell injection and exploitation of a SharePoint vulnerability in order to deploy the wiper malware.

  *Check Point Anti-Virus blade provides protection against this threat* *(Trojan.Win32.ZeroCleare)*
- A new phishing method has been spotted, using HTML files with obfuscated JavaScript as mail attachments. Once the victim opens the file, the script will generate a fake Microsoft Docs login form and send the entered credentials to the attacker, without requiring the attacker to craft a phishing URL.

  *Check Point Anti-Virus blade provides protection against this threat* *(Phishing.Win32.Phishing HTML)*
- Researchers have discovered a new macOS malware suspected to belong to the North-Korean APT group Lazarus. The sample, which was discovered on an online cryptocurrency trading platform, can load a mach-O executable file from memory and execute it as a fileless malware. The sample discovered does not retrieve any payload from the C2 server, suggesting that the malware is still under development.

  *Check Point Anti-Virus blade provides protection against this threat* *(Trojan.Mac.Generic)*