August 26 – September 01, 2019

Check Point SOFTWARE TECHNOLOGIES LTD.

YOUR CHECK POINT THREAT INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- PerCSoft and Digital Dental Record, two online cloud based backup providers used by hundreds of dental practices across the US to safeguard their medical records and other patient information, have been hit by a ransomware attack. Sources say Sodinokibi ransomware was used in the attack and the companies are currently working on decryption after allegedly paying attackers an unpublished sum.

  Check Point SandBlast provides protection against this threat

- Researchers have identified a new threat group targeting Middle East critical infrastructure organizations with novel malware sent though targeted phishing emails. There is insufficient evidence for clear attribution of the group, now named LYCEUM, but researchers say several methods used by it are indicative of other groups with ties to the Iranian government.
- The popular web hosting provider Hostinger has been hit by a massive data breach. Unknown hackers gained access to one of its databases holding personal information of nearly 14 million customers. Investigation to the source of the breach is ongoing and the company has reset passwords for all affected accounts.
- A broad campaign of iPhone hacking has been revealed. For at least two years, attackers have been using compromised websites and exploiting 14 separate vulnerabilities in Apple's iOS to install spyware on thousands of Apple devices innocently visiting websites. Attackers gained access to location data, photos, contacts, Keychain passwords, WhatsApp and other communication and social media content.
- 80 e-commerce websites have been compromised by Magecart groups who used outdated versions of Magento CMS to install JS code and send customers' payment information to attackers. Attackers either sold credit card details or used merchandise mules for fraudulent purchases to launder transactions.
- Cyber security company Imperva has alerted its customers that it suffered a data breach exposing sensitive information of some of its Cloud Web Application Firewall (WAF) clients. The exposed data includes email addresses, scrambled passwords, API keys and SSL certificates.

VULNERABILITIES AND PATCHES

- Cisco has advised its customers of a new critical vulnerability, CVE-2019-12643, which could affect several of its routers and allow attackers to gain full control over them. Cisco released patches to relevant models.
- A vulnerability in Google Chrome which could allow arbitrary code execution has been reported and patched. The vulnerability (CVE-2019-5869) resides in Blink, an open-source browser engine that powers Google Chrome.

THREAT INTELLIGENCE REPORTS

- CamScanner, a popular PDF creator app for Android devices with more than 100 million users, has been found to include a hidden Trojan Dropper that allows download and installation of malicious programs in its latest version. The malicious module is part of a third party advertising library. Following the report, Google removed CamScanner from its Play Store.

  Check Point SandBlast Mobile provides protection against this threat

- French police has remotely disinfected more than 850,000 computers infected with the Retadup botnet, used mostly for cryptomining. Taking over the C&C server that was hosted in France, the police used a flaw in its communication protocol to command botnet instances to self-destruct.

  Check Point Anti-Bot blade provides protection against this threat (Trojan.Win32.Retadup)

- New research finds that FIN6, a financially motivated cybergang, has switched to target e-commerce checkout pages in search of payment card data. The group, active since 2015 and until now mostly targeting Point of Sale (POS) machines in the US and Europe, has deployed a variety of tools and social engineering techniques in this new attack line.
- A feature in Google calendar, which by default allows addition of calendar events from external emails, is being actively exploited to insert malicious links into users' calendars. This is part of the growing use of cloud-based data storage services which seem more trustworthy by both users and spam filters for malicious purposes.

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