November 18 - 24, 2019

Check Point
SOFTWARE TECHNOLOGIES LTD.

YOUR CHECK POINT
THREAT INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- Ryuk ransomware attack on Virtual Care Provider Inc. IT services provider has resulted in the shut-down of IT services for 110 US nursing homes and could ultimately cause the untimely demise of some of its patients. Access to patient medical records, phone systems, internet services, email, salaries and billing were all denied on condition of payment of a $14 million ransom. Evidence suggests VCPI was compromised by Trickbot, Emotet, or both, as far back as September 2018.

  Check Point SandBlast Anti-Ransomware and Anti-Bot blades provide protection against this threat (Trojan-Banker.Win32.TrickBot; Trojan.Win32.Emotet)

- Additional noticeable ransom attacks this week have hit the Rouen University Hospital Centre (CHU) in France, 400 veterinary hospitals of the National Veterinary Associates with Ryuk ransomware and a large-scale coordinated ransomware attack on the Louisiana State Government.

  Check Point Anti-Bot blade provides protection against this threat

- The official Monero cryptocurrency site has been hacked and existing files were replaced with malicious versions designed to steal funds from users' wallets.

- Website of Chinese smartphone producer OnePlus has been breached and attackers gained access to customer PII (Personally identifiable information) and order information.

- Telecom giant T-Mobile has reported it suffered a data breach of personal information of its customers. The company did not release further details and is currently notifying affected customers.

- Macy's department store website has been compromised in a Magecart style attack, skimming credit card details of customers using its desktop shopping site.

- HackBack hacktivists group has published 2TB of confidential information exfiltrated from the Cayman National bank, including customer names and balance information. The materials were released following a $100K "hack bounty" announcement by HackBack, calling for politically motivated attacks.

VULNERABILITIES AND PATCHES

- Hundreds of popular Android apps investigated on Google Play, including Yahoo Browser, Facebook, Instagram and WeChat, are still exposed to long-known vulnerabilities. As reported by Check Point Research, this is caused by failure of app maintainers to incorporate security fixes made in open source sub-components into new versions of popular application.
- A vulnerability (CVE-2019-2234) in a camera application, pre-installed on millions of Android smart phone models by Google, Samsung and others, could be leveraged by rogue apps to take photos, record videos and eavesdrop, even when the app is closed, screen turned off and phone locked.
- A critical bug has been discovered in Jetpack, a popular WordPress security plugin maintained by WordPress, with over 5 million active installations. WordPress released a patch and stated it has no evidence of exploits in the wild.

THREAT INTELLIGENCE REPORTS

- Check Point Research in-depth analysis of the Phorpiex botnet has revealed a large-scale operation, controlling more than 1 Million Windows-operated machines, generating an annual income of approximately half a million US dollars. Phorpiex revenue-generating activities include crypto-jacking, sextortion spam, crypto-clipping and malware infection services.

  Check Point Anti-Bot blade provides protection against this threat (Worm.Win32.Phorpiex.)*
- A new mobile banking Trojan dubbed Gimp is attacking Android devices, and was available on the official Google Play Store. The Trojan has been active for the last 5 months, and derives its code from the infamous Anubis banking Trojan. It can take over as the default SMS app, perform overlay attack on social media and banking apps, and elevate its permissions over the device to admin.

  Check Point SandBlast Mobile provides protection against this threat
- Research by the Vanderbilt University finds that hospitals hit by a data breach or ransomware attack can expect an increase in death rate among heart patients in the months or years following attacks due to delays caused by the attacks and cybersecurity remediation efforts.
- After a week-long shutdown of Iran's internet in an attempt to combat nationwide protest over gasoline prices, with an estimate of over 100 casualties, Iranian authorities have now restored internet connectivity. Shut down took 24 hours to coordinate between ISPs and mobile data providers and has emphasized domestic discussion about Iran's nationwide intranet and its sustainability.