January 7 - 13, 2019

Check Point SOFTWARE TECHNOLOGIES LTD.

YOUR CHECK POINT

THREAT INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- A 20-year-old German student has confessed that he was responsible for last week's major data breach that hit German chancellor Merkel and more than 1,000 other German politicians, celebrities and journalists. The information published included telephone numbers, addresses, credit card data, photographs, and private communications.
- The cryptocurrency exchange platform Coinbase has suspended the trading of Ethereum Classic (ETC) after double-spend attacks worth $1.1 Million. Attackers controlling more than 50% of miners on the ETC network were able to reorganize the Ethereum blockchain and transfer previously spent coins to their wallets.
- Security experts have uncovered a wide DNS hijacking campaign targeting government, telecommunications and internet infrastructure entities across the Middle East and North Africa, Europe and North America. Initial research suggests the actor or actors responsible have a nexus to Iran.
- Attackers used a recently addressed vulnerability in Office 365 to bypass existing phishing protections and deliver malicious messages to victims' inboxes.
- A cybersecurity researcher has discovered a massive online database containing records of more than 202 million Chinese citizens that was accessible to anyone on the Internet. Data is believed to have been collected from job seekers' resumes in various Chinese classified websites using a scraping tool called "data-import".
- U.S. government shutdown leaves dozens of government websites vulnerable to cyber-attacks or altogether inaccessible after not renewing expired Transport Layer Security (TLS) certificates. Affected sites include sensitive government payment portals and remote access services for organizations like NASA, the U.S. Department of Justice and the Court of Appeals.

VULNERABILITIES AND PATCHES

- Microsoft has issued its first Patch-Tuesday for this year to address 49 CVE-listed security vulnerabilities in its Windows operating systems and other products, 7 of which are rated critical. None of the vulnerabilities is known to be actively exploited in the wild.

  Check Point IPS blade provides protection against these threats

- Security researchers have discovered three vulnerabilities in Systemd, a popular init system and service manager for most Linux operating systems, that could allow unprivileged local attackers or malicious programs to gain root access on the targeted systems.

- Intel has patched three high-severity vulnerabilities that could allow the escalation of privileges across an array of products.

THREAT INTELLIGENCE REPORTS

- TA505, a financially motivated actor who was behind many of the Dridex campaigns that plagued organizations in 2015 and introduced Locky ransomware in 2016, has introduced two new malware families - "ServHelper" and "FlawedGrace" - a downloader and a RAT mostly targeting banks, retail businesses, and restaurants through spear phishing attacks.

  Check Point Anti-Virus and Anti-Bot blades provide protection against this threat *(Trojan.Win32.Servhelper)*

- Reports published this week attribute Ryuk ransomware to financially-motivated Russian cyber-criminals, and not North Korean state-sponsored hackers. Researchers believe North Korean hackers bought the same Hermes ransomware kit from hacking forums and used in an attack on the Far Eastern International Bank (FEIB) in Taiwan.

  Check Point SandBlast and Anti-Bot blades provide protection against this threat *(Trojan-Ransom.Win32.Ryuk)*

- French exploit vendor Zerodium, who buys and sells zero-day exploits to government agencies around the world, has announced an increase in prices. A bounty of $2,000,000 is offered for a persistent iOS jailbreak that can be executed remotely without any user interaction.

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