Check Point
SOFTWARE TECHNOLOGIES LTD.

February 3 - 9, 2020

YOUR CHECK POINT
THREAT INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- Twitter has suspended a network of fake accounts abusing its API to match millions of usernames and phone numbers. The feature, intended to indicate accounts matching existing contacts, was used on millions of randomly generated phone numbers. Twitter traces this campaign to state-sponsored actors with some evidence leading to Iran, Israel and Malaysia.
- The Israeli voter registration database, holding personal information of 6.5 million Israelis, has leaked after the ruling Likud party uploaded it to its election-day management application. Leaked information includes names, identity numbers, phone numbers and addresses of the entire Israeli population in voting age, in addition to custom data entered by Likud users.
- Threat actors are currently exploiting multiple vulnerabilities in the Linear eMerge E3 access control system for smart buildings. PoC and metasploit module published in November have led to attacks on thousands of units and ongoing scanning for more systems, mostly used for installation of DDoS bots.
- TVEyes, a TV search engine used for monitoring TV and radio broadcasts, has suffered a ransomware attack, causing an outage of all its services. The company announced it does not intend to pay ransom demand and is working on rebuilding its services on fresh hardware. TVEyes is widely used by political campaigns for the 2020 elections to monitor opponents and track ads.
- Australian logistics and transportation corporation Toll Group has suffered a targeted ransomware attack affecting over 1000 servers and disabling most of its services. Toll Group reports the ransomware used in the attack was a variant of Mailto aka Kokoklock.

  Check Point SandBlast and Anti-Virus blades provide protection against this threat (Ransomware.Win32.Mailto)
- The FBI has reported a DDoS attack on a state level voter registration site. The attacks, which occurred over the course of at least one month, included anomalous DNS server requests consistent with a Pseudo Random Subdomain (PRSD) attack.
- A database containing over 460,000 payment card records has been offered for sale on a popular underground cardshop. The database, comprising mostly of Indian banks' clients, is estimated at $4.2M, $9 per unit, and includes card number, expiration date, CVV/CVC and cardholder name and email.

VULNERABILITIES AND PATCHES

- Five high severity vulnerabilities have been reported in Cisco routers, switches, IP phones and cameras, collectively dubbed 'CDPwn'. The vulnerabilities expose clients to RCE and man-in-the-middle attacks by invaders already on their local network. Cisco released updates with patches to all these vulnerabilities.
- WhatsApp has released a patch for a vulnerability (CVE-2019-18426) in its desktop application that could enable cross-site scripting and lead to arbitrary code execution by attackers. Successful attack required the target to click on a link in a specially crafted text message.
- A vulnerability (CVE-2019-18634) in the Sudo utility for Unix could allow low privilege users or programs to execute commands with root privileges. Version 1.8.31 of Sudo, released last week, includes a patch to this problem.
- Google addressed a critical RCE vulnerability in Android OS that could be exploited to spread laterally to proximate targets through Bluetooth. The vulnerability, tracked as CVE-2020-0022, requires no user interaction.

THREAT INTELLIGENCE REPORTS

- Check Point Research has released a report discussing brand phishing for Q4 2019; frauds imitating brand websites using lookalike domains. The analysis shows that Facebook leads the list of brands abused in phishing attempts. Other brands in the list include Yahoo, Netflix, PayPal and Microsoft. Campaigns dedicated to mobile platforms were dominated by banking and social media brands, phishing for credentials, while other campaigns aimed to generate direct revenue.
- Researchers have exposed a new campaign by the Charming Kitten group, thought to be related to the Iranian intelligence services. The campaign targets journalists, political and human rights activists with phishing emails requesting interviews with leading news agencies aiming to take control over their email accounts.
- Comprehensive report (published in Dutch) finds that the TA505 financially motivated hackers group was behind the Maastricht university ransomware attack. The attack, which hit on December 23, deployed Clop ransomware on 267 windows systems. Initial infection was through two phishing emails received on October 15 and resulted almost three months later in payment of 30 Bitcoin. TA505 has used a variety of bankers (Dridex and Trickbot) and ransomware (Locky, BitPaymer, Philadelphia, GlobeImposter, and Jaff) in previous attacks.

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