Check Point
SOFTWARE TECHNOLOGIES LTD.

February 10 - 16, 2020

YOUR CHECK POINT
THREAT INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- Terrorist organization Hamas has targeted Israeli soldiers using a catfishing attack. Check Point researchers have detailed how the attack took place, in a manner similar to ones used in the past by previous APT-C-23 campaigns. Hamas operatives have disguised themselves as attractive single women who convinced the soldiers to download malicious dating apps. Once executed, the apps communicated with a C&C center, collecting data on the victim, such as phone number, location, SMS messages, and more, while having the capability to extend its code via command.

  Check Point SandBlast Mobile provides protection against this threat.

- Iranian APT groups have been exploiting vulnerabilities in Palo Alto Networks, Fortinet and other VPN systems to gain access to organizations from the IT, Telecommunication, Oil and Gas, Aviation, Government, and Security sectors around the world, in a campaign dubbed “Fox Kitten”.

  Check Point IPS blade provides protection against this threat (Pulse Connect Secure File Disclosure (CVE-2019-11510))

- A glitch in the TastSelv tax service has exposed almost 1.2 million CPR numbers of Danish citizens to Google and Adobe. Users who were logged into the service and clicked on ‘Correct contact information’ have encountered an error that subsequently sent their CPR numbers - the Danish personal ID numbers - to Adobe and Google. It appears the information was sent in clear text.

- The US Federal Trade Commission has issued a warning regarding phishing attacks relating to the fears surrounding the Coronavirus, where emails and text messages asking for donation or offer advice are used for attacks.

- Miami Beach police department has suffered a ransomware attack, encrypting computers in the police network.

- The Palm Beach County Supervisor of Elections in Florida has undergone a ransomware attack just before the 2016 US presidential elections. This attack was not reported to authorities until late in 2019.

VULNERABILITIES AND PATCHES

- Microsoft has announced fixes to the IE zero day (CVE-2020-0674) that was first announced in January to be used in "limited targeted attacks". The patch Tuesday fix included 99 security vulnerabilities, including 12 marked 'critical'. Microsoft has further provided fixes to different vulnerabilities in its Remote Desktop Protocol (RDP) client.

  Check Point IPS blade provides protection against this threat *(Microsoft Internet Explorer Use After Free (CVE-2020-0674))*

- SoundCloud has published a fix for API flaws that could have led to account takeovers. A broken authentication issue in combination with a user enumeration bug allowed potential attackers to gain full takeover of a SoundCloud user account.

- Adobe has released its second security patch of 2020, featuring 21 critical CVEs in Framemaker, 12 critical updates to Acrobat Reader and another in Flash Player, which included arbitrary code execution.

- Dell has released a patch for a vulnerability (CVE-2020-5316) in its SupportAssist Client software. The flaw could be exploited by local attackers to execute arbitrary code with administrator privileges.

THREAT INTELLIGENCE REPORTS

- Check Point Research shows that threat actors are using Valentine's Day as a theme for phishing emails and scams, trying to steal money and install malware.

- Researchers claim sextortion emails sent by Emotet are 10 times more effective in generating revenue than their Necurs counterparts. The attacks are carried in a similar fashion, claiming to own footage of the victim while browsing illicit websites, getting legitimacy by "revealing" user passwords obtained via password dumps. Emotet's greater potency is attributed to its use of Bitcoin (rather than Dashcoin), and mostly to the attack arriving at the recipient's work email, rather than a webmail address, causing more urgency to resolve the issue by the victim.

  Check Point SandBlast and Anti-Bot blades provide protection against these threats *(Trojan.Win32.Emotet)*

- US officials claim that Huawei equipment has a secret backdoor for spying, which exists for more than a decade. The White House urges allies to ban the Chinese giant, as US officials claim that cellular networks laid out by Huawei, such as 5G networks, can be used to "covertly access mobile-phone networks around the world through 'back doors' designed for use by law enforcement".

- Attackers have used American Express and Chase Bank fraud protection emails as a sophisticated phishing tool. The attacks use a familiar pattern, showing transactions and asking the customer "Do you recognize these charges?"; Once the victim clicks "NO", they are sent into a fake authentication site, where their credentials are harvested.