March 2–8, 2020

Check Point SOFTWARE TECHNOLOGIES LTD.

YOUR CHECK POINT

THREAT INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- Global fear of the Corona virus epidemic continues to be exploited for malicious cyber operations. Check Point Research reports of thousands of newly registered coronavirus related domains, which are 50% more likely malicious than other domains. CPR also informed of a Trickbot campaign using a fake health warning document to target Italian users.

  Check Point SandBlast and Anti-Virus blades provide protection against this threat (Banking.Win32.Trickbot)

- Colorado based space and defense parts manufacturer, Visser Precision, has fallen victim to a DoppelPaymer ransomware attack. Information stolen from Visser and its customers, including Tesla, Lockheed Martin, SpaceX and Boeing, has been published online in another attempt to extort ransom payment.

  Check Point SandBlast and Anti-Virus blades provide protection against this threat (Ransomware.Win32.Doppelpaymer)

- An unidentified demographic and financial information database, hosted on Google cloud, has been left unsecured for more than a month. Containing over 200 million records, the exposed information included name, address, email address, credit rating, income, net worth property info and more.

- UK based telecom provider Virgin Media has reported an year-long data leak exposing personal information of 900,000 customers, due to misconfiguration of a marketing database.

- Carnival Corporation cruise operator, the world's largest travel leisure company, has disclosed a data breach dating April 2019, in which an unidentified third party gained unauthorized access to employees' accounts, compromising customers' personal information including SSN and payment details.

- EVRAZ, one of the largest steel mining companies has been hit by ransomware attack, most likely Ryuk. The company issued a three-day layoff to its employees in in North America. Another Ryuk attack has hit Durham City and County, North Carolina, over the weekend and took down their systems.

  Check Point SandBlast and Anti-Virus blades provide protection against this threat

VULNERABILITIES AND PATCHES

- Linux systems are exposed to a recently detected 17 years old critical vulnerability in the PPP daemon software, part of almost all Linux based OS. The flaw, tracked as CVE-2020-8597, a stack buffer overflow, can be exploited for remote code execution (RCE) on attacked platforms.
- Cisco has released fixes to multiple bugs, including two RCE vulnerabilities tracked as CVE-2020-3127 and CVE-2020-3128 in the Webex Meetings application. Additional patches addressed issues in Cisco Prime Network Registrar and an SSL certificate validation flaw.
- Google's March security updates for Android address over 70 bugs and vulnerabilities, including several critical and high severity bugs.

THREAT INTELLIGENCE REPORTS

- A report by a South Korean research center finds increased activity of the financially motivated hacking group TA-505, targeting South Korean enterprises. Phishing attempts at finance, manufacturing and medical services included Excel documents delivering "FlawedAmmyy" RAT.

  Check Point SandBlast blade provide protection against this threat (RAT.Win32.FlawedAmmyy)

- A new sample of the Krakoff malware suggests Iranian affiliated APT34 is still active, currently conducting a campaign against the Lebanese government. This ongoing operation, first reported in November 2018, shows continued evolvement of TTPs and capabilities, presently exploiting a Microsoft exchange server.

  Check Point SandBlast and Anti-Virus blades provide protection against this threat (Trojan.Win32.OilRig)

- Qihoo 360, China's largest cyber-security company, has released a report attributing 11 years of offensive cyber activity against Chinese entities to the US CIA, naming the activity APT-C-39. The report links CIA tools like Fluxwire and Grasshopper of the Vault 7 project, details of which were leaked in 2017, to various attacks on China's aviation industry, scientific research institutions, petroleum industry, large internet companies and government agencies. US press links the report to recent US charges against Chinese APT groups.
- A recent paper demonstrates the use of ultrasonic guided waves to hack into mobile phones by exploiting voice assistant services. Dubbed SurfingAttack, the attack utilizes hard surfaces to conduct ultrasonic vibrations and access various information, bypassing 2FA protection without being detected.