Check Point
SOFTWARE TECHNOLOGIES LTD.

Aug 03 - 09, 2020

YOUR CHECK POINT
THREAT INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- Reddit has suffered an attack, in which tens of channels have been defaced to show messages in support of Donald Trump's reelection campaign.
- Canon has suffered from a Maze ransomware attack that impacts numerous services, including Canon's email, Microsoft Teams, USA website, and other internal applications. In an internal alert sent to employees, Canon mentioned that 10TB of company data has been stolen.

  Check Point SandBlast and Anti-Ransomware provide protection against this threat
- Intel Corporation has suffered a data breach leaking more than 20GB of the company source code and proprietary data. This is allegedly the first out of a multi-part series of Intel-related leaks.
- cPanel, web-sites administrative software, has been hit by a phishing scam. The unknown attackers spread phishing emails to cPanel users with a fake security advisory alerting them of a critical vulnerability in their web hosting management panel. Victims who clicked the malicious link were redirected to a phishing website asking for their cPanel credentials.

  Check Point SandBlast and Anti-Virus provide protection against this threat
- The British Dental Association (BDA) has suffered a data breach causing fears that the bank account details of several of UK dentists have been stolen.
- ProctorU, an online exam tool, has confirmed a data breach exposing private data of more than 400,000 accounts online. The tool is being used by educational institutes worldwide.
- A new credit card skimming campaign making use of homoglyph – domain lookalike – techniques has been connected to an existing Magecart threat group that utilizes the inter kit and favicon to hide skimming activity and lure a victim into purchasing on malicious websites.

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

VULNERABILITIES AND PATCHES

- Check Point Research has found 400 vulnerabilities , dubbed “Achilles”, in Qualcomm’s snapdragon mobile chipset. The vulnerabilities impact over 40% of all mobile devices globally including high-end phones from Google, Samsung, LG, Xiaomi, OnePlus and more. The vulnerabilities can allow an attacker to turn the device into a spying tool, or alternatively to render it constantly unresponsive, requiring factory reset.

  Check Point SandBlast Mobile provides protection against this threat

- Check Point Research has shared the details about vulnerabilities in Philips Hue IoT lightbulbs. By masquerading as a legitimate ZigBee lightbulb, researchers were able to infiltrate the IP network using a remote over-the-air ZigBee exploit.

  Check Point Cyber Security for IoT Networks and Devices provides protection against this threat

- Researchers have discovered tens of vulnerabilities in a Mercedes-Benz-E-Class, including issues that can be exploited to remotely hack the car.

- TeamViewer has fixed a vulnerability (CVE-2020-13699) that could allow an attacker to establish a quiet connection to a victim’s computer and execute code or obtain password hashes.

THREAT INTELLIGENCE REPORTS

- Check Point Research has launched an Anti-Debug Encyclopedia, describing anti-debug tricks which work on the latest Windows releases with the most popular debuggers (such as OllyDbg, WinDbg, x64dbg). The repository is implemented in a Check Point open-source project, and can help provide a better understanding of how anti-debugging techniques work or to assess debuggers and anti-debug plugins.

- Check Point Research has released a report showing that Google and Amazson were the brands most imitated in phishing attacks during Q2 2020. In phishing attacks on mobile devices, the top exploited brands are Facebook and WhatsApp.

- Sensitive data of more than 900 pulse secure VPN enterprise servers has been leaked on a Russian forum. The data contained a list of plaintext usernames and passwords, along with IP addresses, SSH keys, and more.

- New EtherOops attack is taking advantage of faulty Ethernet cables. The attack can be used to bypass network defenses and attack devices inside a closed enterprise network.