Check Point
SOFTWARE TECHNOLOGIES LTD.

Sep 14 - 20, 2020

YOUR CHECK POINT
THREAT INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- Check Point Research has unraveled an ongoing surveillance operation by Iranian entities that have been targeting Iranian expats and dissidents for years. The campaign targets both PCs and mobile devices, and is focused on stealing keys and data from social apps.

  Check Point SandBlast Mobile, SandBlast Network, SandBlast Agent and Anti-Bot provide protection against this threat (Trojan.WIN32.RampantKitten)

- A major hospital in Düsseldorf, Germany has been hit by a ransomware attack, as Düsseldorf University clinic's IT systems gradually crashed throughout a week. A woman who needed urgent admission died after she had to be taken to another city for treatment.

- Stolen Data of over 1,000 high-ranked Belarus police officers has been published by the Belarusian news agency, 'Nexta'. The data, collected and given to Nexta by a group of hackers in response to alleged violent police brutality against anti-government demonstrations, included names, dates of birth, and officers' department and job titles.

- Tutanota, a German provider of end-to-end encrypted email service, has suffered a series of Denial of Service (DDoS) attacks targeting its website and its DNS providers. The attack shut down the service for millions of users around the world for several hours.

- University hospital New Jersey (UHNJ) has been hit by a ransomware attack. SunCrypt ransomware operators leaked the data they had stolen, including a 1.7 GB archive containing over 48,000 documents from the institution.

- Quebec's Department of Justice has been hit by a cyber-attack, affecting 14 inboxes with Emotet malware. The attacks began on Aug 11, when email addresses were accessed and used to steal information and infect additional mailboxes.

  Check Point SandBlast and Anti-Bot provide protection against this threat (Trojan.WIN32.Emotet)

- IPG Photonics, a US developer of fiber lasers for cutting, welding, medical use, and laser weaponry, has suffered a ransomware attack that is disrupting their operations worldwide and affecting email, phones, and network connectivity in the offices.

VULNERABILITIES AND PATCHES

- The US Cybersecurity and Infrastructure Security Agency, CISA, has releases an emergency directive addressing a critical vulnerability in Microsoft Windows Net logon remote protocol (CVE-2020-1472).

  Check Point IPS blade provides protection against this threat (Microsoft Netlogon Elevation of Privilege (CVE-2020-1472))

- Apple has released updates for iOS and iPadOS operating systems that fix several security vulnerabilities on iPhone, iPad, and iPod devices.

- Researchers have found a vulnerability in the Firefox web browser on smartphones. The vulnerability can be exploited by attackers connected to the same Wi-Fi network and lead to remote command execution.

THREAT INTELLIGENCE REPORTS

- Check Point Research has published a report about an increase in the number of attacks targeting academic and research institutions globally, with the highest increase demonstrated in the US. On a similar note, the UK national cybersecurity center (NCSC) has issued an alert about a surge in ransomware attacks targeting education institutions, urging to follow the recommendations to mitigate the risk of exposures.

- Check Point Research has published a report about the different generation of a malware that serves for both crypto-mining and DDoS. The malware has versions for both Windows and Linux, and is currently attacking IoT devices by exploiting CVE-2018-10561, attacking unpatched Dasan GPON routers.

  Check Point IoT Protect, IPS, Anti-Bot and Anti-Virus provide protection against this threat (Dasan GPON Router Authentication Bypass (CVE-2018-10561) and others)

- A researcher has discovered how the Googles App Engine, a cloud-based service platform for developing and hosting web apps on Google's servers, can be abused to deliver phishing and malware.

- Nearly 2000 online stores running Magento e-commerce version that is past end-of-life have been hit as a part of one of the largest ever skimming campaign.

- The maze ransomware operation has been found to be evolving to launch a ransomware attack from within a virtual machine, adopting a tactic previously used by the Ragnar Locker gang.

  Check Point SandBlast provides protection against this threat