March 23 - 29, 2020

YOUR CHECK POINT
THREAT INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- Chubb, a major cybersecurity insurance provider for businesses hit by data breaches, has itself become a target of a data breach, after being hit by Maze ransomware. This case follows a December warning by the FBI of an increase of Maze ransomware attacks.

  Check Point SandBlast provides protection against this threat

- In Spain, the Android banking Trojan Ginp masquerades as a Coronavirus Finder app. After infection, a web page called "Coronavirus finder" shows the number of people infected around the victim's location, and urges them to pay a small sum to see their exact location, thus stealing credit card data.

  Check Point SandBlast Mobile provides protection against this threat

- Hackers hijack D-Link and Linksys routers' DNS to spread malicious COVID-19 Apps. The DNS rerouting results in opening a web page presumably from the World Health Organization (WHO), luring the victim to download malicious content.

- Finastra, a UK-based firm providing technologies to banks globally, has suffered a ransomware attack and was forced to shut down its servers.

- General Electric has suffered a data breach of private identifiable information of employees and beneficiaries including direct deposit forms, driver's licenses, passports, birth certificates, bank account numbers and more. The breach resulted from a breach in Canon, a GE service provider, in February.

- Ryuk Ransomware keeps targeting Hospitals, while other ransomware groups, including Maze and DoppelPaymer, have vowed not to attack the health industry.

  Check Point SandBlast and Anti-bot provide protection against this threat (Ransomware.Win32.Ryuk)

- University of Utah Health has suffered a breach to its systems, causing abuse of employees' email accounts that were used to send malicious phishing emails. Private data of patients such as names, dates of birth, medical record numbers and limited clinical information were also breached.

VULNERABILITIES AND PATCHES

- Microsoft has announced two zero-day flaws that could allow remote code execution, are being exploited in the wild, and are yet to be patched. The vulnerabilities relate to the Adobe Type Manager (ATM) library, which manages PostScript Type 1 fonts. The flaws can be exploited when the victim views the files in "preview mode" using Windows File Explorer, without even opening the malicious document.

  Check Point IPS blade provides protection against this threat (Adobe Type Manager Library Remote Code Execution)

- Adobe has released a patch for a critical vulnerability in its Creative Cloud desktop application. The vulnerability involved an abuse of the time-of-check time-of-use (TOCTOU) race condition that could be exploited to delete arbitrary files in the user's system.

- A critical bug (CVE-2020-10245) in CODESYS web server allows a remote attacker to crash a server or execute arbitrary code. The bug is a heap-based buffer overflow vulnerability, due to a faulty library that allows an attacker to request a vast amount of memory allocation, causing the overflow. CODESYS is mostly used for controller applications in industrial environments. A patch has been released, and is critical since this is an easily exploitable bug with a public PoC.

  Check Point IPS blade provides protection against this threat (CODESYS Web Server Buffer Overflow (CVE-2020-10245))

- 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 has discovered a new mobile malware family, dubbed 'Tekya', which hides itself in children's games and various utility apps, available to download on Google Play Store. The malware obfuscates native code to avoid detection by Google Play Protect and utilizes the 'MotionEvent' mechanism in Android (introduced in 2019) to imitate the user's actions and generate clicks.

  Check Point SandBlast provides protection against this threat

- Check Point Research has analyzed the mLNK builder, a tool specifically built to assist malware payloads to evade security solutions. The tool does so by converting payloads to LNK shortcuts. The analysis includes a technical breakdown, as well as a look at how the sellers of mLNK promote their product on more dubious parts of the web.

  Check Point SandBlast provides protection against this threat

- Russia has shut down a major credit card fraud ring. The Russian Federal Security Service (FSB) said 25 individuals were charged with circulating illegal means of payment in connection with some 90 websites that sold stolen credit card data.