Nov 1 – 7, 2021

YOUR CHECK POINT

THREAT INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- Check Point Research warns of scammers using Google Ads to steal crypto wallets, after seeing over $500k worth of cryptocurrency stolen from victims during one weekend. Scammers are placing ads at the top of Google Search that imitate popular wallet brands, such as Phantom and MetaMask, to trick users into giving up their wallet passphrase and private key.

- Check Point Research detected over 100 attacks in recent weeks using the new version of the banking Trojan Mekotio that targeted Latin America in the past, despite the arrests of people associated with its propagation. Security researchers report on its new, stealthier infection flow which starts with a phishing email containing a link to a zip file attachment.

  Check Point Threat Emulation provides protection against this threat *(Win.PSBypass.A; Wins.obfusBat.A)*

- Canadian provinces Newfoundland and Labrador health-care system has suffered a cyberattack, "the worst in Canadian History", which led to severe disruption to healthcare providers and hospitals.

- The UK Labour Party has disclosed that information concerning members, registered and affiliated supporters, was impacted in a data breach after a ransomware attack hit a third-party organization that was managing the party's data.

- CERT France has issued a warning concerning new ransomware group Lockean responsible for many attacks against French companies over the past two years, including pharmaceutical groups and newspapers.

- US defense contractor Electronic Warfare Associates (EWA) has confirmed they were victim of a data breach after threat actors launched a phishing campaign and hacked their email system. Hackers were able to exfiltrate files containing personal information.

- New threat actor "Tortilla", predominantly targeting US victims, has been hacking Microsoft Exchange servers and breaching corporate networks using the ProxyShell flaw to install the Babuk Ransomware.

  Check Point IPS, Harmony Endpoint and Threat Emulation provide protection against this threat *(Microsoft Exchange Server Remote Code Execution (CVE-2021-34473); HEUR:Trojan-Ransom.Linux.Babuk; Ransomware.Win.Babuk)*

VULNERABILITIES AND PATCHES

- Google has released the November 2021 Android security updates addressing 18 flaws in the framework and system components as well as 18 other vulnerabilities in the kernel and vendor components.
- Cisco has released security updates to address critical vulnerabilities in their products allowing unauthenticated hackers to log in using hard coded credentials or default SSH keys to take over vulnerable systems.
- Mozilla has released Thunderbird 91.3 patching several severe vulnerabilities to prevent attacks such as denial-of-service, spoof the origin, security policies bypass, and arbitrary code execution.
- The Philips TASY Electronic Medical Record used by hospitals as a medical record solution and healthcare management system, is vulnerable to two critical SQL injection vulnerabilities that may result in patient data exposure if exploited.
- A serious heap-overflow security flaw in the Transparent Inter Process Communication module of the Linux kernel tracked CVE-2021-43267 could allow local exploitation and remote code execution, leading to full system compromise.
- CISA has ordered US federal agencies to patch 276 vulnerabilities actively exploited from 2017 to 2021, posing a significant risk to government agencies.

THREAT INTELLIGENCE REPORTS

- The HelloKitty ransomware gang (aka FiveHands) has added distributed denial-of-service (DDoS) attacks to their extortion tactics.

  Check Point Harmony Endpoint provides protection against this threat

- Ransomware gangs are targeting companies involved in "significant financial events" such as corporate M&A.
- Cybercriminals are asking fraud schemes victims to use cryptocurrency ATMs and QR codes to facilitate payments.
- The BlackMatter ransomware group says it is shutting down due to pressure from the authorities and recent law enforcement operations. Following the news, their affiliates are transferring their victims to the competing LockBit ransomware site for continued extortion.

  Check Point Harmony Endpoint provides protection against this threat

- Researchers have found a new attack method called "Trojan Source" allowing vulnerabilities injection into the source code of a software project in a way that is very difficult to detect.
- The US government is offering a $10 million reward in exchange of information leading to the identification or arrest of members of the DarkSide ransomware gang and its rebrands.