Apr 18 – 24, 2022

Check Point Research

WEEKLY INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- Russian state-sponsored APT actor Gamaredon (aka Shuckworm) has targeted Ukrainian organizations using at least four different variants of the Pterodo backdoor, likely to maintain persistence on infected computers. The group has been performing cyber-espionage campaigns in Ukraine since at least 2014.

- Researchers have found a new spyware operation targeting at least 65 high profile victims in Catalonia (Spain), with 63 of them infected with the NSO's Pegasus spyware and a few with Candiru's. Targets included politicians, legislators and members of civil society organizations, sometimes including their family members. A newly undisclosed iOS zero-click vulnerability dubbed HOMAGE is at the source of these exploits.

- A malicious campaign is leveraging a fake Windows 11 upgrade through a website imitating Microsoft's promotional page to lure users. The file contains a new infostealer called "Inno Stealer", capable of collecting web browser cookies and stored credentials, data in crypto wallets and from the file system.

  Check Point Anti-Virus provides protection against this threat

- Microsoft Exchange servers vulnerable to the ProxyShell flaws have been attacked by Hive ransomware, using different backdoors, including Cobalt Strike. The attackers performed extensive discovery across the network before deploying the ransomware and encrypting files within the organization.

  Check Point Harmony Endpoint, Threat Emulation and IPS provide protection against these threats *(Ransomware.Win.Hive; Trojan.Win32.Cobalt Strike Beacon.TC; Microsoft Exchange Server Remote Code Execution (CVE-2021-34473); VER0 Microsoft Exchange Server Remote Code Execution (CVE-2021-34523); Microsoft Exchange Server Security Feature Authentication Bypass (CVE-2021-31207))*

- Docker servers are actively being targeted by the LemonDuck botnet to mine cryptocurrency on the Linux platform. The operation is ran anonymously through proxy pools hiding wallet addresses, and is evading detection by targeting Alibaba Cloud's monitoring service.

  Check Point Anti-Virus provides protection against this threat (Trojan.Win32.Lemonduck.TC)

- The FBI has issued a warning addressed to the Food and Agriculture (FA) organizations on the greater risks of ransomware attacks during the harvest and planting periods.

- CISA, the FBI and the US Treasury Department alert on the North Korean APT group Lazarus targeting companies in the blockchain and cryptocurrency sectors, using social engineering on employees.

  Check Point Threat Emulation provides protection against this threat (Backdoor.Wins.Lazarus)

VULNERABILITIES AND PATCHES

- Check Point Research identified “ALHACK”, a set of vulnerabilities in the ALAC audio format that could have been used for remote code execution on two-thirds of the world's mobile devices. The vulnerabilities affected Android smartphones powered by chips from MediaTek and Qualcomm, the two largest mobile chipset manufacturers.

  Check Point Harmony Mobile provides protection against this threat

- Check Point Research identified a vulnerability in the Everscale blockchain wallet. If exploited, the vulnerability would have given an attacker full control over a victim’s wallet and subsequent funds. The vulnerability was discovered in the web version of Everscale’s wallet, known as Ever Surf. Available on Google Play Store and Apple’s App Store, Ever Surf is a cross-platform messenger, blockchain browser, and crypto wallet for the Everscale blockchain network.

- Atlassian has issued an alert concerning Jira and Jira Service Management products vulnerable to a critical authentication bypass flaw in Seraph. Tracked CVE-2022-0540, it could let a remote hacker bypass authentication with an HTTP request.

- QNAP patched its network-attached storage firmware to address critical flaws: CVE-2022-22721, a buffer overflow, and CVE-2022-23943, an out-of-bounds write vulnerability in mod_sed of Apache HTTP Server.

- Lenovo has released an advisory on three flaws (CVE-2021-3970, CVE-2021-3971 & CVE-2021-3972) affecting its Unified Extensible Firmware Interface (UEFI).

THREAT INTELLIGENCE REPORTS

- Check Point Research has issued its Q1 2022 Brand Phishing Report, highlighting the brands that hackers most imitate: Social media platform LinkedIn was related to 52% of phishing attacks globally, taking the first place of the ranking. Shipping company DHL is now second with 14% of phishing attempts.

- The cybersecurity authorities of the US, Australia, Canada, New Zealand, and the UK have released a joint advisory to warn organizations that Russia backed groups could perform attacks on organizations both within and beyond the region of Ukraine. This could occur as a response to the economic costs imposed on Russia as well as materiel support provided by the US, its allies and partners.

- Following a period of several months of inactivity, the REvil Ransomware gang’s Tor leak site is now redirecting to a newly launched RaaS operation. While it is not clear who is behind the maneuver, the new site includes lists of REvil’s previous victims and new ones.

  Check Point Harmony Endpoint and Threat Emulation provide protection against this threat
  (Ransomware.Win.Revil.ja; Ransomware.Win32.REvil.TC; Trojan.Win32.Sodinokibi)