Check Point Research
WEEKLY INTELLIGENCE REPORT
June 27 – July 3, 2022

TOP ATTACKS AND BREACHES

- Iranian steel manufacturing plants have suffered a cyberattack which reportedly forced them to halt production. The hacker group Gonjeshke Darande, which has previously attacked the Iranian railway system, assumed responsibility for the attack. Check Point Research found and analyzed a malware sample used as part of this attack, connecting it to the tools used in previous attacks targeting Iran.
- Both Norway and Lithuania were victims of large-scale DDoS attacks in the past week. The attacks are assumed to have been carried out by separate pro-Russian hacker groups, with the goal of discouraging the nations' support of Ukraine.
- US book Publishing group Macmillan has shut down its IT systems after being hit by a cyberattack. According to Macmillan's spokesperson, the attackers encrypted files in the company's network, causing delays in orders, shipments and deliveries.
- Iranian-affiliated hacker group Sharp Boys has leaked personal and financial information of over 100,000 Israeli citizens. The information was obtained in a hack of multiple websites related to the Israeli tourism industry.
- US chipmaker giant AMD has had 450 GB of its data exfiltrated by "partners" of the hacker group RansomHouse. According to RansomHouse, they intend to sell the data to interested third parties rather than wait for AMD to pay the extortion fee.
- A report detailing the activity of the SessionManager IIS backdoor has been released. SessionManager is a malicious module for IIS, delivered via exploiting a ProxyLogon vulnerability in Exchange servers. According to the researchers, the backdoor has been used to spy on dozens of NGOs, government, military and industrial organizations.

  Check Point IPS and Anti-Virus provide protection against this threat *(Microsoft Exchange Server Remote Code Execution (CVE-2021-34473); Backdoor.Win32.SessionManager.TC.*, Backdoor.Win64.BadIIS.*)*

- Researchers have observed the usage of newly discovered vulnerabilities, as well as new features, in a cryptomining campaigns targeting Linux systems. The campaign now exploits vulnerabilities in Atlassian Confluence and Oracle WebLogic to gain access to Linux servers.

  Check Point IPS and Anti-Virus provide protection against this threat *(Atlassian Confluence Remote Code Execution (CVE-2022-26134), Oracle WebLogic Server Remote Code Execution (CVE-2019-2725))*

VULNERABILITIES AND PATCHES

- A critical vulnerability in Zoho ManageEngine ADAudit Plus has been discovered. The vulnerability allowed attackers to exploit a chain of flaws to enable remote code execution. ManageEngine has issued a security patch to cover this threat.

  Check Point IPS provides protection against this threat *(Zoho ManageEngine ADAudit Plus Remote Code Execution (CVE-2022-28219))*

- Jenkins has released a security advisory containing dozens of new vulnerabilities affecting many Jenkins deliverable plugins, only 4 of which have been patched.

- Mozilla has released version 102 of the Firefox browser. This version includes fixes for more than 20 security vulnerabilities.

THREAT INTELLIGENCE REPORTS

- As summer begins, Check Point Research warns of threat actors using travel-related lures in their phishing attacks.

- Ransomware-as-a-service group Lockbit has released version 3.0 of their ransomware. Among its new features is a bug bounty program, promising monetary rewards to those who can find security flaws in the group's ransomware.

  Check Point Harmony Endpoint and Threat Emulation provide protection against this threat *(Ransomware.Win.Lockbit)*

- Researchers have discovered a new malware that gains access to local area networks by targeting routers, dubbed ZuoRAT. ZuoRAT allows the attacker to enumerate the infected router, and perform man-in-the-middle attacks to download Trojans onto hosts within the router's LAN. Due to the malware's sophistication, the researchers suspect it was created by a state-level actor.

- A detailed timeline of the Android malware Flubot's activity has been published. While the complex Android malware's infrastructure was taken down in June 2022, the researchers believe it is likely to resurface once it can reestablish its C&C domains.

  Check Point Harmony Mobile provides protection against this threat

- An article detailing the threat of toll fraud Android malware has been published. This type of malware abuses a feature to stealthily subscribe to services that are directly added to the users' phone bill, thus avoiding the need for financial credentials.