August 14 – 20, 2023

Check Point Research

WEEKLY INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- The German Federal Bar (BRAK) Association, which oversees 28 regional bars throughout Germany and represents approximately 166,000 lawyers on a national and international scale, is currently investigating a ransomware attack on its Brussels office. NoEscape ransomware group claimed responsibility for this attack.

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

- Discord.io has confirmed that the company is handling a data breach exposing the information of 760,000 members, which led to the temporarily suspension of services. This comes after a cybercriminal going by the moniker Akihirah has posted the database of Discord in an underground forum.

- Colorado's Department of Health Care Policy and Financing (HCPF) has released a notice that personal health data of about 4 million members of state health programs from IBM-managed systems has been obtained in Cl0p ransomware group's third-party MOVEit attack during May 2023.

  Check Point IPS blade, Harmony Endpoint and Threat Emulation provide protection against this threat (Progress MOVEit Transfer Multiple Vulnerabilities; Webshell.Win.Moveit, Ransomware.Win.Clop, Ransomware_Linux_Clop; Exploit.Wins.MOVEit)

- Suspected North Korean hackers, thought to have ties to a North Korean entity Kimsuky group, have targeted a joint U.S.-South Korea military exercise. Reportedly, no classified information was stolen.

  Check Point Threat Emulation and Anti-Bot Blade provide protection against this threat (TrojanDownloader.Win.Kimsuky.A; Backdoor.WIN32.Kimsuky.A)

- Following a confidential data breach at Tesla, caused by two employees during May 2023 and affecting over 75K people, the company began notifying current and former employees that their information (Social Security numbers, names and addresses) has been exposed in the breach.

- Researchers have identified a widespread hacking campaign targeting LinkedIn accounts worldwide. They have noticed the attackers are using leaked credentials from 3rd party websites, or brute-forcing to gain control of as many LinkedIn accounts as possible, leading to many victims have losing access to their accounts, with some even forced to pay ransoms to regain control to their accounts.

- Researchers have found a large-scale phishing campaign aiming to harvest Zimbra credentials, targeting small and medium businesses and governmental entities worldwide. The largest number of campaign's victims are based in Poland, Ecuador, Mexico, Italy, and Russia.

VULNERABILITIES AND PATCHES

- Nearly 2,000 Citrix NetScaler servers have been compromised with a backdoor, leveraging the recently disclosed critical RCE vulnerability (CVE-2023-3519). This is part of a large-scale attack in which over 1,200 servers were backdoored before patch installation, and remain compromised without necessary checks for successful exploitation signs.

  Check Point IPS provides protection against this threat (Citrix NetScaler Remote Code Execution (CVE-2023-3519))

- CISA has issued a warning regarding the critical Citrix ShareFile secure file transfer vulnerability (CVE-2023-24489), noting threat actors are actively targeting it. The agency has also included this vulnerability in its list of known security flaws exploited in the wild.

  Check Point IPS provides protection against this threat (Citrix ShareFile StorageZones Controller Directory Traversal (CVE-2023-24489))

- Ivanti Avalanche, an enterprise mobility management solution, is affected by two critical buffer overflows collectively tracked as CVE-2023-32560. With a CVSS v3 rating of 9.8, the flaws can be exploited remotely without user authentication.

THREAT INTELLIGENCE REPORTS

- Check Point researchers discuss the security challenges faced by web server management and describe Turnstile - an alternative to CAPTCHA that offers a user-friendly approach to differentiate between human users and bots. The article warns that the same mechanisms that make Turnstile user-friendly also present a potential risk if exploited by malicious actors.

  Check Point's Zero Phishing AI provides protection against this threat.

- Trend Micro has analyzed the return of the Monti ransomware group after a two-month break, while the group is targeting now legal and government organizations. At the same time, the company has observed a new Linux-based variant, showing notable differences from previous Linux-based versions.

  Check Point Harmony Endpoint and Threat Emulation provide protection against this threat.

- Several U.S. intelligence agencies have issued warnings about a rising trend of cyberattacks directed at American space firms by undisclosed foreign intelligence entities. These attacks primarily aim to gain proprietary data and have also been associated with instances of intellectual property misuse.

- Researchers report on a Chinese APT group (possibly Bronze Starlight) targeting gambling institutions in Southeast Asia. The group uses DLL sideloading to deliver malicious payloads in order to steal sensitive information from victims' networks.