Check Point
SOFTWARE TECHNOLOGIES LTD.

Oct 4 – 10, 2021

YOUR CHECK POINT

THREAT INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- UK newspaper & Media outlet The Telegraph has accidently leaked 10 TB of subscribers’ data after leaving an Elasticsearch cluster unsecured. Leakage includes internal logs, names, emails, device type, URL requests, IP addresses, authentication tokens & unique reader identifiers.
- Twitch source code and users' sensitive data have been leaked on anonymous website 4chan: A threat actor shared a torrent link directing to a 125GB archive comprising of data stolen from 6000 internal Twitch Git repositories. Following the breach, Twitch was defaced with a close-up portrait of Jeff Bezos.
- Security experts have discovered a new Iranian threat actor, MalKamak, which has been running cyber espionage campaigns since at least 2018. This APT group seems to focus their operations in the Middle East, the US, Russia and Europe with a new Remote Access Trojan (RAT) dubbed ShellClient.
- Google has released a warning to 14,000 of its users about being targets of a phishing campaign from Russian state-sponsored group APT28, aka Fancy Bear, which has been responsible for very high profile attacks in recent years.
- Atom Silo, a new ransomware operator, is targeting a recently patched and actively exploited Atlassian Confluence Server & Data Center vulnerability (CVE-2021-26084) to deploy their ransomware payloads.
- Syniverse, a service provider for large telecommunications companies like AT&T, T-Mobile, Verizon and Vodafone, revealed that threat actors have been hacking into its databases for years and compromised login credentials belonging to more than 200 customers, potentially exposing millions of users.
- Unknown ransomware gang is using a Python script to encrypt virtual machines on VMware ESXi server: Attackers broke into a TeamViewer account and encrypted a victim's virtual machines running on a vulnerable ESXi hypervisor three hours following the initial breach.

VULNERABILITIES AND PATCHES

- Google has issued October's Android security updates, fixing 41 high to critical severity flaws, including a set for the vulnerabilities tracked CVE-2021-0870, CVE-2020-11264, and CVE-2020-11301.
- The Apache Software Foundation urges to update to version 2.4.51 of the HTTP Web Server to address two zero day vulnerabilities, which could allow remote code execution: CVE-2021-41773 & CVE-2021-42013 can lead threat actors to map URLs to files outside the expected document root by launching a path traversal attack.

  Check Point IPS provides protection against this threat (Apache HTTP Server Directory Traversal (CVE-2021-41773))
- Dahua cameras are vulnerable to authentication bypass flaws tracked as CVE-2021-33044 and CVE-2021-33045, and if unpatched are both remotely exploitable during the login process by sending specially crafted data packets to the target device.
- Medtronic is urgently recalling the MiniMed remote controllers for insulin pumps exposed to security vulnerabilities. The devices sold in the US allow users to communicate with the pump remotely to deliver a specific dosage of insulin.
- Microsoft has fixed a bug blocking Azure Virtual Desktop (AVD) devices from downloading and installing monthly updates via Windows Server Update Services (WSUS). The problem affected both client (Windows 10 Enterprise multi-session, version 1909) and server (Windows Server multi-session, version 1909) platforms.

THREAT INTELLIGENCE REPORTS

- Check Point Research reports 40% increase in weekly cyberattacks on organizations in 2021 compared to 2020 with Education/Research again as the most targeted Industry.
- Check Point Research reports that Trickbot has returned as the most prevalent malware in September 2021, while the Remote Access Trojan njRAT has entered the index for the first time and Phorpiex dropped from the list since it is no longer active.

  Check Point Threat Emulation and Anti-Bot provide protection against this threat (Trojan-Banker.Win32.Trickbot)
- Security researchers report that 58% of the past year's nation-state cyber-attacks originated from Russian actors, primarily targeting government agencies from the United States, Ukraine and UK for intelligence gathering purposes.
- Researchers have uncovered a new UEFI bootkit capable to backdoor Windows devices and remain persistent on the EFI System Partition by installing a malicious Boot Manager.
- Researchers have found a previously undetected Linux malware family named FontOnLake.

  Check Point Anti-Virus provides protection against this threat