July 26 – August 01, 2021

YOUR CHECK POINT

THREAT INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- The company that manages COVID-19 vaccination appointments in the Lazio Region in Italy has been hit by ransomware. The attack took down its IT systems, making the booking site unreachable and suspending the vaccination of the entire region surrounding Rome.

  Check Point Harmony Endpoint provides protection against this threat

- Threat actors have been using Google ads to promote a website that impersonated the official website for the Brave browser. When visitors try to download the browser from the fake website, it actually downloads remote access malware known as ArechClient or SectopRat.

  Check Point Zero-Phishing provides protection against this threat (Backdoor.SectopRat)

- Experts have spotted a previously undocumented Chinese-speaking threat actor tracked as GhostEmperor using a new PlugX variant in an ongoing attack targeting Microsoft Exchange flaws on high-profile victims, mainly South Asian entities and governments.

  Check Point Anti-Bot provides protection against this threat (Trojan.Win32.Plugx)

- A new file wiping malware traced as "Meteor" has been found used in the recent attack against Iran's railway system. "Meteor" is a wiping malware that intentionally deletes files on a computer and causes the system to become unbootable.

- New camping named "BazaCall" has been spotted using fake call centers for tricking victims into downloading malware, performing data exfiltration, and deploying ransomware on affected machines.

- Video game company Electronic Arts (EA) has suffered a data breach after refusing to pay ransom following an attack in June. The data published by the threat actors includes the source code for the FIFA 21 soccer game and the Frostbite game engine.

- The US Department of Justice has disclosed that the Microsoft Office 365 email accounts of employees at 27 US Attorneys' offices were breached by the Russian Foreign Intelligence Service (SVR) during the SolarWinds global hacking spree.

VULNERABILITIES AND PATCHES

- Zero-day flaws in Kaseya's cloud-based enterprise solution can be exploited for remote code execution and privilege escalation on client-side. Users are warned to avoid exposing the service to the internet.
- Flaws in Zimbra's email collaboration software could allow attackers to compromise email accounts and cloud secrets by sending a malicious email containing a JavaScript payload.
- Apple has released a security update to address a vulnerability in macOS and iOS that may have already been exploited to deliver malware (CVE-2021-30807).
- Researchers have disclosed details about a recently patched critical flaw in Microsoft Hyper-V (CVE-2021-28476) that can trigger a DoS condition and remote code execution.
- Node.JS has released an update for the use-after-free sever HTTP vulnerability (CVE-2021-22930) that could be exploited to corrupt the process and cause application crash and potentially remote code execution.

THREAT INTELLIGENCE REPORTS

- Check Point Research has released its 2021 mid-year security report, highlighting the threat trends in the first half of this year, including the global 29% increase in cyber-attacks, 93% surge in ransomware attacks fueled by the Triple Extortion technique, and rise in supply chain attacks.
- Check Point Research has analyzed an XLoader variant for macOS, similar to the Formbook malware, including its anti-analysis tricks, encryption, network communication, and supported commands.

  Check Point Threat Emulation, Anti-Bot and Anti-Virus provide protection against these threats (Trojan.WIN32.Formbook; InfoStealer.Win.Formbook; Banking.Win32.Formbook; Trojan.Mac.XLoader)

- Researches have spotted a new strain of Android banking Trojan Vultur, which uses screen recording and keylogging for the capturing of login credentials.

  Check Point Harmony Mobile provides protection against this threat

- A new variant of the LockBit 2.0 ransomware has been found with an ability to use Windows Active Directory group policies to disable Windows Defender security features and launch the ransomware executable across an entire network.

  Check Point Harmony Endpoint provides protection against this threat (Ransomware.Win32.LockBit)

- Experts have released a decryptor and file recovery tool for "Prometheus" ransomware, brute-forcing encryption keys. Since its release two weeks ago, the ransomware group hasn't published new data on its dark web leak site, potentially seizing operation.

  Check Point Harmony Endpoint provides protection against this threat