May 4 - 10, 2020

Check Point
SOFTWARE TECHNOLOGIES LTD.

YOUR CHECK POINT THREAT INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- Check Point Research have discovered an ongoing cyber espionage operation against government entities in the Asia Pacific (APAC) region. The operation is attributed to the Naikon APT group, using a backdoor dubbed Aria-body to take control of the victims' networks. One of the attack vectors was infecting a foreign embassy as a launching pad to propagate the attack to government entities via malicious emails.

  Check Point SandBlast and Anti-bot provide protection against this threat

- Fresenius, Europe's largest private hospital operator, has suffered a ransomware attack. The apparent culprit is Snake ransomware, known for targeting IT processes tied to enterprise management tools and large-scale industrial control systems (ICS), such as production and manufacturing networks.

  Check Point SandBlast and Anti-bot provide protection against this threat (Ransomware.Win32.Snake)

- Unacademy, an India-based online learning platform, has suffered a major data breach that exposed details of 22 million users. The compromised information included usernames, hashed passwords, first and last names, and other account profile details, and was offered for $2,000 on darknet forums.

- Grubman Shire Meiselas & Sacks, an NYC law firm that serves major stage and screen stars, is being ransomed by REvil ransomware. The firm's portfolio stretches from companies Facebook, Sony and HBO, to stars like LeBron James, Robert DeNiro, Elton John and Madonna. The attackers claim to hold 756GB of contracts, telephone numbers, email addresses, personal correspondence, and NDAs.

  Check Point SandBlast and Anti-bot provide protection against this threat (Ransomware.Win32.REvil)

- Logistics giant Toll Group has been hit by ransomware twice in three months – first by MailTo, then by Nefilim. The Australia-based logistic group has had to suspend IT systems due to the attacks.

  Check Point SandBlast and Anti-bot provide protection against this threat (Ransomware.Win32.Mailto)

- UK's National Cyber Security Centre (NCSC) is warning of targeted cyber attacks against UK universities and scientific institutes involved in COVID-19 research.

VULNERABILITIES AND PATCHES

- Samsung has revealed a “zero-click” vulnerability that allowed remote code execution on every Galaxy smartphone from 2014 onwards. The vulnerability (CVE-2020-8899) has a 10 out of 10 severity score and has been patched in Samsung’s May 2020 security update. It stems from the way Samsung Android OS handles .qmg images sent to the device, which can be processed as thumbnails images – effectively allowing a single MMS message to allow a complete takeover of the device.

- Google has fixed a critical bug in Android (CVE-2020-0103) that allowed attackers to deploy a complete remote control access attack on a targeted device. The attack could allow attackers to completely take over someone’s device to install programs, steal or change data, or create new accounts with full privileges. It was among 38 other flaws patched by Google in this batch.

- Cisco has fixed 12 high-severity flaws in its Adaptive Security Appliance software and Firepower Threat Defense software. The flaws could lead to a variety of attacks – from denial of service to data leaks.

- A recently patched Oracle WebLogic Server remote code execution vulnerability has been exploited in the wild.
  Check Point IPS provides protection against this threat (Oracle Fusion Middleware WebLogic Server Insecure Deserialization (CVE-2020-2883))

- Attackers have been exploiting SaltStack flaws to gain access to core systems at the Android-based LineageOS project and the Ghost open source blogging platform.

  Check Point IPS provides protection against this threat (Saltstack Salt Authentication Bypass (CVE-2020-11651))

- A researcher has published a PoC for the recently discovered vulnerability on OpenSSL 1.1.1d-1.1.1f (CVE-2020-1967). The issue, that can occur during or after a TLS 1.3 handshake, can lead to a denial of service attack, and has been fixed in OpenSSL 1.1.1g.

THREAT INTELLIGENCE REPORTS

- Check Point Research have demonstrated how fuzzing the Windows kernel using research tools can expose security vulnerabilities – leading to the publication of 8 new vulnerabilities and a number of bugs.

- Nazar, a previously misidentified and unknown threat group, has recently come to light after a thorough analysis of the last leak by the Shadow Brokers. Check Point Research delve deeper into its execution flow.

- A new ransomware codenamed “ColdLock” has targeted several organizations in Taiwan. It has similarities to Lockergoga, Freezing, and EDA2. The ransomware, deployed as .dll file, appears to have so far being targeted at specific companies.

  Check Point SandBlast and Anti-bot provide protection against this threat (Ransomware.Win32.Coldlock.TC)