Check Point
SOFTWARE TECHNOLOGIES LTD.

Feb 7 – 13, 2022

YOUR CHECK POINT

THREAT INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- APT group called “ModifiedElephant” has been operating since 2012, targeting human rights activists, academics and lawyers in India with the goal of planting incriminating digital evidences using spear phishing methods.
- Researchers have discovered that North Korean APT group Kimsuky has been active in campaigns involving commodity open-source remote access tools dropped with their custom backdoor, Gold Dragon. Their latest campaign is primarily focused on South Korean targets.
- The Palestinian APT group Molerats (aka TA402) has been spotted using a new intelligence gathering Trojan called “NimbleMamba” in a cyber-espionage phishing campaign leveraging geofencing and URL redirects to legitimate websites in the Middle-East and North Africa.
- Data of 6,632 employees of the German sportswear company Puma has been breached, after a ransomware attack hit Kronos, their HR management service providers, in December 2021.
- The financially motivated “Roaming Mantis” SMS phishing campaign is targeting German and French Android and iPhone users with malicious applications and phishing pages.
- Over 500 e-commerce stores using the Magento 1 platform have been hit by a massive breach involving a payment skimmer loaded from the naturalfreshmall.com domain. Hackers associated an SQL injection and PHP object injection to gain control of the Magento stores.
- 200,000 people have been impacted by a data breach that exposed personal information of users of Croatian phone carrier A1 Hrvatska.
- Iranian APT34 group (aka OilRig) has implemented a new backdoor called ‘Marlin’, with most victims located in Israel, Tunisia and UAE, from the diplomatic, technological and medical sectors.

  Check Point Threat Emulation provides protection against this threat

VULNERABILITIES AND PATCHES

- Apple has released a patch for a new zero-day flaw leveraged by threat actors on iPhones, iPads, and Macs. Tracked as CVE-2022-22620, the vulnerability is a Use-After-Free issue in Webkit browser, which could lead to unexpected OS crashes and arbitrary code execution on vulnerable devices.
- Thousands of WordPress websites are vulnerable to critical remote code execution flaws in open-source plugin PHP Everywhere that could allow low privileged users to execute code on compromised website.
- Mozilla has fixed a high severity privilege escalation vulnerability in Mozilla Maintenance Service, after Firefox 97 release, allowing hackers to escalate their privileges to NT AUTHORITY\SYSTEM rights.
- Google has released Android security updates for two critical vulnerabilities, the first is a critical remote escalation of privilege tracked as CVE-2021-39675 on Android 12, and the second, CVE-2021-30317, affects a closed-source component of Qualcomm on Android devices using Qualcomm's hardware.

THREAT INTELLIGENCE REPORTS

- Microsoft has announced that the Office VBA macro feature, exploited in numerous cyberattacks, will soon be blocked by default. Check Point Research analyzed the history of this threat.

  Check Point Threat Emulation and Threat Extraction provide protection against this threat

- Check Point Research has revealed new techniques that can be used by malware to evade sandbox detection.

  Check Point Threat Emulation provides protection against this threat

- Check Point Research has found that the LokiBot InfoStealer is back in the list of most prevalent malware while Emotet has replaced TrickBot at the top. Apache Log4j is still the most exploited vulnerability.

  Check Point Harmony Endpoint and IPS provide protection against these threats

- Check Point Research has observed an increase in malicious phishing email campaigns with Valentine's Day as their theme, with a 152% increase in new Valentine's Day domains registered in January.
- The Medusa Android banking Trojan has been pairing with FluBot Android spyware's distribution network in high-volume campaigns, using the same smishing infrastructure.

  Check Point Harmony Mobile provides protection against this threat

- Threat actors have started a campaign using fake Windows 11 upgrade installers to users of Windows 10, where victims are lured into downloading and executing the RedLine password stealing malware.

  Check Point Anti-Virus provide protection against this threat *(Trojan.Win32.Redlinestealer)*