Check Point SOFTWARE TECHNOLOGIES LTD.

Jan 24 – 30, 2022

YOUR CHECK POINT

THREAT INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- Hacktivist group from Belarus called “Belarusian Cyber Partisans” has breached the computers systems of Belarusian Railways. Threat actors claim to have encrypted the network and are extorting the Belarusian government, asking for the release of 50 political prisoners and a pledge from Belarussian Railways to halt transport of Russian soldiers as Russia prepares for a possible invasion of Ukraine.
- The Canadian ministry of foreign affairs has been hacked, resulting in the interruption of some of its internet-based services. There is currently no indication that additional departments were impacted.
- NSO’s Pegasus spyware has been leveraged to spy on Finnish Diplomats’ phones while on their diplomatic missions overseas.
- Delta Electronics, a Taiwanese Apple and Tesla contractor, has been hit by a Conti Ransomware attack. The company stated that only non-critical systems were compromised. Ransomware operators demanded a $15 million ransom payment in exchange for the decryption key.

  Check Point Harmony Endpoint provides protection against this threat (Ransomware.Win32.Conti)
- The Nobel Foundation has disclosed a cyber-attack that took place during the award ceremony in December 2021; the institution’s website was hit by a distributed denial of service (DDoS) attack.
- Hackers have stolen $80 million worth of crypto assets from the DeFi finance platform Qubit Finance. Threat actors then contacted the company and proposed to return the stolen amount in exchange for the maximum bug bounty.
- Russian state-sponsored cyberespionage group APT29 (aka CozyBear) has established persistence in the networks of several organizations using a variant of the “GoldMax” backdoor for Linux and new stealthy malware called “TrailBlazer”.
- In a new phishing campaign, attackers gain users’ corporate credentials, then use them to send internal phishing emails and outbound spam.

VULNERABILITIES AND PATCHES

- An unauthenticated stack-based buffer overflow flaw (CVE-2021-20038) impacting SMA 100 series appliances in SonicWall Secure Mobile Access gateways is actively being exploited by threat actors. The vulnerability could enable remote unauthenticated hackers to execute code in SonicWall appliances.
- VMware Horizon has released patches addressing Log4j vulnerabilities and is urging users to update exposed servers which are currently targeted in attacks. These campaigns have been linked with the "Prophet Spider" initial access broker group.

  Check Point IPS provides protection against this threat *(Apache Log4j Remote Code Execution (CVE-2021-44228))*
- Apple has released iOS 15.3 and macOS Monterey 12.2 updates to patch CVE-2022-22587, a zero day vulnerability actively exploited in the wild that could be leveraged by a malicious application to execute arbitrary code with kernel privileges.
- Exploits have publically been disclosed for the Microsoft vulnerability CVE-2022-21882, a local privilege escalation bug in Windows 10 system patched earlier this month.

  Check Point IPS provides protection against this threat *(Microsoft Windows Win32k Elevation of Privilege (CVE-2022-21882))*

THREAT INTELLIGENCE REPORTS

- Check Point Research has released its annual security report, revealing the key attack vectors and techniques used by threat actors during 2021. The report includes top leveraged malware and vulnerabilities, some of the key attacks, and explores cyberattack trends including the disruption to individuals' day-to-day lives, supply-chain attacks and risks, and the cracks we start identifying in the ransomware ecosystem.
- Check Point Research has revealed how hackers created new fraudulent tokens to lure victims into buying the tokens, and then 'rug pulling' all the money from smart contracts using misconfiguration in smart contract's functions to steal funds.
- The Taiwanese hardware vendor QNAP has advised users to secure network-attached storage (NAS) appliances and routers against a new ransomware gang "DeadBolt".
- North Korean APT group Lazarus is using the Windows Update client as a living-off-the-land tool, to run malicious code on Windows in an email phishing campaign masquerading as job offers.

  Check Point Threat Emulation and Harmony Endpoint provide protection against this threat *(APT.Win.Lazarus)*
- New MacOS cyberespionage malware dubbed "DazzleSpy" is being leveraged in Watering-Hole attacks. The backdoor is delivered via a Safari exploit, targeting politically active Hong Kong residents.