Jul 12 - 18, 2021

Check Point
SOFTWARE TECHNOLOGIES LTD.

YOUR CHECK POINT

THREAT INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- An ongoing Chinese APT espionage campaign tracked as “LuminousMoth” has been targeting entities from Southeast Asia including Mongolia, Myanmar and the Philippines.
- Ecuador’s state-run national telecommunication corporation (CNT) has been hit by RansomEXX ransomware. The attack caused havoc in the business operations, the payment gateways, and the company’s customer support portal, and exposed hundreds of GB of data.

  Check Point Harmony Endpoint provides protection against this threat
- SonicWall and CISA have released a warning about threat actors targeting a known, previously patched, vulnerability found in SonicWall secure mobile access (SMA) and secure remote access (SRA) products with end-of-life firmware. This vulnerability has been exploited by the “HelloKitty” ransomware, among others.

  Check Point Harmony Endpoint provides protection against this threat
- Testcoronanu, a Covid testing company, has suffered a leak that made it possible to fake Covid Vaccination cards or test results in CoronaCheck application.
- Researchers have discovered a misconfigured Amazon S3 bucket belonging to an online art retail service, Artwork Archive. The data was left exposed unencrypted and without any password creating a data breach that affected around 7,000 costumers including galleries’ artists and collectors.
- Comparis.CH, a Swiss based website with 80 million visits a year, has been hit by a ransomware attack demanding 400,000 dollars in cryptocurrency. The attack shut down the site operation for 3 days and had access to certain internal costumer data.
- The Joker premium billing-fraud malware has been spotted back on Google Play with some new evasion techniques.

  Check Point Harmony Mobile provides protection against this threat

VULNERABILITIES AND PATCHES

- Google has issued multiple security updates including a patch for a zero-day (CVE-2021-30563) bug in Chrome browser already exploited in the wild.
- Yet another vulnerability in Windows Print Spooler service has been published. Tracked as CVE-2021-34481, this is a privilege elevation vulnerability, and the only current "patch" is disabling the Print Spooler service.
- Instagram has introduced a new security feature dubbed "Security Checkup". The new feature will help users recover their compromised accounts that have been taken over by bad actors.
- Network equipment vendor D-Link has released a firmware hotfix to fix multiple vulnerabilities in the DIR-3040 AC3000-based wireless internet router, which could allow attackers to execute code, steal information or crash the device.
- Cisco has addressed a high severity denial of service (DoS) vulnerability in the Adaptive Security Appliance (ASA) and Firepower Threat Defense (FTD) software.

THREAT INTELLIGENCE REPORTS

- Check Point Research have reported on the most prevalent malware for June 2021, and the most imitated brands in phishing attacks in Q2. Interestingly, the top of both lists is consistent with previous reports – Trickbot is the leading malware for the second month in a row, and Microsoft has been the leading brand all year long.

  Check Point Harmony Email provides protection against these threats

- Israeli offensive cyber firm Candiru, tracked as Sourgum, has exploited multiple Windows zero-day vulnerabilities to deliver a new spyware dubbed DevilsTongue. At least 100 activists, journalists, and government dissidents across 10 countries were targeted with the spyware.
- Researchers have identified a new functionality in Trickbot. The Russia-based botnet is now using a virtual network computing (VNC) module, which mirrors the victim's desktop through a virtual desktop. It helps in stealing data, but also in identifying the victim and its critical assets.

  Check Point Threat Emulation and Anti-Bot blade provide protection against this threat (Trojan-Banker.Win32.Trickbot)

- HelloKitty ransomware has had a Linux variant targeting VMware ESXI servers and virtual machines running on them since at least the attack on the Polish gaming company CD Project Red in March 2021.

  Check Point Harmony Endpoint provides protection against this threat

- New analysis of the macOS malware threat landscape suggests that Shlayer and Bundlore are the most prevalent malware.