Check Point
SOFTWARE TECHNOLOGIES LTD.

Jun 14 - 20, 2021

YOUR CHECK POINT

THREAT INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- South Korea's Korea Atomic Energy Research Institute (KAERI) disclosed a breach in their internal network caused by a VPN vulnerability. The state-run nuclear institute's network was attacked last month by what appears to be a North Korean threat actor.
- Researchers have identified LastConn, a malware distributed by TA402 also known as MoleRAT, targeting government institutions in the Middle East as well as global government associated with geopolitics in the region. Malicious emails included a malware-laced PDF claiming to be a report on Hamas meetings with the Syrian government.

  Check Point SandBlast provides protection against this threat (Phishing.Win32.Molerats)
- Wegmans, a US-based supermarket chain, has suffered a data breach exposing customers' information online as a result of online availability of two of its databases due to a misconfiguration issue.
- Carnival Corporation, the world's largest cruise ship operator, has disclosed a data breach after attackers gained access to its IT systems exposing personal, financial, and health information belonging to customers, employees, and crew.
- A nameless malware has stolen over 26 million login credentials holding 1.1 million unique email addresses, 2 billion cookies, and 6.6 million files from Windows-based computers globally, and took photos of the victims through the webcam. Infection vectors included malicious emails and cracked software such as Adobe Photoshop.
- Iran-linked Ferocious Kitten APT group has been using instant messaging apps and VPN software like Telegram and Psiphon to deliver Windows RAT and spy on targeted victims.
- Researchers have found fake DarkSide ransomware demanding 100 BTC from companies. After the original DarkSide gang had quit its operation last mount a new threat actor has been delivering look-alike emails to companies claiming to have stolen sensitive information and demanding ransomware.

VULNERABILITIES AND PATCHES

- Google has released a security update for Chrome including four security fixes for the latest 0-day vulnerabilities (CVE-2021-30554 – CVE-2021-30557).
- Multiple flaws have been discovered in smart switches of Cisco's Small Business 220 series. The vulnerabilities impact devices running an old version framework with the web-based management interface enabled. (CVE-2021-1541 – CVE-2021-1543, CVE-2021-1571).
- A bug has been found in the Microsoft Teams chat service. The vulnerability can allow a threat actor to gain Read/Write privilege for a victim user's emails, team chats, OneDrive, SharePoint, and more services.
- A vulnerability found in ThroughTex's P2P SDK exposes millions of internet-connected cameras to espionage. The flaw is in a function that allows remote access to audio/video streams over the internet.
- Instagram has addressed a new flaw that allowed access to view archived posts and stories in private accounts without having to follow them.
- Apple has issued two out-of-band security fixes for its Safari web browser, fixing a zero-day vulnerability that was actively exploited in the wild (CVE-2021-30761, CVE-2021-30762).

THREAT INTELLIGENCE REPORTS

- Check Point Research has analyzed a surge in malicious activity in the run-up to Amazon Prime Day 2021, where nearly 80% of domains containing the word "Amazon" are potentially dangerous. Cybercriminals are impersonating the Amazon brand ahead of the annual shopping event in order to trick consumers into credential theft of their email addresses, payment details and passwords, and more.
- Threat actors have been abusing Google Drive and Docs to bypass security filters and exploit them in a new phishing campaign meant to steal credentials and deliver malware through fake Google login web pages.

  Check Point Harmony mail, sandblast and anti-Phishing blade provide protection against this threat.
- Threat actors are exploiting a recently patched 0-day vulnerability in Google Chrome, in the web graphics library JavaScript API that is used to render interactive 2D/3D without the use of a plugin (CVE-2021-30554).
- An unusual new malware blocks victims from visiting illegal download sites. The malware blocks users' ability to visit websites dedicated to software piracy by modifying the host file on the infected system.
- The Tinder dating application is the latest platform to be abused in a spam campaign with hidden "handwritten" links in fake profile images.
- Researchers have disclosed a new evasion technique dubbed "Process Ghosting" that could potentially be abused by threat actors to circumvent protections and stealthily run malicious code on Windows systems.