July 02 – 08, 2018

Check Point
SOFTWARE TECHNOLOGIES LTD.

YOUR CHECK POINT THREAT INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- Check Point security researches have revealed the comeback of an APT campaign against institutions in the Palestinian Authority. Dubbed 'Big Bang', the campaign uses phishing emails with an attached self-extracting archive containing a malicious executable and a Word file. The document serves as a decoy, while the malware is installed in the background.

  Check point SandBlast provides protection against this threat

- Iranian 'Charming Kitten' APT group has attempted to pose as the Israeli cyber-security firm "ClearSky", by creating a rogue copy of its website. The fake website included "sign in" options for credential theft.

- Hamas cyber-operatives have lured Israel Defense Forces (IDF) soldiers into downloading malicious Apps onto their mobile devices, using fake women's Facebook profiles. The apps, disguised as World Cup and dating apps, are capable of taking control over the infected device, exfiltrating sensitive data out of it, capturing the user's GPS location, and more.

  Check point SandBlast Mobile provides protection against this threat

- Tens of thousands of 'Fortnite' gamers have been infected with a malware injecting fraudulent ads into every website they visit. The adware disguised as a Fortnite hack tools and installed a root certificate on infected computers, allowing attackers to modify all network traffic using a man-in-the-middle attack.

- A former employee of the Israeli security company "NSO" has attempted to sell mobile hacking tools on the dark web for $50 Million. The stolen source code called 'Pegasus' is a powerful spyware allowing remote attackers to access sensitive information from the infected device, including text messages, calendar entries, emails, WhatsApp messages, user's location, microphone and camera, and more.

- Samsung devices including Galaxy S9 and S9+ have been found to randomly be sending photos taken with the camera to contacts in the address book without the user's consent. The unwanted messages were sent via the Samsung Messages App but with no record of the sending.

VULNERABILITIES AND PATCHES

- The release of a new Chrome version has brought back an old bug in the browser, Download Bomb, which involves initiating hundreds or thousands of downloads to freeze a browser on a specific page. This enables different attacks, mainly tech scams, to trap users on malicious web pages.

  Check point IPS blade provides protection against this threat (Multiple Browsers Download Bomb Trick)

- A new version of the popular email client 'Thunderbird' has been released. The new version addresses many security vulnerabilities including EFAIL encryption issues that can be exploited by threat actors to leak S/MIME plaintext when a message is forwarded and to build S/MIME and PGP decryption in HTML messages.

  Check point IPS blade provides protection against this threat (ROBOT TLS_RSA Scanning Attempt)

- The ISP Advanced Digital Broadcast (ADB) has released security patches addressing three critical vulnerabilities affecting broadband routers. The vulnerabilities are a privilege escalation bug, an authorization bypass issue, and a local jailbreak bug.

THREAT INTELLIGENCE REPORTS

- Security researches have revealed a new technique leveraging the CoinHive "URL shortener" service to mine Monero cryptocurrency instead of injecting the infamous CoinHive JavaScript. Threat actors are abusing this service that allows creating a short link for any URL with a delay, so it can mine Monero for an interval of time before redirecting the user to the original URL.

  Check point IPS, Anti-Bot and Anti-Virus blades provide protection against this threat (Multiple Websites Mine Cryptocurrencies CPU Hijacking; Trojan.WIN32.CoinHive; Trojan.Win32. CoinHiveMiner)

- Security researchers have discovered a new variant of 'Rakhni' Ransomware with crypto-mining abilities, capable of deciding whether the final infection payload will be crypto-miner or Ransomware, depending on the existence of a 'Bitcoin' folder in the AppData section.

  Check point Anti-Bot and Anti-Virus blades provide protection against this threat (Trojan- downloader.Win32. Rakhni)

- Version 4 of the GandCrab Ransomware has been spotted in the wild. The changes in the malware include different encryption algorithms, a new '.KRAB' extension, a new ransom note name, and a new TOR payment site.

  Check point SandBlast provides protection against this threat

- The IoT botnet dubbed Hide 'N Seek (HNS) discovered earlier this year has been observed evolving to also target cross-platform database solutions.

  Check point IPS blade provides protection against this threat (Netgear DGN Unauthenticated Command Execution)