Check Point
SOFTWARE TECHNOLOGIES LTD.

May 18 - 24, 2020

YOUR CHECK POINT THREAT INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- Thousands of Israeli websites have been defaced in an Anti-Israeli Campaign carried out by the “Hacker of Savior” group. All websites were hosted on a local Israeli hosting company called uPress, and the attackers centrally exploited a vulnerability in a WordPress plugin to publish an anti-Israeli message on the websites’ homepages with an embedded link to attempt to get webcam access.
- Check Point Research has identified a phishing document impersonating the IRS 1040 form, one of the official documents that US taxpayers use to file their annual income tax return. Uploaded to Google Drive, the PDF document was called “2018 1040 Tax Forms5.pdf” and came with a phishing kit.

  Check Point Anti-Virus provides protection against this threat
- Indonesia’s election commission has suffered from a data breach leaked on a well-known hacker forum. The data posted includes more than 200 million voters’ personal information such as names, addresses, ID numbers, birth dates, and more. The leaked information appears to date back to 2013.
- Iranian Chafer APT group has targeted government and air transportation companies in Kuwait and Saudi Arabia in a recent attack campaign that included several hacking tools and a custom-built backdoor.
- UK airline EasyJet has been hit by a cyber-attack exposing email addresses and travel information of 9 million customers, and credit card details of 2,200 customers.
- Thailand’s Android users are being targeted by a new variant of DenDroid name “WolfRAT”, operated by Wolf researchers, over messaging apps like WhatsApp, Facebook Messenger and Line. The new variant performs spying functions, stealing photos, audio, text messages and more.
- A hacking group called CyberWare is targeting companies that allegedly conduct loan scams with MilkmanVictory ransomware and multiple denial of service attacks. The ransomware encrypts files and deletes the key, as the hackers intend to create irreversible damage rather than ask for ransom.

  Check Point SandBlast provides protection against this threat

VULNERABILITIES AND PATCHES

- Researchers have disclosed a security flaw in the Bluetooth and Wi-Fi protocols that left multiple devices, such all iPhones, MacBooks, and the Samsung Galaxy S series, vulnerable to a new attack named Spectra.
- Five windows zero-day vulnerabilities that allow attackers to escalate privileges have been disclosed. Four vulnerabilities are treated as critical. (CVE-2020-0915, CVE-2020-0986, CVE-2020-0916, CVE-2020-0915)
- Docker has fixed a security vulnerability in Dockers windows client. The vulnerability (CVE-2020-11492) allows attackers to run programs as SYSTEM which can lead to executing commands with the highest privileges.
- Microsoft has released a security update to a vulnerability in Edge (Chromium-based) (CVE-2020-1195). An attacker could exploit this vulnerability to write files to arbitrary locations and gain elevated privileges.
- Cisco has fixed a critical remote code execution vulnerability (CVE-2020-3280) in Cisco Unified Contact Center Express.
- VMware has released a patch for a VMware cloud directory code injection vulnerability, which may lead to arbitrary remote code execution (CVE-2020-3956).

THREAT INTELLIGENCE REPORTS

- Check Point Research has introduced a new security mechanism for Linux called “safe-linking”. This mechanism, which protects against exploitation of single-linked lists, is now deployed in popular open-source libraries such as glibc.
- Researchers have analyzed “DEFENSOR ID”, a banking Trojan that can steal the victim’s bank account credentials, cryptocurrency wallet private key, two-factor authentication and more. The Android app was available on the official Google Play store.

  Check Point SandBlast Mobile provides protection against this threat
- Ragnar Locker ransomware has improved and is now opening a virtual machine on the victim’s device to avoid detection while running the ransomware, then mapping network drives and encrypting them.

  Check Point SandBlast provides protection against this threat *(Ransomware.Win32.Ragnarlocker)*
- Researchers have released a new jailbreak tool that can unlock all iPhones that run versions of iOS from 11 to 13.5. It is yet unknown which vulnerabilities were used in building the jailbreak.
- Winnti hacking group is using a new malware named PipeMon with a novel method to achieve persistence in attacks aimed at video game companies.