June 25 – July 1, 2018

Check Point SOFTWARE TECHNOLOGIES LTD.

YOUR CHECK POINT

THREAT INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- A data leak has taken place at Exactis, a Florida based marketing firm. Data of over 340 million people was exposed online, including phone numbers, email and home addresses, habits and interests, and number, gender, and age of their children. It is unclear whether the data was accessed by rogue actors.
- Sportswear company Adidas has announced a potential security breach of its American website, leading to the exposure and possible leak of the data of millions of customers, including contact information, user names and encrypted passwords. Relevant clients are contacted by the company.
- Entertainment ticketing service Ticketmaster has announced a security breach in its UK website, leading to the possible leak of customers' personal and payment data. The breach occurred in a customer support chat application provided by the AI Company Inbenta, which has been injected with malicious code transferring client data to an unknown actor.
- A new attempt by the threat-group "AsiaHitGroup Gang" to infiltrate Google Play with malicious apps has been revealed. The app uses the push notification service to subscribe users to premium-rate services, customized by region, thereby stealing their money.
- Security researchers have discovered a in the wild exploit of the recently-discovered PROPagate code injection technique, where an attacker could abuse the SetWindowSubclass API, a function in Windows OS that manages GUIs. The technique is being used as part of a campaign utilizing RIG Exploit Kit, using compromised websites, and the code injected installs a Monero miner on the victim's machine.

  Check Point IPS blade provides protection against this threat (RIG Exploit Kit Landing Page; Suspicious Exploit Kit Website Redirection; RIG Exploit Kit Website Redirection; RIG Exploit Kit URL; RIG Exploit Kit Landing Page URL)

- Researchers have reported that the GitHub account of the Gentoo Linux organization has been hacked, and the attacker replaced parts of the code hosted on Github with malicious code which may compromise user-data. The organization advised users and organizations that downloaded Gentoo Linux images from the GitHub mirror to restore the OS to a previous point, or reinstall it from scratch.

VULNERABILITIES AND PATCHES

- Researchers have discovered a flaw in the core of WordPress, which allows users with basic Author permissions to insert malicious code into the site that deletes crucial system files. WordPress has not yet addressed the issue.
- Oracle has patched issues arising from the new variant of Meltdown and Spectre exploits, variant 4, exposed in May, which affects Oracle Linux versions 6 and 7, and Oracle VM 3.4.

  Check Point IPS and Anti-Bot blades provide protection against this threat (WordPress Core File Delete to Code Execution; Web Servers Malicious Upload Directory Traversal; Trojan-Ransom.Win32.Spectre.)*

THREAT INTELLIGENCE REPORTS

- Researchers have uncovered an attempt by the Chinese APT "Tick" to compromise a secure USB drive built by a South Korean defense company, likely with the intent of compromising air-gapped systems. The researchers hypnotized that the attack, specifically targeting systems running Windows XP or Windows Server 2003, may be meant to work in cahoots with another malware developed by the APT, "SymonLoader". They do not, however, have evidence that this is an ongoing campaign.
- Security researchers have warned against a new set of techniques, dubbed "RAMpage", which could bypass existing mitigation techniques and re-enable an unprivileged Android app running on the victim's device to exploit a hardware vulnerability, which could allow an attacker to gain root privileges on a device. The vulnerability could impact devices manufactured in 2012 onwards.
- Security researchers have released a free decryption tool for files encrypted by the Thanatos ransomware. This tool is particularly crucial, as a flaw in the ramsonware's design leads to failure to decrypt files even after the ransom is paid.
- Security researchers have developed three new ways to penetrate mobile 4G networks (LTE). All the attack vectors abuse the data link layer, which maintains the wireless communication between the users and the network. Two of the attacks are passive, allowing an attacker to listen to communication between the victim and base stations. One, however, is an active man-in-the-middle attack which could enable the attacker to intercept victim's communications and redirect the victim to malicious websites.
- Security researchers have discovered security flaws in Fredi Wi-Fi baby monitors, which could be used by remote attackers to view video-streams. The flaw is due to the fact that authentication vis-à-vis the p2p service where the video-feed is sent requires only 8-digit device number and a default password shared between all devices, a flaw which may be relevant to other IoT devices that use the same firmware.