Airbus, the world's second-largest manufacturers of commercial airplanes, has confirmed it was subject to a data breach exposing personal data of its employees. The company is still investigating the full scope of the breach.

Home remodeling and design platform “Houzz”, which has over 40 million monthly users, has informed customers that it suffered a data breach that exposed personal information.

Altran Technologies, a global engineering and R&D services corporation, has shut down its computer network and applications after being hit by a new strand of ransomware called “LockerGoga”.

Check Point SandBlast and Anti-Virus blades provide protection against this threat (Ransomware.Win32.LockerGoga)

A severe flaw at the back-end service of the Chinese “Caref Watch” corporation has exposed sensitive information of 35,000 kids and 20,000 individual accounts of GPS-tracking watches. Breached information included real-time child location, name, parent’s details etc.

“Chafer”, an Iran-linked APT, has been targeting various diplomatic entities based in Iran with an enhanced version of the Remexi malware capable of exfiltrating keystrokes, screenshots and browser-related data like cookies and history.

In an attempt to fight the “Joanap” botnet, part of the allegedly North Korean Lazarus APT Group, the US government has announced its efforts to map infected computers and notify victims. Being a P2P based botnet, the FBI uses intentionally infected computers in order to map infected machines.

Check Point SandBlast, Anti-Bot and Anti-Virus blades provide protection against this threat (Backdoor.Win32.Joanap)

Apple has revoked Facebook’s enterprise certificates, intended for internal apps only, after Facebook used it to offer non-Facebook-employees, as young as 13 years old, monthly $20 gift cards in return for installing a “Facebook research” app that gave the company invasive access to large swathes of user data. Apple soon restored Facebook’s certificate permission.
VULNERABILITIES AND PATCHES

- Apple has issued a partial fix for recent FaceTime spying bug that gave callers access to audio of unanswered FaceTime calls. The bug was discovered by a 14-year-old from Arizona, who attempted to report the flaw to Apple for more than 10 days without success. A full fix is expected later this week.

- Researchers have published a PoC to an exploit of Cisco RV320/RV325 routers demonstrating the vulnerability of 10,000 routers worldwide. Combination of two vulnerabilities (CVE-2019-1652 and CVE-2019-1653) allow remote attackers to take full control of affected routers. Administrators are recommended to install Cisco RV320 and RV325 firmware release.

  *Check Point IPS blade provides protection against CVE-2019-1652, and will provide protection against CVE-2019-1653 in its next online package (Cisco RV320 OS Command Injection (CVE-2019-1652))*

THREAT INTELLIGENCE REPORTS

- Newly discovered malware dubbed “CookieMiner” steals web browser cookies, text messages and credentials of Mac users in an attempt to withdraw funds from their cryptocurrency exchange accounts.

  *Check Point Anti-Virus blade provides protection against this threat (Cryptominer.OSX.CookieMiner)*

- Europol and law enforcement agencies worldwide are investigating DDoS-for-hire services and hunting users that paid them to carry out cyber-attacks. DDoS related offences in the U.S. and U.K. in recent years reach up to 10 yrs. prison sentences.

- “The Moon” IoT botnet which targets broadband modems and routers is now offered as a service (MaaS) to cybercrime gangs using it for credential brute forcing, video advertisement frauds, general traffic obfuscation and more.

- “Zepakab” malware, recently used by the “Sofacy” APT28 group, is utilizing code from publicly available scripts to bypass most traditional antiviruses.

  *Check SandBlast, Anti-Bot and Point Anti-Virus blades provide protection against this threat (Trojan-PSW.Win32.Sofacy; Backdoor.Win32.Zebrocy)*

- Following the new Golang (Go) programming language trend, researchers have published an analysis to a cryptocurrency wallet stealer written in GO.

  *Check Point SandBlast and Anti-Virus blades provide protection against this threat (Infostealer.Win32.CryptoStealerGo)*

For comments, please contact: TI-bulletin@checkpoint.com