Check Point
SOFTWARE TECHNOLOGIES LTD.

May 17-23, 2021

YOUR CHECK POINT
THREAT INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- Check Point Research has discovered multiple misconfiguration flaws in third party cloud services of Android applications, which have led to the exposure of sensitive personal data of more than 100 million Android users and developers. Many flaws were the result of improper configuration of real-time databases.

  Check Point Harmony Mobile provides protection against this threat (Trojan.AndroidOS.CopyCat)

- CNA Financial, one of the largest insurance corporations in the US, has reportedly paid $40 million, considered to be the highest ransom paid by a single ransomware victim. The company suffered an attack in late March, in which data was stolen and employee access to the company network was blocked.

- Air India has disclosed a data breach affecting the personal information of almost 4.5 million of its customers. The breach is the result of an attack targeting the SITA PSS component, a data processor as part of the passenger service system. Breached records include passport numbers and credit card information.

- Japanese e-commerce company Mercari has suffered a data breach made possible as part of the Codecov supply-chain attack. Some 27,000 customer records have been exposed, among them 17,000 records containing banking information and 8,000 records of business partners.

- The Alaska Department of Health has been forced to go offline by a malware attack, possibly involving ransomware. The incident follows a recent attack that had hit Alaska's court system.

- Large-scale campaign has been distributing a Java-based RAT dubbed 'STRRAT' that disguises itself as a ransomware and features enhanced data theft functions. The campaign leverages compromised email accounts and malicious images pretending to be PDF attachments.

  Check Point Threat Emulation and Anti-Virus provide protection against this threat (RAT.Win32.JavaSTRRAT)

- Brazilian banking malware dubbed 'Bizarro' has been targeting customers of some 70 banks in South America and Europe, in a campaign that relies on tax-themed phishing emails. The malware terminates existing sessions with online banking portals, forcing the user to log-in again.

VULNERABILITIES AND PATCHES

- Patches have been released for four zero-day vulnerabilities in Android. The vulnerabilities have already been exploited in-the-wild in targeted attacks, influencing a limited number of users. The four flaws impact Qualcomm GPU and Arm Mali GPU Driver components.
- Five vulnerabilities have been discovered in the infotainment system of Mercedes-Benz cars. Four of the flaws can be exploited remotely and allow the attackers to gain control over several non-physical functions of the vehicle. The system was launched in 2018 but uses an outdated version of Linux Kernel.
- Researchers have detected a 10-year old vulnerability in Dell dbutil kernel mode Driver, installed on Windows OS machines using firmware update utility packages used to update the BIOS, such as Dell Update. The flaw, assigned CVE-2021-21551, might lead to information disclosure or privilege escalation.

THREAT INTELLIGENCE REPORTS

- QNAP has been warning its customers against an attack on Hybrid Backup Sync (HBS) 3 app that runs on their Network Attached Storage (NAS) devices. The attack exploits an improper authorization vulnerability assigned CVE-2021-28799 and delivers the Qlocker ransomware.
- The FBI has reported that the Conti ransomware, which operates in a Malware-as-a-Service model, is behind at least 16 attacks targeting healthcare and first responders facilities in the US in the past year, including law enforcement agencies and emergency medical services.

  Check Point Threat Emulation and Harmony Endpoint provide protection against this threat (Ransomware.Win32.Conti)
- New botnet called 'Simps' has recently emerged, designed to launch DDoS attacks against targets from the gaming arena and more, using IoT devices as bots. The malware has been dropped by the Gafgyt botnet on Realtek and Linksys endpoints, leveraging a flaw assigned CVE-2014-8361.

  Check Point Threat Emulation and Anti-Bot provide protection against this threat (Botnet.Linux.Gafgyt; Backdoor.Linux.Gafgyt)
- Threat actors have developed a new infection scheme used to distribute the BazarLoader backdoor. The vishing-based technique, dubbed 'BazarCall', features a phone-call conducted by an alleged call center operator following a phishing email. The operator offers the victim assistance unsubscribing from a service.

  Check Point Anti-Virus provides protection against this threat (Backdoor.Win32.BazarCall)
- Researchers have observed a spike in phishing attacks against cloud-based business services in Q1 2021. Hackers used the trusted reputation of cloud storage to send phishing emails and host attacks. In Q1 only, researchers observed around 100 million malicious messages from Google and Microsoft Office 365.