Check Point
SOFTWARE TECHNOLOGIES LTD.

June 17 - 23, 2019

YOUR CHECK POINT
THREAT INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- Oregon's Department of Human Services has announced that it was a victim of a data breach, potentially impacting the personal details and health information of 645,000 clients. The breach happened last January, following a phishing attack that hit the department where at least 9 employees were deceived.
- Canadian Desjardins credit union has revealed that it suffered a massive data leak in December 2018, when a bank employee stole banking information of 2.9 Million users.
- Over 7 Million transactions scraped from the Venmo digital wallet app, owned by Paypal, have been leaked online by a security researcher. The dataset was leaked after Venmo repeatedly failed to protect their users' transactions and kept streaming them to a publicly available URL.
- Eatstreet, the online food ordering service, has disclosed a security breach that occurred on May after an attacker gained access to the company's database. The breach, which was discovered two weeks later, exposed customer payment information as well as personal information.
- The Riviera Beach City, Florida, has agreed to pay $600,000 in ransom to decrypt its records following a ransomware attack that hit them towards the end of May. The decision was made after the IT personnel failed to restore the encrypted data, which was directly affecting the city's critical infrastructures.
- The patient recovery agency American Medical Collection Agency (AMCA) has filed for bankruptcy after their recent data breach, where attackers broke into their web payment portal. The breach greatly damaged AMCA, impacting around 19.7 million of its patients and causing both financial and legal consequences for the organization.
- The file sharing service WeTransfer revealed that for two days it was sending their users' shared files to the wrong recipients. While the reason for this issue is still unclear, the URLs used in the incident were blocked and the affected accounts had their passwords reset.

VULNERABILITIES AND PATCHES

- A zero-day vulnerability has been discovered in TP-Link Wi-Fi extender, which allows remote attackers to execute arbitrary code on vulnerable devices through a malformed User-Agent field in HTTP headers.

  Check Point IPS blade provides protection against this threat *(TP-Link WiFi Extender Remote Code Execution (CVE-2019-7406))*

- Evernote's Web Clipper Chrome extension has been found vulnerable to a cross-site scripting vulnerability that allows attackers to access sensitive user information from third-party web platforms. The flaw, assigned CVE-2019-12592, can allow hacking into active sessions of other websites and bypassing Chrome's same-origin policy.

  Check Point IPS blade provides protection against this threat *(Evernote Web Clipper Cross Site Scripting (CVE-2019-12592))*

- Three Denial-of-Service vulnerabilities in Linux Kernel's TCP\IP implementation has been found. One of the flaws, assigned CVE-2019-11477, is considered to be high severity and may trigger a kernel panic condition in the affected system, impacting the system's availability.

  See Check Point response in this SK

THREAT INTELLIGENCE REPORTS

- Check Point Researchers have revealed that some of the new variants of DanaBot are demanding ransom payment. The newly-discovered variants, belonging to European campaigns of the infamous banking Trojan, were observed dropping executables that turned out to be ransomware.

  Check Point Anti-Bot blade and SandBlast Agent provide protection against this threat *(Trojan.Win32.DanaBot)*

- A new mobile cyberespionage campaign targeting Android devices in the Middle East has been discovered. The campaign, dubbed "Bouncing Golf", is planting pieces of malware inside tainted applications that are commonly used in Middle Eastern countries. Information stolen from devices appears to be military-related, and there are several connections to the Domestic Kitten campaign revealed by Check Point in 2018.

  Check Point SandBlast Agent provides protection against this threat

- Turla, the Russia-linked cyberespionage group, has been hijacking other threat groups' infrastructure in their recent attacks against Middle Eastern targets. As part of one of their newest campaigns, Turla has introduced a new backdoor which was using the C2 servers of the Iran-linked group OilRig.

- A new campaign is targeting managed service providers (MSPs) by replacing downloads in legitimate websites with ransomware installers, in attempt to spread them to the managed endpoints. The ransomware, dubbed Sodinokibi, was also seen distributed via wide-net spam campaigns.

  Check Point Anti-Virus blade provides protection against this threat *(Ransomware.Win32.Sodinokibi)*