Check Point
SOFTWARE TECHNOLOGIES LTD.

August 19 - 25, 2019

YOUR CHECK POINT
THREAT INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- Mastercard has disclosed a data breach that impacted customer data belonging to German and Belgian customers that were part of the company's Priceless Specials program. The incident was discovered after files of the stolen data, which included credit card numbers as well as personal information, were published online.

- Over 20 Texas government organizations have been hit with ransomware in what appears to be a pre-coordinated attack against the entities. The cybercriminals behind the attack demanded $2.5 million in ransom to decrypt the data.

  Check Point SandBlast Agent provides protection against this threat

- Employees of a nuclear power plant in Ukraine are suspected of abusing the systems of the power plant's internal network to mine cryptocurrency. The employees allegedly connected some of the systems to the internet, exposing the sensitive internal network of the plant to security breaches.

- MoviePass, the popular movie ticket subscription service, left an exposed database online containing 161 million records of personal data, including unencrypted credit card details of its customers as well as other billing information and login credentials.

- Personal email addresses of over a million adult content website users were found exposed in an unsecured Elasticsearch database online. The database included full names for some of the users, as well as user activity logs.

- A hacker who carried out phishing attacks against hundreds of companies worldwide and sold their stolen data online has been ordered to pay back more than $1.1 million he earned in bitcoin and other cryptocurrencies. Among the attacked companies to receive compensation are Uber, Sainsbury's, Groupon and T Mobile.

©2019 Check Point Software Technologies Ltd. All rights reserved. [Protected] Non-confidential content

VULNERABILITIES AND PATCHES

- A heap buffer overflow vulnerability has been discovered in some versions of Squid web proxy cache servers. The vulnerability, tracked as CVE-2019-12527, may allow attackers to trigger a denial-of-service condition and execute arbitrary code on the vulnerable servers.
- A zero-day privilege-escalation vulnerability has been found in Steam client for Windows, affecting over 96 million users. The vulnerability may allow an attacker to run executables using Steam Client Service's elevated permissions.
- Two severe vulnerabilities exist in all versions of the Kubernetes open-source system that may allow an unauthorized attacker to trigger a denial-of-service condition. Kubernetes has already released patched versions to address the issues.

THREAT INTELLIGENCE REPORTS

- An Android music app infected with AhMyth Remote-Access-Trojan has managed to bypass Google Play's security mechanisms twice in the span of two weeks. The app is able to steal contacts, harvest files stored on the device and send SMS messages from it.

  Check Point SandBlast Mobile provides protection against this threat

- Threat actors are cloning popular websites, and specifically the NordVPN website, to distribute the Bolik banking Trojan. These actors were previously known for hacking into websites and hijacking download links to refer to their malware.

  Check Point SandBlast provides protection against this threat

- A report uncovers the recent activity of Silence APT, a Russian-speaking group targeting financial organizations in former Soviet states. The group is expanding their geography and aggressively targeting banks in more than 30 countries all over the world, while also enhancing their arsenal.
- Researchers have uncovered the recent activity of APT41, the China-linked APT group, which is known for its financially motivated operations as well as state-sponsored espionage activity. The group was recently observed targeting a web server at a US-based research university, exploiting several vulnerabilities to compromise its systems and load different payloads.

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

- The Command and Control servers of the Emotet botnet have resumed their activity and are now delivering binaries again, after a break of almost 3 months.

  Check Point SandBlast and Anti-Bot blades provide protection against this threat *(Botnet.Win32.Emotet)*