April 6 - 12, 2020

YOUR CHECK POINT

# THREAT INTELLIGENCE REPORT

## TOP ATTACKS AND BREACHES

- Hammersmith Medicines Research LTD (HMR), a research firm on standby to perform live trials of coronavirus vaccines, has suffered a data breach by the Maze ransomware. HMR has decided not to pay the ransom, only to have stolen data published a week later on the attackers "News" site. The attack compromised volunteers' identity documents and test results, including positive HIV and drug tests.

  *Check Point SandBlast and Anti-bot provide protection against this threat (Ransomware.Win32.Maze)*

- Finastra, a major banking industry software company, who suffered a data breach and a ransomware attack by the Ryuk ransomware, chose not to pay the ransom and instead opted to take thousands of servers offline. The attackers roamed through Finastra systems for 3 days, stealing passwords and installing backdoors in dozens of servers, and eventually installed Ryuk ransomware.

  *Check Point SandBlast and Anti-Bot provide protection against this threat (Ransomware.Win32.Ryuk)*

- Travelex has opted to pay $2.3 million to release its information. Travelex, a London-based foreign exchange company, was crippled for weeks due to the attack by the Sodinokibi gang. Travelex has negotiated with the group for the last few weeks until reaching the sum.

  *Check Point SandBlast and Anti-Bot provide protection against this threat (Ransomware.Win32.Sodinokibi)*

- Cisco Webex web conferencing platform has suffered a phishing campaign trying to steal users' credentials. Emails were sent from a spoofed Webex email address with the subject "critical security advisory", and included a genuine security advisory from 2016.

- San Francisco Airport (SFO) has had two of its websites hacked, leading to the exposure of Windows credentials of users who have accessed the site remotely.

- Italian email hosting website Email.it has suffered a major breach, exposing 600,000 users' details including plaintext passwords, security questions, email content and attachments from the years 2007-2020. The attackers, failing to obtain the ransom, chose instead to attempt to sell the information.

## VULNERABILITIES AND PATCHES

- VMware has patched a critical information disclosure flaw in VCenter Server (CVE-2020-3952), with the maximum CVSSv3 vase score of 10.0. The flaw resides in the VMware Directory Service (vmdir), which under certain conditions could allow a malicious attacker with network access to obtain sensitive information.
- Firefox has fixed memory safety bugs (CVE-2020-6825/6) that can lead to arbitrary code execution, as well as other two high-risk bugs that can be exploited to leak sensitive data (CVE-2020-6821) or to trick the mobile browser into displaying the incorrect URI (CVE-2020-6827).
- Google has removed the Android VPN app "SuperVPN" from the play store after being notified of a critical man in the middle vulnerability in it. The app was downloaded more than 100 million times.

## THREAT INTELLIGENCE REPORTS

- Check Point Research has discovered 16 malicious apps, all masquerading as legitimate coronavirus-related apps, which contained a range of malware aimed at stealing users' sensitive information or generating fraudulent revenues from premium-rate services, including Mobile Remote Access Trojans (MRATs), Banker Trojans, and Premium Dialers.

  *Check Point SandBlast Mobile provides protection against this threat.*

- Check Point Research has shown that threat actors are migrating their infrastructure to the cloud. Malware such as Nanocore, Lokibot, Remcos, Pony Stealer and Legion Loader are hosted on Google Drive and Dropbox rather than locally at the threat actors' servers.

  *Check Point SandBlast and Anti-Bot provide protection against these threats*

- In the midst of the coronavirus pandemic, Interpol are warning about an increase in the number of ransomware attacks against hospitals.
- Researchers have found more than 2,300 usernames and passwords to Zoom accounts, including corporate accounts belonging to banks, healthcare providers and more. Some of the accounts included meetings IDs, names and host keys. The researchers have noted dark web discussions include discussing checking services (to check the viability of credentials) and credential stuffing (brute testing a batch of stolen credentials) to automate attacks on the Zoom platform.

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