May 25 - 31, 2020

YOUR CHECK POINT

# THREAT INTELLIGENCE REPORT

## TOP ATTACKS AND BREACHES

- The US NSA has warned that Russia's Sandworm APT group, an arm of Russian military intelligence, has been exploiting a vulnerability in the Exim mail traffic agent since August of last year, giving it remote code execution abilities. Sandworm is believed to have been responsible for the Ukraine grid disruptions in 2015.

  *Check Point IPS provides protection against this threat (Exim Mail Server Remote Code Execution (CVE-2019-10149))*

- New ransomware called FuckUnicorn has been targeting Italian health entities through emails with links to a COVID-19-related app for PC. The links direct users to a malicious domain imitating the site of the Italian Pharmacist Federation. Researchers suspect the actors behind this attack are Italians.

- In a supply chain attack, threat actors have used GitHub projects to spread the Octopus Scanner backdoor. 26 open-source NetBeans Java projects included the malware, intended to steal information from developers.

- Popular math app, Mathway, has been breached and its database of 25M users is offered for sale in various forums. The hacker behind that attack, ShinyHunters, responsible for multiple recent attacks, is believed to have sold access to more than 200 million user details.

- Michigan State University has been compromised by the NetWalker ransomware. Threat actors shared images of the stolen information and threatened to leak sensitive data unless ransom is paid.

- Six of Cisco's Virtual Internet Routing Lab Personal Edition (VIRL-PE) backend servers have been compromised by exploiting critical SaltStack vulnerabilities, patched last month. Exploitation of two SaltStack vulnerabilities (CVE-2020-11652 and CVE-2020-11651) provide unauthenticated attackers with full read and write access. Analysis from May 1st found more than 5,000 exposed vulnerable servers.

  *Check Point IPS provides protection against this threat (Saltstack Salt Authentication Bypass (CVE-2020-11651))*

- Following its reported attack earlier this year on the state-owned Bank of Costa Rica, the Maze group, infamous for a recent wave of double-extortion attacks, has started releasing payment card data obtained in

the attack. The group reports it is in possession of some 4 million unique payment card numbers, including 140,000 allegedly belonging to U.S. customers.

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

## VULNERABILITIES AND PATCHES

- Apple's iOS 13.5 and iPadOS 13.5 have patched two zero-click vulnerabilities affecting their Mail app. The patched vulnerabilities, tracked as CVE-2020-9819/8, have been exploited in the wild by a nation-state since at least January 2018.
- A new critical vulnerability has been reported for Android OS, tracked as CVE-2020-0096, aka StrandHogg 2.0. The vulnerability is a privilege elevation flaw that could grant hackers access to almost all apps installed on a devices including camera and microphone, device location, read SMS and capture login credentials including 2FA codes sent via SMS.
- A Bug in the 'Sign in with Apple' feature, which allows users to sign in to 3rd party apps like Dropbox, Spotify, Airbnb and more, exposed any user to full account takeover by potential attackers. The vulnerability was responsibly reported to Apple, patched and according to the company hasn't been exploited in the wild.

## THREAT INTELLIGENCE REPORTS

- Check Point Research has exposed the identity of a Brazilian hacker known as Vanda TheGod, responsible for attacks and defacements of thousands of websites from numerous countries, including Brazil, the Dominican Republic, Trinidad and Tobago, Argentina, Thailand, Vietnam, and New Zealand. The attacker targeted governments, universities, and hospital websites.
- Chinese tech companies are taking action to disrupt the activity of the DoubleGuns botnet that controls hundreds of thousands of infected computers in China, used for stealing credentials and for adware and spamming purposes. The companies concentrate in locating and removing image files stored by their services and used by the botnet to provide instructions to bots using steganography.
- Report finds that a revised version of the ComRAT remote access tool has been used by Turla, an APT group linked to the Russian government, to attack government entities in Eastern Europe and Caucasus region. The new version exfiltrates AV logs, thus notifying attackers of detection and includes the ability to control the malware through Gmail accounts.

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