March 9-15, 2020

YOUR CHECK POINT
THREAT INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- A campaign leveraging the COVID-19 pandemic to target the Mongolian government and public sector has been detected by Check Point Research. The campaign, attributed to a China-linked APT group, used spear-phishing and coronavirus-themed documents to install a custom remote-access Trojan.

  Check Point SandBlast Agent provides protection against this threat *(Backdoor.Win32.Viciouspanda)*

- Cybercriminals continue to exploit the fear surrounding the COVID-19 outbreak and are now distributing instances of AZORult info stealer using a weaponized application for Coronavirus heat map. The app displays a legitimate Coronavirus map while the info stealer is running in the background.

  Check Point Anti-Bot provides protection against this threat *(Backdoor.Win32.Viciouspanda)*

- The European electricity transmission operator ENTSO-E has been the victim of a security breach, after threat actors managed to penetrate its network. The attack affected only the office network of the operator, who also manages 36 European electricity distribution companies which were not impacted.

- Whisper, the popular confessions app, has been found to expose nearly a billion records of its users, after storing data in plaintext in unsecured ElasticSearch servers. The logged data did not include names or other PII, however it contained users' age, hometown, ethnicity and nickname. It also disclosed membership of private groups and geo-coordinates of where the confession was published from.

- A ransomware attack has hit the city of Marseille, France. The ransomware managed to infect and disable around 300 machines in the city hall network. Despite its broad impact, the attack is not expected to disrupt the upcoming municipal elections in the city.

- A cyberattack has hit a major Coronavirus testing laboratory in a hospital in the Czech Republic, resulting in shutdown of some of the IT networks of the laboratory and two other branches of the hospital.

- Entercom, the second-largest radio company in the United States, suffered a cyber-attack in August 2019. The attack potentially exposed sensitive user data such as names and Social Security numbers.

VULNERABILITIES AND PATCHES

- A critical wormable vulnerability in Windows SMBv3 servers has been addressed and patched by Microsoft. The vulnerability, which may allow a remote attacker to execute code on the target SMB server or client, currently impacts certain versions of Windows 10 and Windows Server.

  Check Point IPS blade provides protection against this threat *(Microsoft Windows SMBv3 Remote Code Execution (CVE-2020-0796))*

- A new vulnerability affecting Intel's CPU has been discovered, and may allow a low-privileged attacker to steal sensitive information stored in the protected memory in the processor. The new vulnerability differs from previously discovered ones, as it potentially allows the attacker to load and execute malicious data into the memory rather than simply view or steal it.

- 16 security issues and vulnerabilities in Zyxel Network Management Software have been discovered, exposing users to a variety of cyber-attacks. The discovered array of vulnerabilities includes default credentials issues, insecure memory storage and backdoor accounts.

- VMWare has addressed three serious vulnerabilities in its products. One of them, a critical flaw affecting VMWare Workstation and Fusion, could be exploited to execute code from the guest machine on the host machine or trigger a denial-of-service condition for certain services.

THREAT INTELLIGENCE REPORTS

- Check Point Research has published the second part of their ongoing analysis of the malicious modules deployed onto victim machines of the Phorpiex botnet. This article addresses additional modules integrated in the botnet, including XMRig miner loader and a NetBIOS worm module.

  Check Point Anti-Virus and Anti-Bot blades provides protection against this threat *(Worm.Win32.Phorpiex)*

- Over 239,000 payment card records are being offered for sale in underground markets, collected from thousands of online shops that used to run a tainted version of Volusion e-commerce software. The estimated revenue for the sellers reaches an astounding $100 million.

- A new backdoor malware, dubbed BlackWater, has been discovered. BlackWater is dropped by a weaponized Word document pretending to provide information on the COVID-19 outbreak. The backdoor abuses Cloudflare Workers execution environments as its C2 servers.

- Researchers have discovered a series of watering hole attacks injecting malicious code into several high-profile American websites. By displaying a fake Adobe Flash update to selected victims, the actors delivered malware pieces tracked as NetFlash and PyFlash. The campaign is attributed to the Russia-linked APT Turla, known to target diplomatic and government organizations in the Americas and EMEA.