March 16 - 22, 2020

Check Point
SOFTWARE TECHNOLOGIES LTD.

YOUR CHECK POINT
THREAT INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- The U.S Health and Human Services Department has suffered a DDoS attack on its website Sunday night during the nation's response to the coronavirus pandemic. The attack appears to have been intended to slow the agency's system down.
- Aerial Direct, O2 telco's largest partner in the UK, has suffered a data breach through an external back up database containing 6 years' worth of customer names, dates of birth, business addresses, email addresses, phone numbers, and product information.
- APT36, Pakistani state-sponsored threat actor, has been spreading the Crimson RAT via a spear-phishing campaign using coronavirus themed document disguised to a health advisory email. The RAT steals credentials from the victim's browser, capturs screenshots, collects anti-virus software information, lists running processes, and more.
- Finastra, a financial technology company based in London, has been hit by a ransomware attack that shut down all services. The company provides services to more than 9000 customers from 130 counties including 90 of the top 100 banks globally. The company is currently working on bringing back the system.
- Zero-day vulnerabilities in digital video recorders (DVRs) for surveillance systems manufactured by LILIN have been exploited by multiple DDoS botnet operators. The flaw abuses a chain of vulnerabilities that use hard-coded login credentials, potentially granting the modification of the DVR's configuration file and injecting backdoor commands when FTP or NTP configurations are synchronized.

  Check Point Anti-Bot blade provides protection against this threat *(Chalubo.TC)*
- Fake coronavirus tracking applications are infecting smartphones with ransomware demanding $100 to unlock the smartphone.

  Check Point SandBlast Mobile provides protection against this threat

VULNERABILITIES AND PATCHES

- Trend Micro has released patches for critical vulnerabilities found in the company's Apex one and OfficeScan XG. At least one of the vulnerabilities has been exploited in the wild.
- Slack has fixed a critical HTTP Request Smuggling vulnerability that could be exploited for account takeover.
- Adobe has released security updates for Adobe Acrobat and Adobe Reader fixing 13 vulnerabilities, 9 of them rated critical and allowing arbitrary code execution.

  Check Point IPS blade provides protection against this threat *(Adobe Acrobat and Reader Out-of-Bounds Read (APSB20-13: CVE-2020-3804), Adobe Acrobat and Reader Use After Free (APSB20-13: CVE-2020-3805))*

THREAT INTELLIGENCE REPORTS

- Check Point Research has uncovered who is behind a Nigerian fraud campaign, how they operate, where they source email addresses, and how much money they generated.
- Check Point Research has found additional phishing attacks in which threat actors leverage the coronavirus pandemic to lure victims into clicking malicious links and opening malicious files.
- A new ransomware called Nefilim that shares the same code as Nemty, appeared active in the wild at the end of February and now threatens to release stolen data. Experts believe the malware is being distributed through exposed Remote Desktop Services.

  Check Point SandBlast Agent provides protection against this threat *(Ransomware.Win32.Nefilim)*
- France's cybersecurity agency (CERT) has announced a new wave of ransomware attacks carried out by a new version of the Mespoinoza ransomware, also known as Pysa ransomware, targeting networks of local government authorities using brute-force attacks.

  Check Point SandBlast Agent provides protection against this threat *(Ransomware.Win32.Virlock.TC.pysa)*
- Researchers have found half a million confidential legal and financial documents exposed online, 425GB in total, related to two financial companies. The Amazon Web Services (AWS) S3 bucket was not using any form of encryption, authentication or access credentials, which enabled anyone to access the data.

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