October 28- November 3, 2019

YOUR CHECK POINT

THREAT INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- India's nuclear power plant has been hit by a cyber-attack after malware designed for data extraction was identified in one of its systems. The malware, linked by experts to the North-Korean group Lazarus, infected a computer in the plant's external network, rather than the operational one.

  Check Point SandBlast provides protection against this threat

- Web.com, one of the world's top domain registrars and web hosting services, has disclosed a data breach affecting former and current customers of Web.com, Network Solutions and Register.com. The breach occurred after a third-party gained unauthorized access to a number of the company's computer systems and accessed customer records such as contact details and services purchased.

- A cyber-attack hit the U.S-based renewable energy provider sPower last March. The attackers exploited a known flaw in Cisco Firewalls to carry out Denial-of-Service attacks for 12 hours, causing some of the operators to disconnect from the power generation sites, while actual power generation was intact.

- UniCredit, an Italian banking company, has suffered a data breach that resulted in the leak of personal information belonging to 3 million customers, after an unknown attacker compromised an old file from 2015 containing records of Italian customers, including names, phone numbers and email addresses.

- Nikkei, one of the world's largest media corporations, has lost 29 million dollars after an employee fell victim to a Business Email Compromise and was tricked by scammers to transfer the funds.

- Unknown hackers have targeted 2,000 websites in Georgia in a wave of mysterious cyber-attacks. Among the attacked websites were Georgia's general jurisdiction court, government agencies and other media outlets. The targeted websites were defaced by the hackers to deliver political messages.

- TrialWorks, a provider for legal case management software for law firms, has been hit by ransomware attack that disabled access for legal documents hosted on their platform. The company eventually regained access to their data center, and it is still unknown how their systems were infected.

VULNERABILITIES AND PATCHES

- Two critical remote code execution flaws have been reported in rConfig, the network configuration management utility. Both flaws affect all versions of rConfig and are yet to be patched. Proof-of-concept exploits were published for the vulnerabilities, tracked as CVE-2019-16662 and CVE-2019-16663.

  Check Point IPS blade will provide protection against this threat in its next online packages

- Google has released updates addressing two high severity use-after-free vulnerabilities in chrome. One of the vulnerabilities, a zero-day tracked as CVE-2019-13720, is being actively exploited in the wild. The vulnerabilities could be exploited by tricking Chrome users into visiting specially-crafted websites.

- A security issue affecting Android 8 could be exploited by attackers to infect nearby devices via NFC beaming. Devices running Android 8 or later would not display any security warning to the users when installing apps from an unknown source, exposing them for unauthorized NFC file transfer.

THREAT INTELLIGENCE REPORTS

- Researchers have spotted an attempt to weaponize the BlueKeep RDP vulnerability to compromise vulnerable systems and spread Monero cryptocurrency malware. The exploit is still highly unreliable and does not have self-spreading capabilities.

  Check Point SandBlast Agent and IPS provide protection against this threat (Microsoft Remote Desktop Services Remote Code Execution (CVE-2019-0708))

- A new backdoor called “MessageTap” is being used by APT41, a Chinese state-sponsored espionage group, targeting telecommunications companies in an attempt to spy on text messages of highly targeted individuals, and was found installed in one of the largest telcos.

  Check Point Anti-Virus blade provides protection against this threat (Backdoor.Linux.MessageTap)

- 21 million stolen plaintext credentials from Fortune 500 companies have been found available for sale in multiple dark web markets. 76% of the login credentials discovered were compromised during the last 12 months, with Technology, Finance and Health Care being the top 3 compromised industries.

- A new spam email campaign targeting Italian users is delivering the Maze ransomware via malicious macros in weaponized attachments. The emails pretend to be from the Italian Tax and Revenue Agency and contain “RSA encrypted” documents, prompting the user to enable macros to view the content.

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

- Fancy Bear, the Russian APT group, is reportedly targeting anti-doping authorities and sporting organizations around the world in a new wave of attacks believed to be linked to the upcoming 2020 Olympics in Tokyo. The group was also accused in 2018 of conducting the Olympic Destroyer attack.