December 17 - 23, 2018

YOUR CHECK POINT

THREAT INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- NASA has fallen victim to a personal information breach after unknown hackers managed to gain access to one of its servers. Any NASA Civil Service employee who joined, left, or transferred within the agency from July 2006 to October 2018 may have had their personal data compromised.
- Two Chinese government hackers have been indicted in the US over global hacking campaign related to APT10 group. They allegedly targeted more than 45 companies and government agencies from 2006 to 2018, including managed service providers, the U.S. Navy, NASA and the Department of Energy.
- Twitter has disclosed a suspected state-sponsored attack after a minor data breach. The company discovered a bug being misused to access users' exposed information by multiple inquiries originating from IP addresses in China and Saudi Arabia, thus raising suspicions of a state-sponsored attack.
- Newly detected malware retrieves concealed commands from meme images in Twitter account. Information gathered according to the retrieved command is then sent to a C&C server whose address is a hard-coded URL on pastebin.com

  Check Point SandBlast and Anti-Virus blades provide protection against this threat (Trojan.win32.meme_reader)

- The FBI has seized domains of 15 "DDoS-for-hire" websites and charged two individuals running some of these services. The FBI stated that both operators of DDoS attacks and individuals hiring a DDoS service to do it are considered cyber criminals.
- Caribou Coffee has suffered from a credit card breach that hit more than 260 of its stores in the United States. Compromised records include names and payment card information, such as card number, expiration date, and card security code.

VULNERABILITIES AND PATCHES

- Microsoft has issued an urgent security update to patch a critical zero-day vulnerability in Internet Explorer (IE) Web browser that attackers are already exploiting in the wild. A successful exploitation may allow attackers to take control of the affected system as well as to install programs; view, change, or delete data; or create new accounts with full user privileges.

  Check Point IPS blade provides protection against this threat (Microsoft Internet Explorer Scripting Engine Memory Corruption (CVE-2018-8653))

- Siemens has addressed several vulnerabilities in its SINUMERIK industrial CNC controllers, including denial-of-service, privilege escalation and code execution issues.

- Researchers have discovered serious flaws in some ABB PLC gateways, used for communication between control systems. The flaw may allow attackers to change device settings, cause a DoS condition, or inject malicious code via the administrative HTTP and telnet interfaces. ABB will not release firmware updates as the impacted products have reached the end of life.

- A hacker has uncovered an unpatched Windows zero-day exploit an announced it on his Twitter account. The exploit could allow a low-privileged user or a malicious program to read the content of any file on a targeted Windows computer, otherwise available only through admin privileges.

- Cisco Adaptive Security Appliance (ASA) Software is affected by a vulnerability that could be exploited by an attacker to retrieve files or replace software images on a device.

- Huawei's new vulnerability marked as CVE-2018–7900 reveals routers with default credential, thus allowing attackers to find a list of exposed devices, login, and hack into victims' networks with minimal hacking skills.

THREAT INTELLIGENCE REPORTS

- A sophisticated spam injection malware has targeted WordPress websites, injecting concealed elements into html code to promote attacker's websites in search engine results and redirect attacked site visitors to spam content.

- Analysis of the Shmoon-3 leads researchers to conclude that APT33 or a group camouflaged as APT33 is behind the attacks earlier this month on oil, gas, energy, telecom, and government organizations in the Middle East and southern Europe. A new variant of the open-source SuperDelete wiper tool was integrated and used in the attack.