March 18 – 24, 2019

Check Point SOFTWARE TECHNOLOGIES LTD.

YOUR CHECK POINT THREAT INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- Aluminum Company 'Norsk Hydro' has been forced to shut down several of its plants after a 'LockerGoga' ransomware attack hit its operations. Hydro declared it will not pay ransom. Two American chemical companies were reported to have been attacked by LockerGoga earlier this month.

  Check Point Sandblast provides protection against this threat *(Ransomware.Win32.LockerGoga)*

- Magecart hacking groups have targeted online shoppers' credit card details in a code injection attack on websites of bedding retailers MyPillow and Amerisleep. Customers and potential credit card owners were not informed.

- A new malspam campaign uses fake emails pretending to originate from "Centers for Disease Control and Prevention" (CDC), warning recipients of a flu pandemic. Macros in an attached document are used to infect victims with the GandCrab v5.2 Ransomware.

  Check Point SandBlast and Anti-Bot blades provide protection against this threat *(Generic.TC.dgaxmr; GandCrab_v5.2.TC)*

- 2 million emails with Protected Health Information (PHI) from more than 350,000 customers of the Oregon Department of Human Services (DHS) have potentially been exposed after 9 employee mailboxes were compromised in a spear phishing attack.

- Two ongoing phishing campaigns are actively targeting Netflix and American Express (AMEX) customers, in an attempt to steal credit card and social security information

- The Federal Emergency Management Agency (FEMA) has disclosed a data leak that exposed banking details and other personal information of 2.3 million disaster survivors.

VULNERABILITIES AND PATCHES

- The popular SSH client program PuTTY has released the latest version of its software that includes security patches for 8 high-severity security vulnerabilities.
- WordPress websites using unpatched Social Warfare installations (v3.5.1 and v3.5.2) are exposed to attacks abusing a stored Cross-Site Scripting (XSS) vulnerability fixed in the 3.5.3 version of the plugin.

  Check Point IPS blade will provide protection against this threat in its next online package
- Libssh2, a popular open source client-side C library implementing the SSHv2 protocol, has released the latest version of its software to patch a total of nine security vulnerabilities. Patched vulnerabilities involve memory corruption issues with possible arbitrary code execution possible implications.
- Vulnerabilities in over a dozen models of Medtronic's heart implantable defibrillator expose patients to life threatening hacks. Examined implantable systems require no authentication and fail to use any encryption.
- A total of 11 security flaws and vulnerabilities have been found in a recent inspection of CUJO, a firewall device designed to supply malware protection for domestic networks. CUJO has begun rolling out a system update to resolve the vulnerabilities.

THREAT INTELLIGENCE REPORTS

- A new variant of the Mirai Internet of Things (IoT) botnet has incorporated an additional set of exploits to allow it to target business environments. Current version includes 27 exploits and a new set of credentials used for brute force attacks.

  Check Point Anti-Virus and Anti-Bot blades provide protection against this threat (Backdoor.Linux.Mirai; Mirai.TC); Check Point IPS blade will provide protection against this threat in its next online package
- The December 2018 FBI crackdown on 15 DDoS-For-Hire services has reduced the overall number of DDoS attacks by 11%. Average and maximum DDoS attack sizes also drastically decreased by 85% and 24% respectively.
- An internal investigation by Facebook reveals that for years, millions of users' passwords were mistakenly stored in plaintext rather than hashed, thus leaving them vulnerable to potential theft and exposure.