Check Point
SOFTWARE TECHNOLOGIES LTD.

September 9-15, 2019

YOUR CHECK POINT
THREAT INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- Garmin, the GPS technology company, has fallen victim to a data breach after their South African shopping site was hosting a malicious software skimmer, capturing customers' payment data from the website. The stolen data also included home addresses, phone numbers and email addresses.
- Ransomware has hit the Wolcott school district in Connecticut for the second time in four months, resulting in a complete shutdown of all internal email and computer systems.
- Wikipedia has suffered sporadic outages after its hosting server was hit by a Distributed Denial of Service (DDoS) attack. The attack continued for nearly three days, and caused the popular site to become unavailable in Europe, Africa and the Middle East.
- A new spam campaign is actively hitting Germany, delivering the destructive Ordinypt Wiper that pretends to be a ransomware. The wiper is delivered by an email PDF attachment that looks like a job application. The attached PDF is a disguised executable, which, once opened, will overwrite all of the victim's files with garbage content and display a ransomware-like message.

  Check Point SandBlast provides protection against this threat

- A new sextortion campaign is targeting Ireland, sending victims fake recordings of them watching illegal pornography to scare them into paying over $6,000 worth of Bitcoins. The victims are told that their computer has been infected with spyware, which helped to capture their camera and browser records.
- Entercom Communications, US radio station owner, has been hit with what appears to be ransomware attack. The incident disrupted their telephone and email communications, and other digital systems.
- A phishing operation that targeted at least 380 Universities in more than 30 countries has been delivering fraudulent requests to validate library account by entering login credentials to a spoofed URL. The activity has been associated with the Iranian-linked APT group Cobalt Dickens, which is known to target educational institutes and sell academic resources to customers in Iran.

VULNERABILITIES AND PATCHES

- A use after free vulnerability has been discovered in VBScript engine. A proof of concept exploiting this vulnerability through Internet Explorer was published, leading to execution of arbitrary code. Other vulnerabilities patched on Microsoft's Patch Tuesday are being exploited in the wild.

  Check Point IPS blade protects against these threats *(VBScript Engine Remote Code Execution (CVE-2019-1208); Microsoft Windows Common Log File System Driver Elevation of Privilege (CVE-2019-1214); Microsoft Windows Elevation of Privilege (CVE-2019-1215))*

- A vulnerability has been revealed in SIM cards that could allow remote attackers to grab SIM card data such as cell-tower location and other identifiers by sending a crafted SMS message. This flaw had been actively exploited by a private company that works with governments and was conducting surveillance on mobile phone users.

- NetCAT, a side-channel vulnerability discovered in Intel's CPU, may allow remote attackers to steal sensitive data from the cache of the processor. The vulnerability, tracked as CVE-2019-11184, could be triggered by crafted network packets sent to the targeted computer.

- Multiple security flaws have been found in D-Link and Comba Telecom WiFi routers that involve insecure storage of credentials. The flaws may allow attackers to change device settings, extract sensitive information, and perform Man in the Middle attacks.

THREAT INTELLIGENCE REPORTS

- A new report uncovers that in a Denial-of-Service attack that caused disruptions at a power utility in the United States a few months ago, the threat actors exploited a known vulnerability in the Firewall used by the utility, and as a result, some energy grid operations in California and two other states were disrupted.

- Researchers have revealed how some of the most popular period tracking apps used by millions of women share their personal health data with Facebook. The apps have been found to send their user-entered data to Facebook via its Software Developer Kit, whether the user is logged into her Facebook account or does not have an account at all.

- The recent activity of the China-linked APT group Thrip has been uncovered. The group is currently targeting entities in Southeast Asia, using both custom malware and legitimate tools. Their attacks have involved new backdoors dubbed "Hannotog", "Catchamas" and "Sagerunex". The latter may indicate that Thrip group is related to another China-linked threat group called Billbug (aka Lotus Blossom).

  Check Point Anti-Virus blade provides protection against this threat *(Backdoor.Win32.Sagerunex, Backdoor.Win32. Hannotog, Backdoor.Win32.Catchamas)*