Check Point
SOFTWARE TECHNOLOGIES LTD.

December 9 - 15, 2019

YOUR CHECK POINT
THREAT INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- Over 750,000 birth certificate applications have been exposed online after an unsecured Amazon S3 bucket was left online. The unsecured bucket belongs to a company that works for US State governments and manages the birth and death certificates.

- Rooster Teeth productions has suffered a data breach that allowed attackers to steal payment card and personal information from the company's online store. The attackers injected a malicious script to the checkout page that redirected users to a phishing page.

- Nearly half a million payment card details belonging to Turkish citizens are offered for sale in an underground market. The payment details were found to be related to top 10 Turkish banks, and included full card information, as well as cardholder name, email and phone number.

- Attackers are targeting Ring camera devices in a wave of recent attacks, using the hacked devices to talk to homeowners, play music and set off the alarm. Some of the hacks appear to be related to an online platform called NulledCast, which is promoting live-streams of hacked Ring and Nest cameras.

- City of New Orleans has bit hit by ransomware. Employees were asked to turn down their computers, and the City's servers, including its website, are down as well. Emergency services were left intact, although police has no access to the database.

- The city of Pensacola, Florida has been hit by ransomware, resulting in shutdown of their services and departments. The operators of Maze ransomware took responsibility for the attack, demanding $1 million. The operators also stated that they intentionally avoided emergency services in the attack.

  Check Point SandBlast provides protection against this threat (Ransomware.Win32.Maze)

- Another Maze ransomware attack has hit the wire and cable manufacturer Southwire. The operators demanded $6 million to decrypt the data, and threatened to publish it if the demands will not be met.

  Check Point SandBlast provides protection against this threat (Ransomware.Win32.Maze)

VULNERABILITIES AND PATCHES

- A new technique to hijack Intel CPU's SGX enclave memory has been discovered, and may allow local attackers to decrypt the sensitive data stored in the hardware-isolated trusted space. The technique, dubbed Plundervolt, allows corrupting the encryption algorithms used by SGX enclaves by tweaking the voltage delivered to a targeted CPU processor.
- Multiple flaws have been discovered in Siemens SPPA control systems that may allow attackers to trigger a denial-of-service condition or execute arbitrary code on vulnerable systems. Exploitation of these flaws may put in risk energy infrastructure and power plants where these systems are installed.
- A new flaw in iPhone, iPad, Mac and iPod devices has been addressed by Apple. The flaw, named AirDos, may allow a nearby attacker to make the device's UI unavailable by repetitively sending an AirDrop share request popup, which will continue appearing even after declining it or locking the device.

THREAT INTELLIGENCE REPORTS

- Check Point researchers have analyzed a packer called CypherIT, sold on the internet and used by attackers to obfuscate their malware and evade detection of Anti-Virus products. Check Point was able to decrypt this popular packer.

  Check Point SandBlast provides protection against this threat

- A highly-configurable ransomware dubbed Zeppelin has been observed by researchers, targeting tech and healthcare companies in Europe and the United States. Zeppelin, which was found to be a variant of the Vega ransomware, will not operate on machines located in Russia and ex-USSR countries.

  Check Point SandBlast provides protection against this threat

- PyXie, a new python-based Remote Access Trojan, is being used in campaigns targeting a wide range of industries. Experts observed it being deployed with Cobalt Strike beacons and evidence shows that PyXie was used to deliver ransomware to the healthcare and education industries.

  Check Point IPS and Anti-Bot blades provide protection against this threat *(Cobalt Strike Payload Remote Code Execution; Cobalt Strike Beacon Suspicious Communication; Backdoor.Win32.CobaltStrike; RAT.Win32.PyXie)*

- A new variant of Trickbot has been analyzed by researchers, targeting high-value targets for financial motives. The variant, named Anchor, was deployed in conjunction of a PowerShell-based malware attributed to the North-Korean Lazarus Group, which is known to pursue targets of financial sectors. The research suggests a possible collaboration between Lazarus and Trickbot operators.

  Check Point Anti-Virus and Anti-Bot blades provide protection against this threat *(Trojan-Banker.Win32.TrickBot)*