Aug 15 – 21, 2022

Check Point Research
WEEKLY INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- South Staffordshire Water, UK's largest water company supplying 330M liters of drinking water to 1.6M consumers daily, has been a victim of ransomware attack launched by Cl0p, a Russian-speaking ransomware gang. The group caused disruption of the company's IT systems, allowing them access to more than 5TB of data including passports, screenshots from water treatment SCADA systems, driver's licenses, and more. Although the ransomware gang claimed they could have easily altered the chemical composition of the water, the company confirms that the attack had no impact on water supply or the safety of drinking water.

  Check Point Harmony Endpoint provides protection against this threat (Ransomware.Win32.Clop)

- A Russian espionage group, APT 29 (aka Cozy Bear or Nobelium), has targeted Microsoft 365 accounts in NATO countries for cyberespionage purposes. The group has abused various Azure features and attempted to access foreign policy information.

- The LockBit ransomware group has claimed responsibility for the attack on cybersecurity vendor Entrust that occurred during June this year. As part of the attack, internal system files were stolen, while security products were not impacted. As LockBit started leaking data allegedly stolen from Entrust's network, the threat actors' leak site was taken down by a DDoS attack.

  Check Point Anti-Virus, Harmony Endpoint and Threat Emulation provide protection against this threat *(Ransomware.Win.Lockbit)*

- Ragnar Locker ransomware group has claimed the attack on The National Natural Gas System Operator (DESFA), a Greek company responsible for operating the country's natural gas system.

  Check Point Harmony Endpoint provides protection against this threat (Ransomware.Win32.Ragnarlocker)

- Argentina's Judiciary of Córdoba has been a victim of a ransomware attack that caused a shutdown of their IT systems and online portal, and employees had to use pen and paper for official documents. The attack was claimed by the Play ransomware group, which encrypts files and adds a '.play' extension to them. The judiciary calls the attack "worst attack on public institutions in history".

VULNERABILITIES AND PATCHES

- Apple has issued an urgent patch for two zero-day flaws actively exploited by attackers to hack iPhones, iPads, or Macs. Among them is CVE-2022-32893, an out-of-bounds write vulnerability in WebKit that would allow an attacker to perform arbitrary code execution, and CVE-2022-32894, an out-of-bounds write vulnerability in the operating system's kernel that would allow an attacker to execute code with kernel privileges.
- Amazon has patched a high-severity vulnerability in the Amazon Ring Android app that has over 10 million downloads. Successful exploitation could have allowed hackers to access Ring's APIs to extract users' sensitive personal information such as full name, emails, phone numbers, location and camera recordings.
- A zero-day vulnerability has been observed in General Bytes Bitcoin ATM servers, a purchases and sales platform of cryptocurrencies. Attackers have exploited this vulnerability to steal cryptocurrency from users.

THREAT INTELLIGENCE REPORTS

- Microsoft has disrupted ongoing phishing campaigns conducted by SEABORGIUM (aka TA446), a Russian state-sponsored threat group. The group's major motivation was espionage campaigns involving credential theft leading to intrusions and data theft.
- BlackByte ransomware gang has released version 2.0 of its dark web site, which includes new extortion techniques that allow victims to pay agreed upon amount of money for different purposes such as: extend the data publication by 24 hours, download the data and even remove it from the site.

  Check Point Harmony Endpoint and Threat Emulation provide protection against this threat (Ransomware.Win32.BlackByte)
- Researchers have observed a Banking Trojan dubbed Grandoreiro targeting organizations in Mexico and Spain. In this campaign, the threat actors impersonate Mexican Government Officials in the form of spear-phishing emails to lure victims to download and execute the Trojan. Grandoreiro utilizes techniques like binary padding to inflate binaries, Captcha implementation for sandbox evasion, and command-and-control (CnC) communication using patterns that are identical to LatentBot.

  Check Point Anti-Virus and Anti-Bot provide protection against this threat (Trojan-Banker.Win32.Grandoreiro; Trojan.Win32.LatentBot)