May 10-16, 2021

YOUR CHECK POINT

THREAT INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- Ireland's Health Services Executive (HSE), a provider of health and social services, among them Covid-19 vaccines, has suffered an attack by Conti ransomware, forcing it to shut down its IT systems. Vaccine appointments have not been affected, however other hospital services might be affected.

  Check Point SandBlast and Harmony Endpoint provide protection against this threat *(Ransomware.Win.Conti.*)*

- Reporters claim that Colonial Pipeline has paid a $5 million ransom. Researchers have determined that the DarkSide ransomware criminal group, probably from Russian origins, are behind the attack, rather than Russian state-sponsored groups. In parallel, the DarkSide gang announced it is shutting down its operations after its servers had been seized and its cryptocurrency funds, used to pay affiliates of the ransomware-as-a-service program, had been stolen.

- A spear-phishing campaign has been targeting travel and aerospace companies utilizing two RATs, RevengeRAT and AsyncRAT, deployed via a newly exposed malware loader. Spoofed email addresses are used in the phishing emails, as well as images posing as PDF files.

  Check Point Check Point Anti-Virus provides protection against these threats *(RAT.Win32.Revengerat; RAT.Win32.AsyncRat)*

- Rapid7 cybersecurity company has disclosed that parts of its source code, as well as data of its MDR customers, have been accessed by threat actors as part of the Codecov supply chain attack.

- The cybercrime gang FIN7, has been distributing a backdoor dubbed ‘Lizar’, disguised as a Windows pen-testing tool for ethical hackers. The group pretends to be a legitimate organization that offers an analysis tool for sale.

  Check Point Anti-Virus and Anti-Bot provide protection against these threats *(Ransomware.Win32.Fivehands; SombRAT)*

- Threat actors have been abusing Microsoft Build Engine, a platform used to build applications, to deliver RATs and password stealers filelessly in a currently active campaign. The malicious Microsoft Build files were embedded with executables and shellcode that deploy backdoors, enabling further information theft.

VULNERABILITIES AND PATCHES

- Multiple vulnerabilities in the Wi-Fi standard have been discovered by researchers. The vulnerability collection, dubbed 'FragAttacks', includes design flaws in the standard and therefore affect most devices using it, including multiple smart devices. Some of the flaws impact devices dating back to 1997.
- Microsoft has addressed some 55 security vulnerabilities in its latest update, among them four critical flaws. The vulnerability assigned CVE-2021-31166 in the HTTP Protocol, a wormable remote code execution flaw, could allow an unauthenticated threat actor to execute code as kernel.

  Check Point IPS provides protection against this threat (Microsoft HTTP Protocol Stack Remote Code Execution (CVE-2021-31166))
- Adobe has released a fix for vulnerabilities in Adobe Acrobat and Adobe Reader, including CVE-2021-28550, a use after free memory corruption flaw exploited in the wild that could allow remote code execution.

  Check Point IPS provides protection against this threat (Adobe Acrobat and Reader Use After Free (APSB21-29: CVE-2021-28550))
- Siemens has published fourteen security advisories, most of them address the 'Sad DNS' cache poisoning vulnerability in the Linux Kernel of third-party components. Tens of vulnerabilities reside in the UltraVNC and SmartVNC remote access tools.

THREAT INTELLIGENCE REPORTS

- The number of organizations affected by ransomware has more than doubled in 2021 so far compared to 2020, according to Check Point Research. Ransomware gangs have recently adopted a new attack technique dubbed 'triple extortion', in which a third-party impacted by the data breach is also extorted for ransom.
- Check Point Research has analyzed and enumerated over public AWS Systems Manager (SSM) documents, finding documents misconfigured to be publically shared containing over five million personally identifiable information records and credit card transactions of companies, including a global sportswear manufacturer.
- Check Point has released its Most Wanted Malware index for April 2021. Dridex remained the topmost prominent malware globally, while AgentTesla, a commodity RAT and info stealer, is in the second place.

  Check Point SandBlast and Anti-Bot provide protection against these threats (Trojan.Win32.AgentTesla; Banking.Win32.Dridex)
- Researchers have published a review of the DDoS attack landscape in Q1 2021. Two significant new botnets have emerged since the beginning of 2021, among them the FreakOut botnet, which infects Linux devices in order to launch DDoS attacks and cryptomining attacks.
- QNAP has alerted on threat actors' attempts to attack Network Attached Storage (NAS) and infect them with the eCh0raix ransomware, by exploiting a zero-day vulnerability in Roon management software server.

  Check Point Anti-Virus provides protection against this threat (Ransomware.Win32.Ech0raix)