cp<r>
CHECK POINT RESEARCH

WEEKLY INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- American blood donation center OneBlood has been a victim of a ransomware attack that caused disruption to its software system, affecting operations across more than 350 hospitals in Florida, Georgia, and the Carolinas. The attack has forced the organization to operate at reduced capacity and manually process blood donations, leading to inventory shortages.

- American pharmaceutical company Cencora has confirmed that a cyber-attack that occurred in February 2024 resulted in the exfiltration of sensitive personal and medical data, including PII and PHI, primarily maintained by a subsidiary providing patient support services. The company has notified potentially impacted individuals, but the exact number affected was not disclosed.

- The City of Columbus, Ohio has experienced a ransomware attack that resulted in the disruption of multiple city services and a potential access to sensitive city information. The Rhysida ransomware gang has claimed responsibility, threatening to leak 6.5TB of alleged data, including employee credentials, emergency services data, access to city cameras and more.

  Check Point Harmony Endpoint and Threat Emulation provide protection against this threat
  (Ransomware.Win.Rhysida; Ransomware.Wins.Rhysida)

- A Taiwanese government-affiliated research institute has been a victim of a data breach conducted by the Chinese state-sponsored group APT41. The attack involved the use of ShadowPad and Cobalt Strike malware to gain unauthorized access to research data and execute commands.

  Check Point Harmony Endpoint and Threat Emulation provide protection against this threat
  (Trojan.Wins.APT41.ta.; Trojan.Win.APT41; APT.Win.APT41; RAT.Wins.Shadowpad.*; RAT.Win.ShadowPad; Trojan.Wins.Cobaltstrike.tayc.*; Trojan.Wins.Cobaltstrike; Trojan.Win.Cobaltstrike)*

- Russian information security firm Avanpost has confirmed a cyber-attack that resulted in the encryption of over 400 virtual machines and physical workstations, the destruction of more than 60TB of data, and the leak of 390GB of valuable information. The attack was claimed by the pro-Ukrainian hacker group Cyber Anarchy Squad. The hackers shared some of the allegedly leaked data on Telegram and Mega, though the authenticity of this data has not been verified.

- HSA provider HealthEquity has suffered a data breach that led to the exposure of personal and protected health information of 4.3M individuals. The compromised data includes names, addresses, Social Security numbers, payment card details, medical data and more.

- World's largest silver producer Fresnillo PLC has disclosed a cyber-attack that led to unauthorized access to its IT systems and data. Despite the breach, business operations remain unaffected with no material operational or financial impact reported.

VULNERABILITIES AND PATCHES

- Check Point Research found that over 20K Ubiquiti cameras and routers are vulnerable to amplification attacks and privacy risks due to exposed UDP ports 10001 and 7004. This vulnerability, CVE-2017-0938, allows unauthorized access to sensitive device information, such as platform names and IP addresses, which can be exploited for both technical and social engineering attacks.

- Microsoft warns of active exploitation of VMware ESXi vulnerability, CVE-2024-37085, which allows ransomware groups to gain administrative access through an Active Directory integration authentication bypass. Ransomware gangs, including Storm-0506 and Storm-1175, have exploited this vulnerability to deploy ransomware such as Akira and Black Basta.

- Researchers have uncovered a critical ITW exploit of Proofpoint's email protection service, dubbed "EchoSpoofing", which allows attackers to send millions of perfectly spoofed phishing emails. This vulnerability bypasses SPF and DKIM authentication by leveraging Proofpoint's infrastructure, making emails appear as if they are from reputable brands such as Disney, Nike, IBM, and Coca-Cola.

THREAT INTELLIGENCE REPORTS

- Researchers have unveiled a sophisticated malvertising campaign exploiting social media platforms. Attackers hijack social media pages to mimic popular AI photo editor apps, and posting malicious links to bogus AI editor sites that trick users into downloading a compromised endpoint management utility. Payloads like Lumma Infostealer are executed, exfiltrating sensitive data, including cryptocurrency wallet files, browser data, and password manager databases.

  Check Point Harmony Endpoint and Threat Emulation provide protection against this threat
  (InfoStealer.Wins.Lumma.ta.; InfoStealer.Win.Lumma; Trojan.Wins.Lumma.ta.*; Trojan-Downloder.Win.Lumma)*

- Researchers have identified a rise in the abuse of TryCloudflare Tunnels for delivering remote access trojans (RATs). The attackers use Cloudflare tunnels to create temporary infrastructure, allowing them to remotely access data and resources without creating an account. The campaigns, observed from February to July 2024, involve URLs or attachments that execute scripts to download Python-based malware such as Xworm, AsyncRAT, VenomRAT, GuLoader, and Remcos.

  Check Point Harmony Endpoint and Threat Emulation provide protection against this threat (Worm.Wins.Xworm; Worm.Win.XWorm; RAT.Win.Asyncrat; RAT.Win.Asyncrat.glmw; RAT.Wins.AsyncRAT.ta.; RAT.Win.Venom; Dropper.Win.GuLoader; RAT.Win.Remcos; RAT.Wins.Remcos; RAT.Wins.Remcos.ta.*)*

- Researchers have discovered a large-scale, Android-targeted SMS stealer campaign active since February 2022, identifying over 107K malware samples. The malware tricks users into sideloading deceptive apps, which then exfiltrate SMS messages, including OTPs, by communicating with Command-and-Control servers via various evolving methods. This campaign has impacted victims in 113 countries, using over 2,600 Telegram bots and targeting over 60 global brands.

  Check Point Harmony Mobile provides protection against this threat