June 3 - 9, 2024

Check Point Research

WEEKLY INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- Pathology services provider Synnovis has experienced a ransomware attack that affected procedures and operations in several major hospitals in London, including the Department of Health and Social Care, NHS England. Qilin (formerly Agenda) ransomware gang claimed responsibility for the attack.

  Check Point Threat Emulation provides protection against this threat *(Ransomware.Win.Agenda; Ransomware.Wins.Qilin)*

- Social media giant TikTok has been a victim of a cyber-attack that targeted high-profile TikTok accounts. Threat actors exploited a zero-day vulnerability in the TikTok's direct messages feature, that enabled zero click account takeovers. Victims include notable accounts like CNN and Sony. The number of affected accounts, attackers' identity and the exact malware details remain unknown.

- The New York Times has been a victim of a cyber-attack that resulted in the leakage of its internal source code and data from the company's GitHub repositories. The stolen data consists of approximately 270GB of files, including IT documentation, infrastructure tools, and more. According to the company, the attack did not affect its internal systems or operations.

- Disney Confluence server was allegedly hacked by the fans of the online game Club Penguin, what led to exfiltration of 2.5GB of internal corporate data. The stolen data includes outdated Club Penguin documents and recent Disney corporate information, such as internal developer tools, strategies, and credentials. Disney has not yet confirmed the breach.

- Dallas-based telecommunications company Frontier Communications has confirmed a ransomware attack in April that impacted the personal information of more than 750K US residents. RansomHub ransomware gang claimed responsibility for the attack.

  Check Point Threat Emulation provides protection against this threat *(Ransomware.Wins.RansomHub.ta.*)*

- Web-based service Clarity.fm has disclosed a data breach that resulted in the leakage of approximately 155K records including personal and business email addresses, payment details, and more. 121K member profiles were affected, including users belong to Mark Cuban, Eric Ries and Brad Field.

- Eye Care Leaders, a provider of performance solutions for the eye care industry, confirmed an event of unauthorized access of its databases. The breach affected several client practices, exposing confidential information such as patient names, contact details, and health insurance information.

VULNERABILITIES AND PATCHES

- PHP patched a new RCE vulnerability in PHP for Windows, CVE-2024-4577. The flaw impacts all versions since 5.x and allows unauthenticated attackers to bypass previous protections, including those for CVE-2012-1823, to execute arbitrary code through a CGI argument injection attack.

  Check Point IPS provides protection against this threat *(PHP CGI Argument Injection (CVE-2024-4577))*

- Progress Software has released updates to fix a critical vulnerability in Telerik Report Server that allows remote attackers to bypass authentication and create rogue administrator accounts. The flaw, CVE-2024-4358, carries a CVSS score of 9.8 and affects versions up to 2024 Q1.

  Check Point IPS provides protection against this threat *(Progress Telerik Report Server Remote Code Execution)*

- Zyxel has issued security patches for critical command injection and remote code execution vulnerabilities found in End-of-Life models of Zyxel NAS devices. Exploiting some of these vulnerabilities, CVE-2024-29972-6, could potentially allow the execution of operating system commands through a crafted HTTP POST request.

THREAT INTELLIGENCE REPORTS

- Check Point Research provides an overview of BoxedApp products and reveals their abuse for malicious purposes. The research includes an in-depth analysis of the relevant packed binary structures with Yara signatures that can be used to statically detect the malicious use of the packer.

- Researchers dived into a new ransomware variant called Fog, which mostly targets the education sector in the US. The ransomware exploits compromised VPN credentials for access and deploy tools like PsExec, focusing on encrypting VMDK files and disabling Windows Defender.

- Researchers have identified a new Linux malware variant used by TargetCompany ransomware group to specifically target ESXi environments. Among this malware capabilities, it uses a custom shell script to download and execute the payload and sends victim information to two servers for data redundancy.

  Check Point Threat Emulation provides protection against this threat *(Ransomware.Wins.TargetCompany)*

- Researchers revealed a new campaign using fake browser updates to deceive users into downloading and executing malicious payloads. This campaign delivers BitRAT and Lumma Stealer, focusing on credential and cryptocurrency theft.

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