Cybersecurity Report

Since the beginning of the calendar year, Palo Alto Networks has detected an uptick in Maze ransomware samples across multiple industries. As a result, we've created this general threat assessment post on the Maze ransomware activities and full visualization of these techniques can be viewed in the Unit 42 Playbook Viewer. Maze ransomware, a variant of ChaCha ransomware, was first observed in May 2019 and has targeted organizations in North America, South America, Europe, Asia, and Australia. This ransomware is typically distributed via emails containing weaponized Word or Excel attachments. However, it has also been distributed via exploit kits such as the Spelevo Exploit Kit, which has been used with Flash Player vulnerabilities CVE-2018-15982 and CVE-2018-4878. Maze ransomware has also utilized exploits CVE-2019-11510 (Pulse VPN), as well as CVE-2018-8174 (Internet Explorer) to get into a network. The malware first establishes a foothold within the environment. It then obtains elevated privileges, conducts lateral movement, and begins file encryption across all drives. However, before encrypting the data, these operators may exfiltrate the files to be used for further coercion, including public exposure. Without the proper protections in place, a Maze ransomware infection will cripple normal business operations, and sensitive information will be compromised, resulting in a monetary loss. Maze has not only been observed globally, but also affecting varying industries, which include: finance, technology, telecommunications, healthcare, government, construction, hospitality, media and communications, utilities and energy, pharma and life sciences, education, insurance, wholesale, and legal. On March 26, 2020, McAfee published a report providing a detailed overview of the Maze ransomware. Palo Alto Networks Cortex XDR contains an Anti-Ransomware Protection module, which targets encryption-based activities associated with ransomware. Customers can also review activity associated with this Threat Brief via AutoFocus. Recently, malicious operators behind the Maze ransomware activities compromised multiple IT service providers. These operators were also able to establish a foothold within another victim's network through insecure Remote Desktop Protocol and other remote service connections or by brute-forcing the local administrator account. Organizations should be mindful of potential compromises through third-party sources and ensure strong passwords are used for all systems capable of remote access. It was also reported that Maze operators pay special attention to cloud backups on the compromised network. If the operators were to obtain login credentials, they are then able to download all backup data to an actor controlled server. Organizations should ensure that all cloud backup files are properly stored and protected.