Feds Warn Healthcare Sector

Emerging Threat Alert: Akira Ransomware Targets Healthcare and Beyond

Federal authorities have issued a warning to the healthcare sector regarding the emerging threat posed by the Akira ransomware-as-a-service group. This group, which has only been active for approximately six months, has already been linked to several dozen attacks, primarily targeting small and mid-sized organizations across various industries. Akira appears to favor organizations lacking multifactor authentication (MFA) on their virtual private networks (VPNs), employing double-extortion attacks that involve data theft and ransomware encryption. Their methods include leveraging compromised credentials, exploiting VPN vulnerabilities, deploying phishing emails, malicious websites, drive-by downloads, and trojans. Researchers have identified similarities between Akira and the disbanded Conti ransomware group, including code overlap and encryption techniques.

While Akira targets encompassed sectors such as finance, real estate, and manufacturing they have recently shifted their focus to the healthcare industry. In their double-extortion approach, Akira exfiltrates an organization's data before encryption and threatens to publicly release sensitive information unless a ransom is paid. They also offer a lower-cost option to prevent the publication of especially sensitive data. Ransom payment demands by Akira have ranged from $200,000 to $4 million. Despite the availability of a free decryptor for Akira ransomware, the group's attacks have continued to evolve, with recent reports indicating increased threat activity targeting Cisco ASA SSL VPN appliances. Implementing MFA is crucial in mitigating such attacks, as many incidents result from weak or compromised credentials due to the absence of MFA enforcement. Health and Human Services Health Sector Cybersecurity Coordination Center recommends additional cybersecurity measures, including regular system updates, account lockout policies, network segmentation, and robust incident response planning.

The CRITICAL**START**® Cyber Research Unit will continue to monitor the situation and work closely with the SOC and Security Engineering team to implement any relevant detections. For future updates the CTI team will post updates via Cyber Operations Risk & Response™ Bulletins and on the CRITICAL**START**® Intelligence Hub.

References:

1. https://www.inforisktoday.com/feds-warn-healthcare-sector-akira-ransomware-threats-a-23073
2. https://www.hhs.gov/sites/default/files/akira-ransomware-sector-alert-tlpclear.pdf