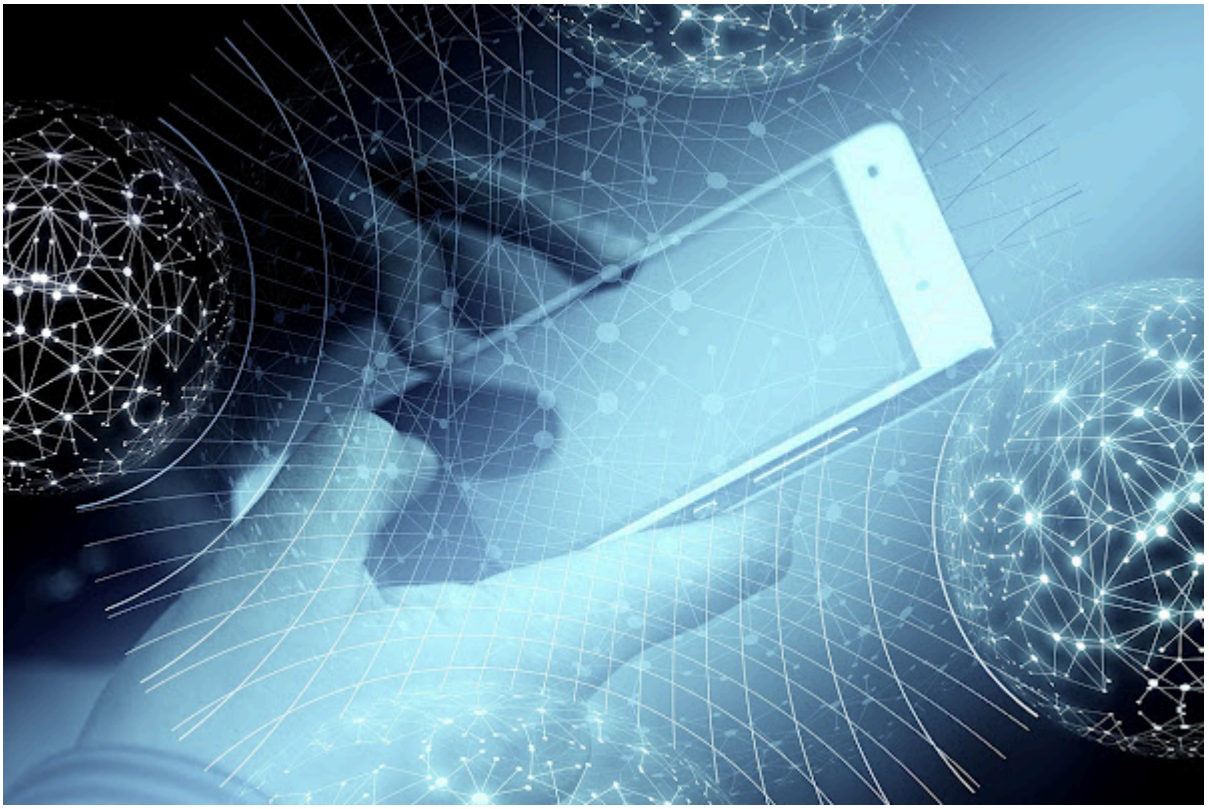
CySecurity News - Latest Information Security and Hacking Incidents: Twisted Spider's Dangerous CACTUS Ransomware Attack

By CySecurity News, twitter.com/ehackernews



In a sophisticated cyber campaign, the group Twisted Spider, also recognized as Storm-0216, has joined forces with the cybercriminal faction Storm-1044. Employing a strategic method, they target specific endpoints through the deployment of an initial access trojan known as DanaBot.

Subsequently, Twisted Spider leverages this initial access to execute the deployment of the CACTUS ransomware. Recent insights from Microsoft Threat Intelligence on X shed light on Storm-0216's tactics. Operating under aliases such as Twisted Spider or UNC2198, this ransomware entity employs an advanced banking Trojan, Danabot. This intricate pairing of cyber threats showcases the evolving and complex nature of Twisted Spider's malicious endeavors.

Additionally, the security researchers highlighted the adaptive tactics of Storm-0216, which was previously recognized for utilizing QakBot's infrastructure for infections. However, following the dismantling of this operation by law enforcement last summer, the group was compelled to pivot to a different platform.

The latest Danabot campaign, initially identified in November, indicates a notable shift. Unlike the previous malware-as-a-service model, the group appears to be using a private version of the info-stealing malware. Microsoft explained that DanaBot, known for providing hands-on keyboard activity to its partners, has undergone a transformation in its deployment strategy.

This shift underscores the group's remarkable adaptability and capacity to evolve tactics, particularly in response to interventions by law enforcement. The ability to navigate and adjust strategies highlights the dynamic nature of cyber threats and the constant cat-and-mouse game between cybercriminals and those working to counteract their activities.

Let’s Understand the Method of the Attack

Upon obtaining the essential login credentials, the Storm-1044 group initiates lateral movement across the network and various endpoints through Remote Desktop Protocol (RDP) sign-in attempts. Once the initial access has been secured, the baton is passed to Twisted Spider. Subsequently, Twisted Spider proceeds to compromise the endpoints by introducing the CACTUS ransomware.

What is CACTUS Ransomware?

CACTUS is emerging as a preferred option among numerous ransomware operators. Recently, Arctic Wolf researchers cautioned that hackers exploited three vulnerabilities in the Qlik Sense data analytics solution to deploy this specific variant, facilitating the theft of sensitive company data.

Why it is More Threatening?

In May, researchers at Kroll made a noteworthy discovery regarding the ransomware's evasion tactics. Laurie Iacono, Associate Managing Director for Cyber Risk at Kroll, revealed that CACTUS employs a unique method to bypass cybersecurity measures—it essentially encrypts itself. This self-encryption mechanism enhances its ability to evade detection, posing challenges for antivirus and network monitoring tools, as highlighted by Iacono in discussions with Bleeping Computer.

Source: https://www.cysecurity.news/2023/12/twisted-spiders-dangerous-cactus.html