BlackCat ransomware hits Azure Storage with Sphynx encryptor

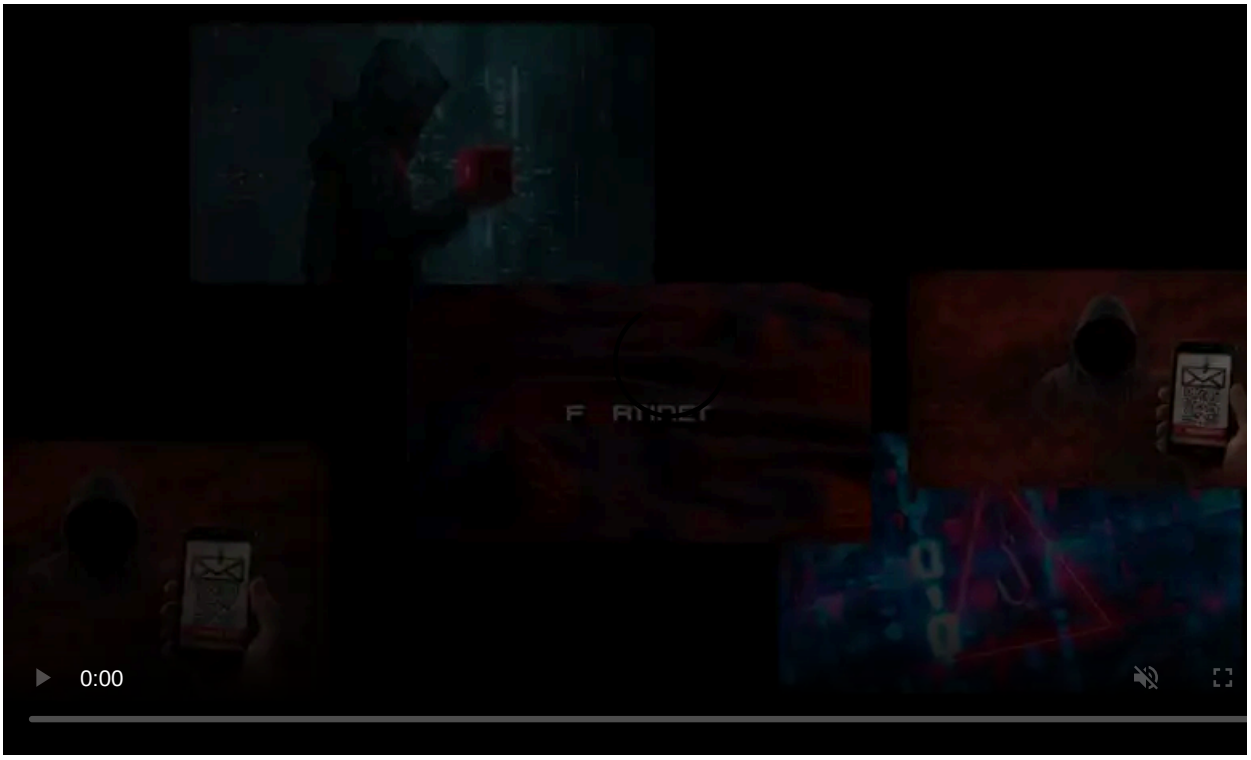
By Sergiu Gatlan

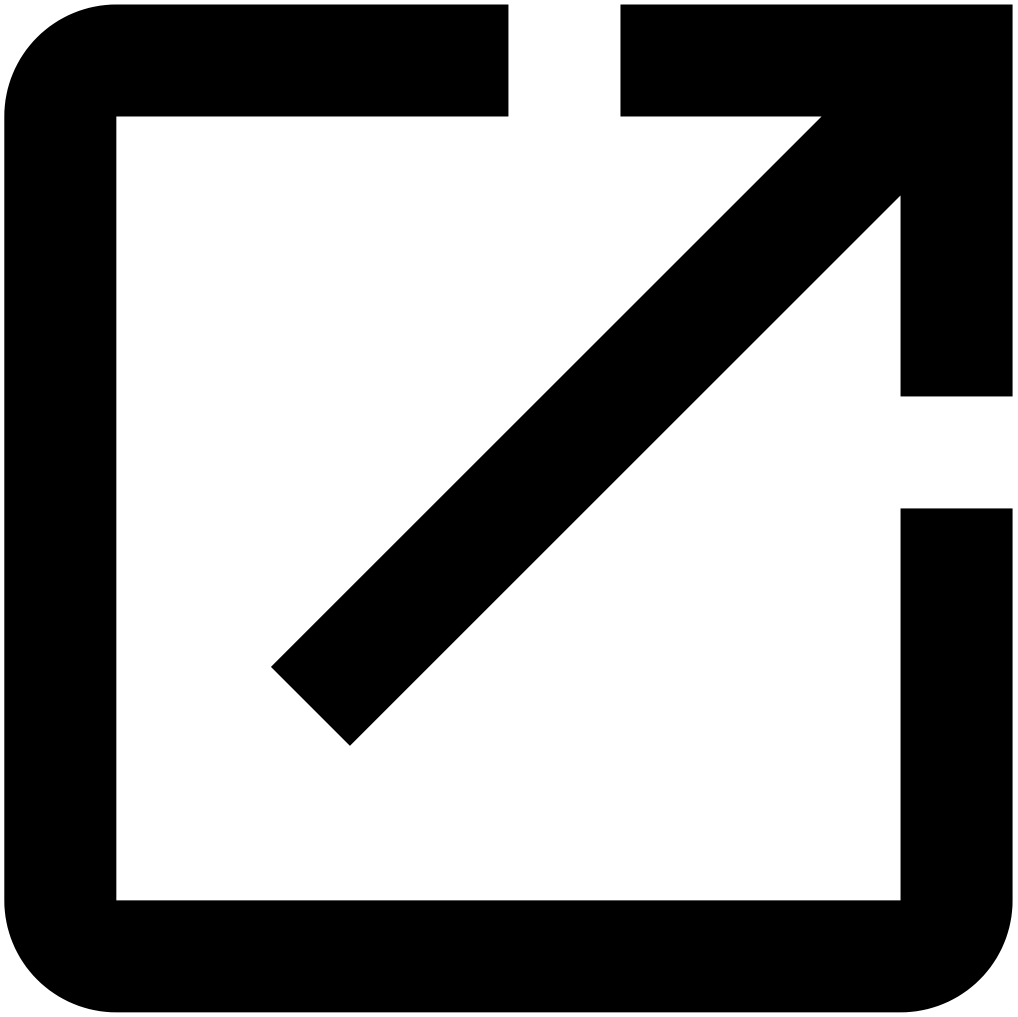
Published: 2023-09-16 · Archived: 2026-04-05 20:49:18 UTC

Image: Midjourney

The BlackCat (ALPHV) ransomware gang now uses stolen Microsoft accounts and the recently spotted Sphynx encryptor to encrypt targets' Azure cloud storage.

While investigating a recent breach, Sophos X-Ops incident responders discovered that the attackers used a new Sphynx variant with added support for using custom credentials.


0:00



After gaining access to the Sophos Central account using a stolen One-Time Password (OTP), they disabled Tamper Protection and modified the security policies. These actions were possible after stealing the OTP from the victim's LastPass vault using the LastPass Chrome extension.

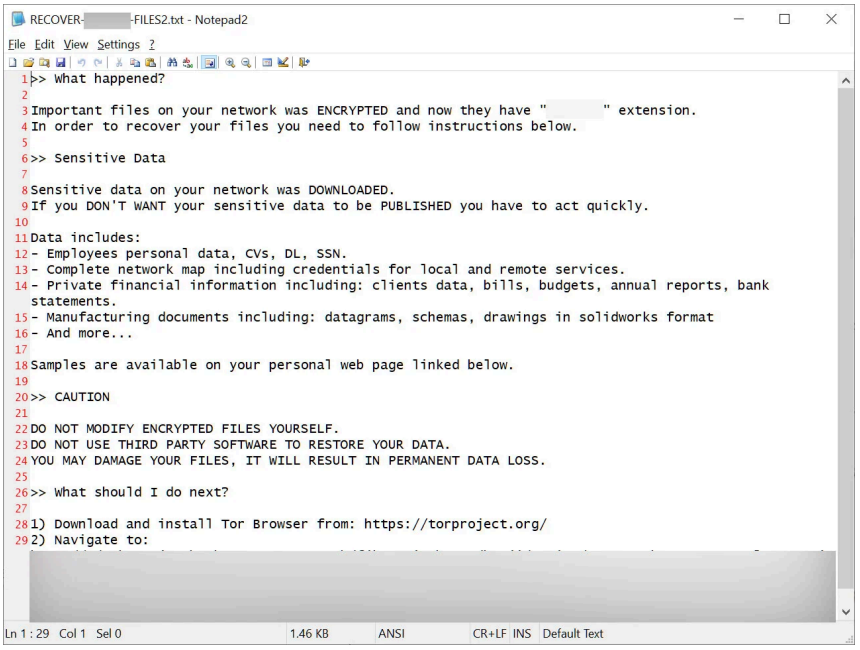
Subsequently, they encrypted the Sophos customer's systems and remote Azure cloud storage and appended the .zk09cvt extension to all locked files. In total, the ransomware operators could encrypt 39 Azure Storage accounts successfully.

They infiltrated the victim's Azure portal using a stolen Azure key that provided them access to the targeted storage accounts. The keys used in the attack were injected within the ransomware binary after being encoded using Base64.

The attackers also used multiple Remote Monitoring and Management (RMM) tools like AnyDesk, Splashtop, and Atera throughout the intrusion.

Sophos discovered the Sphynx variant in March 2023 during an investigation into a data breach that shared similarities with another attack described in an IBM-Xforce report published in May (the ExMatter tool was used to extract the stolen data in both instances).

Microsoft also found last month that the new Sphynx encryptor is embedding the Remcom hacking tool and the Impacket networking framework for lateral movement across compromised networks.



BlackCat ransom note sample

As a ransomware operation that emerged in November 2021, BlackCat/ALPHV is suspected to be a DarkSide/BlackMatter rebrand.

Known initially as DarkSide, this group garnered global attention after breaching Colonial Pipeline, drawing immediate scrutiny from international law enforcement agencies.

Although they rebranded as BlackMatter in July 2021, operations were abruptly halted in November when authorities seized their servers and security firm Emsisoft developed a decryption tool exploiting a vulnerability in the ransomware.

This gang has consistently been recognized as one of the most sophisticated and high-profile ransomware outfits that targets enterprises on a global scale, continuously adapting and refining its tactics.

For instance, in a new extortion approach last summer, the ransomware gang used a dedicated clear web website to leak the stolen data of a specific victim, providing the victim's customers and employees with the means to determine whether their data had been exposed.

More recently, BlackCat introduced a data leak API in July designed to streamline the dissemination of stolen data.

This week, one of the gang's affiliates gang (tracked as Scattered Spider) claimed the attack on MGM Resorts, saying they encrypted over 100 ESXi hypervisors after the company took down its internal infrastructure and refused to negotiate a ransom payment.

Last April, the FBI issued a warning highlighting that the group was behind the successful breaches of more than 60 entities worldwide between November 2021 and March 2022.

Source: https://www.bleepingcomputer.com/news/security/blackcat-ransomware-hits-azure-storage-with-sphynx-encryptor/