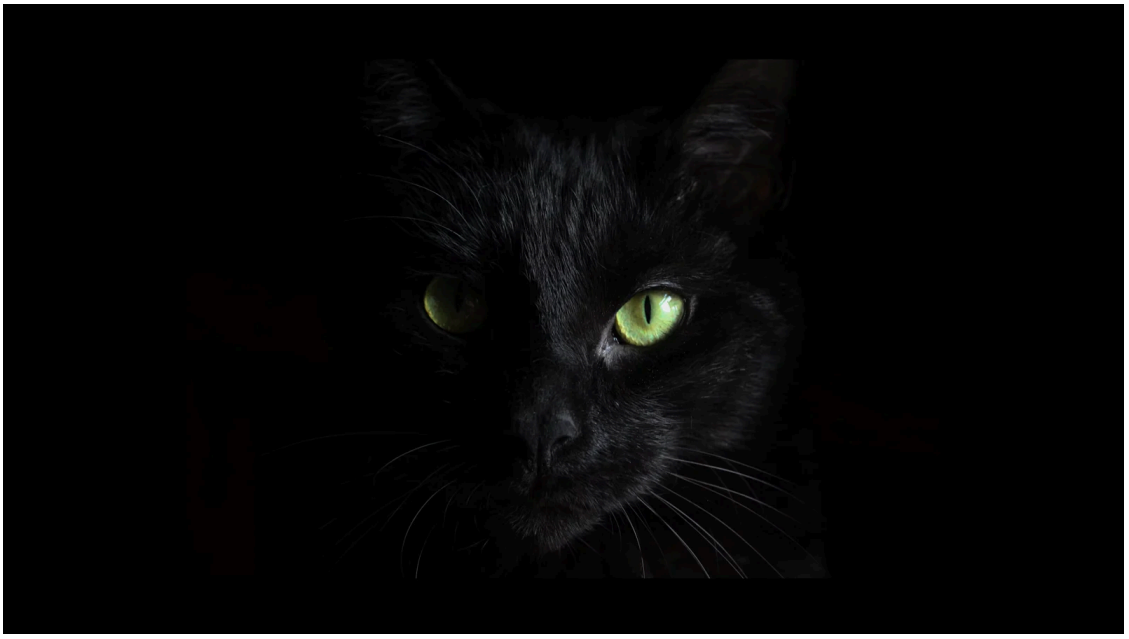
Microsoft: BlackCat's Sphynx ransomware embeds Impacket, RemCom

By Lawrence Abrams

Published: 2023-08-17 · Archived: 2026-04-05 12:40:52 UTC

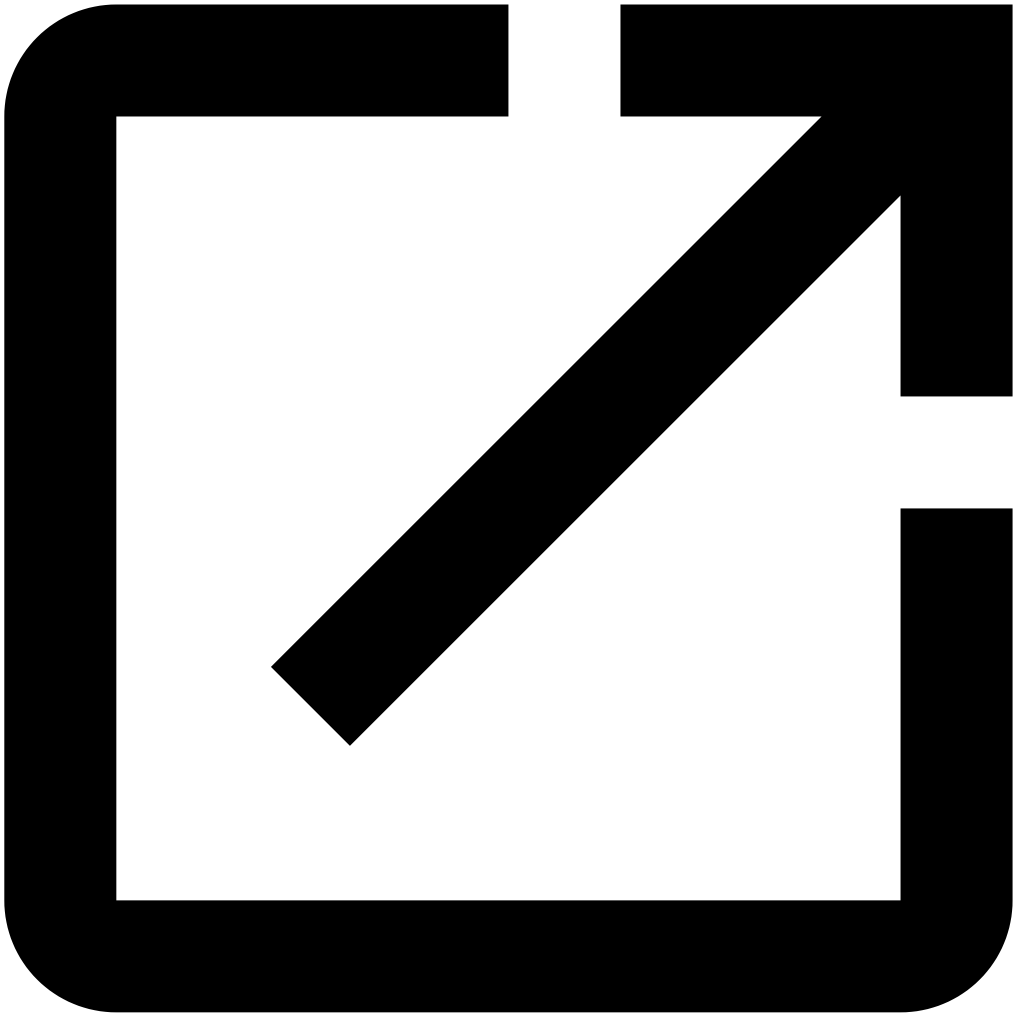


Microsoft has discovered a new version of the BlackCat ransomware that embeds the Impacket networking framework and the Remcom hacking tool, both enabling spreading laterally across a breached network.

In April, cybersecurity researcher VX-Underground tweeted about a new BlackCat/ALPHV encryptor version called Sphynx.

"We are pleased to inform you that testing of basic features ALPHV/BlackCat 2.0: Sphynx is completed," said the BlackCat operators in a message to their affiliates.


DIE LINKE.
0:00



"The code, including encryption, has been completely rewritten from scratch. By default all files are frozen. The main priority of this update was to optimize detection by AV/EDR," further explained the ransomware operations.

Soon after, IBM Security X-Force performed a deep dive into the new BlackCat encryptor, warning that the encryptor evolved into a toolkit.

This was based on strings in the executable that indicated it contained impacket, used for post-exploitation functions such as remote execution and dumping secrets from processes.

```
Launch embedded python module, contains impacket examples such as [smbexec, psexec,
atexec, secretsdump and etc…]
```

Impacket strings found by IBM X-Force
Source: IBM

The BlackCat Sphynx encryptor

In a series of posts today, the Microsoft's Threat Intelligence team says they have also analyzed the new Sphynx version and found that it used the Impacket framework to spread laterally on compromised networks.

"Microsoft has observed a new version of the BlackCat ransomware being used in recent campaigns," posted Microsoft.

"This version includes the open-source communication framework tool Impacket, which threat actors use to facilitate lateral movement in target environments."

Impacket is described as an open-source collection of Python classes for working with network protocols.

However, it is more commonly used as a post-exploitation toolkit by penetration testers, red teamers, and threat actors to spread laterally on a network, dump credentials from processes, perform NTLM relay attacks, and much more.

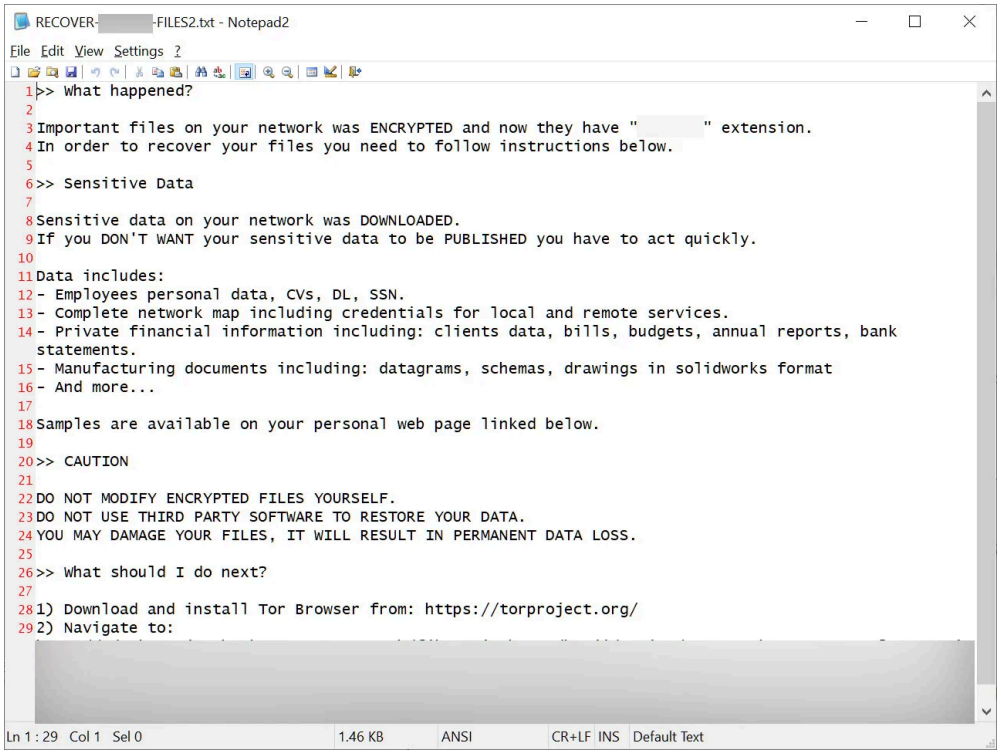
Impacket has become very popular among threat actors who breach a device on a network and then use the framework to obtain elevated credentials and gain access to other devices.

According to Microsoft, the BlackCat operation is using the Impacket framework for credential duping and remote service execution to deploy the encryptor across an entire network.

In addition to Impacket, Microsoft says that the encryptor embeds the Remcom hacking tool, which is a small remote shell that allows the encryptor to remotely execute commands on other devices on a network.

In a private Microsoft 365 Defender Threat Analytics advisory seen by BleepingComputer, Microsoft says they saw this new encrypted used by BlackCat affiliate 'Storm-0875' since July 2023.

Microsoft is identifying this new version as BlackCat 3.0, even though, as we previously said, the ransomware operation calls it 'Sphynx' or 'BlackCat/ALPHV 2.0' in communications with affiliates.



Sample of a BlackCat ransom note

An ever-evolving ransomware gang

BlackCat, aka ALPHV, launched its operation in November 2021 and is believed to be a rebrand of the DarkSide/BlackMatter gang, which was responsible for the attack on Colonial Pipeline.

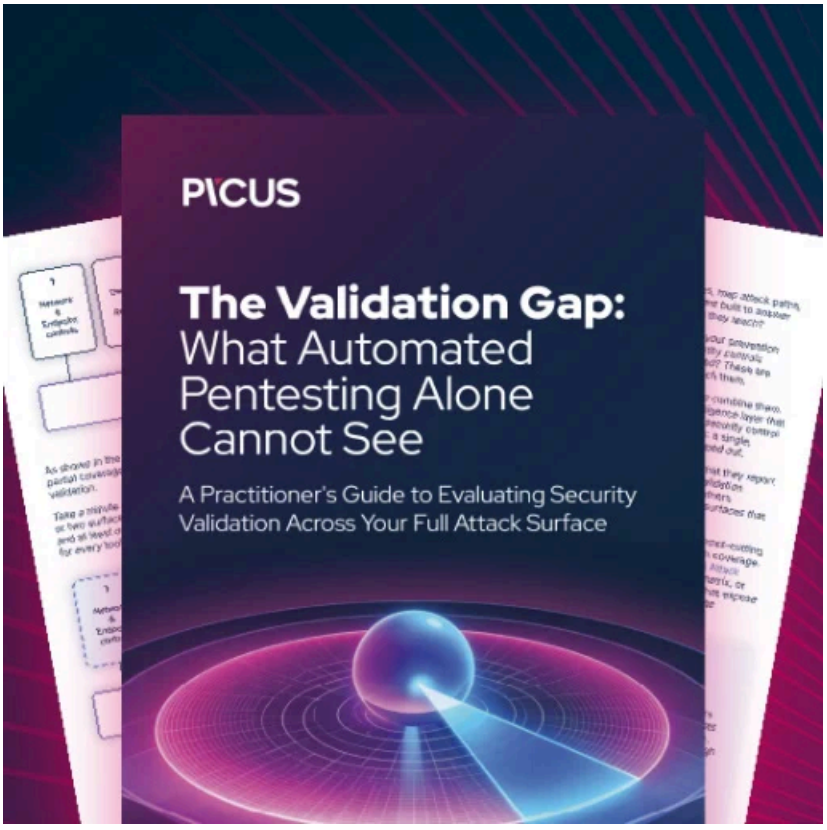
The ransomware gang has always been considered one of the most advanced and top-tier ransomware operations, constantly evolving its operation with new tactics.

For example, as a new extortion tactic last summer, the ransomware gang created a clearweb website dedicated to leaking data for a particular victim, so customers and employees could check if their data was exposed.

More recently, the threat actors created a data leak API, allowing for easier dissemination of stolen data.

With the BlackCat encryptor evolving from a decryptor to a full-fledged post-exploitation toolkit, it allows the ransomware affiliates to more quickly deploy file encryption across the network

As it is vital to detect ransomware attacks as soon as they occur, adding these tools only makes it harder for defenders.



Automated Pentesting Covers Only 1 of 6 Surfaces.

Automated pentesting proves the path exists. BAS proves whether your controls stop it. Most teams run one without the other.

This whitepaper maps six validation surfaces, shows where coverage ends, and provides practitioners with three diagnostic questions for any tool evaluation.

Source: https://www.bleepingcomputer.com/news/microsoft/microsoft-blackcats-sphynx-ransomware-embeds-impacket-remcom/