Fenix24: Rapid, No-Downtime Recovery from Incomplete Ransomware Encryption

Exploiting Encryption Flaws for Faster Data Recovery

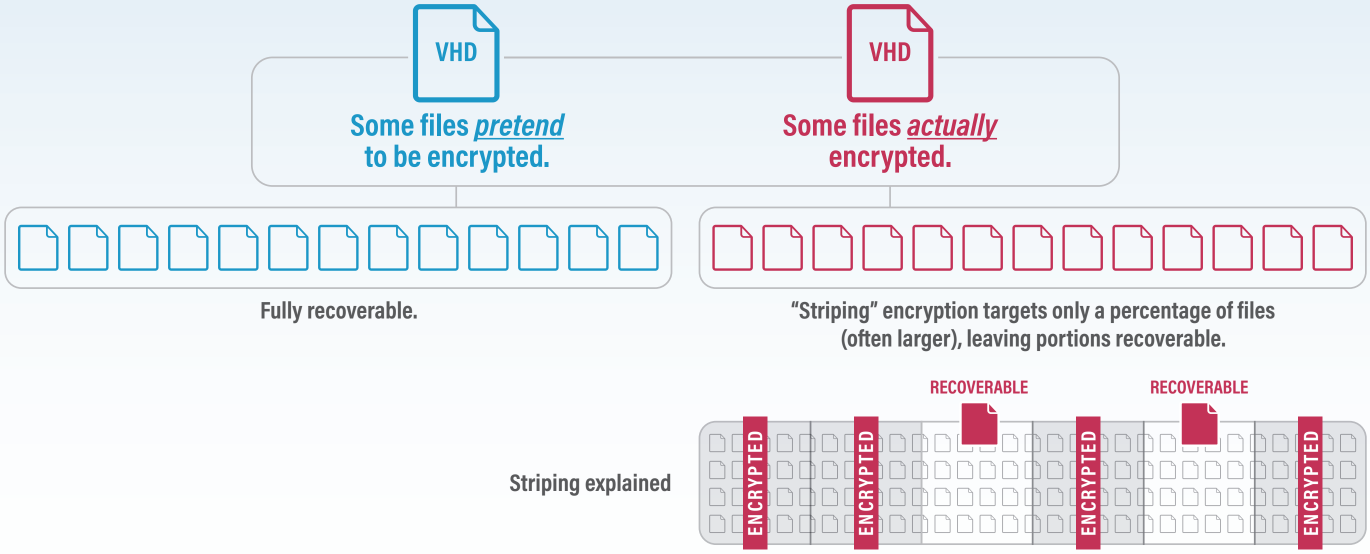
Recent insights from Fenix24's ransomware engagements have exposed critical flaws in the encryption techniques used by threat actors such as Akira, Abyss Locker, LockBit 3.0, Rhysida, BlackSuit, Donut Leaks, and BlackBasta. These weaknesses present significant opportunities for faster, more complete data recovery, and our team has already seen success in restoring files that other experts considered irrecoverable.

Threat actors are increasingly adopting less sophisticated, efficiency-driven encryption techniques, including:

- **PARTIAL ENCRYPTION:** Only the first few bytes of a file are encrypted, deliberately targeting minimal components. This allows us to recover most of the file data.
- **STRIPED ENCRYPTION:** A small percentage of the file is encrypted at random, corrupting access but still allowing data recovery from the unencrypted portions.
- **MOCK ENCRYPTION:** Files are renamed with an encrypted suffix without action, which may be intentional or due to a fault, leaving the data accessible.

These and other tactics are designed to quickly lock systems while minimizing the time spent on each target, creating gaps that can be exploited by skilled recovery experts.

VM: PRESENTED AS "FULLY ENCRYPTED"



Some files *pretend* to be encrypted.

Some files *actually* encrypted.

Fully recoverable.

"Striping" encryption targets only a percentage of files (often larger), leaving portions recoverable.

Striping explained

Our understanding of how Threat Actors attempt to mask "full encryption" allows us to do faster, more complete restoration.

Disaster Recovery Hotline: 1.855.FENIX24, option2 rapidresponse@fenix24.com

A CONVERSANT GROUP COMPANY

Fenix24: Rapid, No-Downtime Recovery from Incomplete Ransomware Encryption

FENIX24®
A CONVERSANT GROUP COMPANY

CASE STUDY:

Restoring 600+ VMs After Ransomware Attack

A client faced a ransomware attack that encrypted more than 600 virtual machines (VMs). Previous experts using conventional methods deemed the data unrecoverable, but **Fenix24 was able to identify that the VMs continued running**, indicating partial or superficial encryption. By leveraging deep technical expertise, **the Fenix24 team restored all the client's VMs without purchasing a decryption key or causing any downtime**—something even the client's cloud and virtualization provider told them was impossible.

> *When we were hit with a ransomware attack, multiple restoration providers told us our data was irretrievable. Fenix24 stepped in and turned everything around. They recovered our critical files and SQL databases within days. Their expertise saved our business from a catastrophic loss.*
>
> — CISO

See If We Can Help: Shoulder-Surf with Fenix24

Experiencing a ransomware attack? Before taking further steps, let Fenix24 provide a second opinion at no cost to you. Our experts can shoulder-surf with your team to assess if our recovery techniques can be applied to your situation.

Take immediate action:

1. Disconnect from the internet. Don't reboot or shut down your systems.
2. If you're using vSAN and still have access to your clusters, don't make any changes. Your data might still be recoverable.
3. Contact Fenix24 immediately. Our team is ready to assist.

For more information or to schedule a consultation,
CONTACT FENIX24 1.855.FENIX24, option2 rapidresponse@fenix24.com