B

BlackCat (ALPHV) Ransomware: Incident Response

What it is BlackCat, also called ALPHV or Noberus, is a ransomware operation known for encrypting Windows and Linux systems and stealing data for extortion. The name can refer to both the ransomware payload and the criminal affiliate...

PUBLISHER
Gridinsoft Support

UPDATED
Jul 17, 2026

READ TIME
2 min

What it is

BlackCat, also called ALPHV or Noberus, is a ransomware operation known for encrypting Windows and Linux systems and stealing data for extortion. The name can refer to both the ransomware payload and the criminal affiliate operation behind attacks. It has targeted organizations rather than relying only on indiscriminate consumer infections.

How it works

Affiliates may gain access through stolen credentials, exposed remote services, phishing, or previously compromised accounts. They then map the network, escalate privileges, collect sensitive data, weaken defenses, and deploy ransomware across servers and endpoints.

Virtualization infrastructure can be targeted because encrypting a host can disrupt many workloads at once.

Key points

- Unusual remote-management tools, bulk archive creation, and access to hypervisors can precede encryption.
- Data theft creates legal and notification obligations even when backups restore operations.
- The criminal infrastructure and branding may change, while techniques and affiliates continue under other names.

What to do

- Isolate affected network segments without destroying volatile evidence needed for investigation.
- Disable compromised identities, rotate privileged credentials, and review identity-provider logs.
- Protect backup systems from the compromised domain before beginning recovery.
- Coordinate incident response, legal, insurance, and required reporting through an established plan.

Focus on behavior, not only the family name

Ransomware brands, infrastructure, and affiliate relationships can change, while the defensive priorities remain stable. Preserve the ransom note, extension, executable, authentication logs, and evidence of data transfer. Isolate affected segments, disable compromised remote access, protect backup credentials, and rotate privileged accounts before restoration. Determine whether data left the network even if encryption was limited. Do not assume a matching family label guarantees a safe decryptor. Use the ransomware response guide to sequence containment, legal and notification review, clean rebuilding, and tested recovery.

NEED MORE HELP?

We are here when the guide is not enough.

Visit the Gridinsoft Support Center for current product guidance or submit a support request with the details of your case.

Open this guide online at support.gridinsoft.com