

S

Snake Malware: The FSB cyberespionage implant explained

What it is Snake is a sophisticated cyberespionage malware framework attributed by several national cybersecurity authorities to a unit of Russia's Federal Security Service, or FSB. It was used for long-term intelligence collection from...

PUBLISHER

Gridinsoft Support

UPDATED

Jul 17, 2026

READ TIME

1 min

What it is

Snake is a sophisticated cyberespionage malware framework attributed by several national cybersecurity authorities to a unit of Russia's Federal Security Service, or FSB. It was used for long-term intelligence collection from high-value government, research, media, and critical-infrastructure targets. This definition refers to that implant, not every unrelated threat named Snake.

How it works

The framework creates a covert peer-to-peer network among compromised systems. Traffic can be relayed through other infected hosts, making the final operator harder to locate. Snake supports commands, data collection, and resilient communications, and was engineered to remain on selected systems for extended periods.

Key points

- Snake is a targeted espionage tool, not ordinary consumer ransomware or a generic Python package with the same word.
- Peer-to-peer relays mean blocking one external server may not remove communications across compromised hosts.
- Attribution and eradication require evidence beyond a filename or an alert containing the word Snake.

What to do

- Preserve memory, disk, and network evidence and involve experienced incident responders.
- Identify every affected host and peer relationship before removing individual components.
- Rotate credentials and inspect trusted administrative paths reachable from compromised systems.
- Apply current government and vendor detection guidance appropriate to the affected environment.

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](https://support.gridinsoft.com)