S

Snake Malware (Uroburos): FSB Implant, Operation MEDUSA, and Response

Snake malware can mean the FSB Uroburos espionage implant, Snake Keylogger, or Snake/EKANS ransomware. Learn how to distinguish them and respond to the correct family.

PUBLISHER
Gridinsoft Support

UPDATED
Aug 19, 2026

READ TIME
5 min

CONTENTS

In this guide

Snake, also known as **Uroburos**, is a sophisticated cyber-espionage implant attributed by a 2023 joint government advisory to Center 16 of Russia's Federal Security Service (FSB). The implant created a covert peer-to-peer network used for long-term access, relay traffic, and theft of sensitive information from selected targets.

"Snake malware" is ambiguous. It can also refer to Snake Keylogger or Snake/EKANS ransomware, which are unrelated families. Confirm the full detection name and behavior before following response guidance.

01 Which Snake malware does an alert mean?

Name	Primary purpose	Typical context
Snake / Uroburos FSB implant	Long-term espionage, remote access, covert P2P relaying, and document theft.	Highly selected government, research, diplomatic, media, and other strategic targets; Windows, Linux, and macOS versions have been documented.
Snake Keylogger / 404 Keylogger	Commodity credential theft, keylogging, screenshots, and data theft.	Windows phishing and malware-as-a-service campaigns.
Snake ransomware / EKANS	Encrypts files and disrupts organizations for extortion.	Human-operated ransomware incidents; may affect local and network resources.

These names do not indicate a shared codebase or operator. A ransomware note, a .NET keylogger alert, and the Uroburos implant require different scoping and recovery.

02 How the FSB Snake implant worked

According to the joint advisory, development began under the Uroburos name in the early 2000s. Snake was engineered for stealth and long-term intelligence collection. Compromised computers could act as both final collection targets and unwitting relay nodes in a custom encrypted P2P network.

The design helped operators route commands and stolen data through multiple infected systems, obscuring the path back to the operator. Additional tools, including keylogging capability, could be deployed alongside the implant. Versions and host components changed over many years to evade research and detection.

03 Operation MEDUSA in 2023

On May 9, 2023, the U.S. Department of Justice announced a court-authorized operation that used an FBI-created tool named PERSEUS to issue built-in commands causing Snake implants to overwrite vital components and disable themselves. Partner governments coordinated actions outside the United States.

The operation disrupted the Snake network, but it did not patch the initial access route, search for every additional tool, or undo credential and document theft. An organization notified of a past infection still needs a full incident investigation.

04 What defenders should look for

- A detection or victim notification specifically referencing the FSB Snake implant, Uroburos, or the 2023 joint advisory.
- Host artifacts, kernel components, or network protocol patterns documented in current government and vendor intelligence.
- Long-lived unexplained access, encrypted peer-to-peer traffic, or a system acting as a relay without a business purpose.
- Keylogger, credential theft, or other Turla-related tools present alongside the implant.
- Use of stolen credentials after the apparent Snake component was disabled.

Do not hunt using only the word "snake." Common filenames, security-tool test artifacts, and the unrelated families above can generate misleading results. Use the technical indicators and detection logic for the correct family and version.

05 Response to a suspected FSB Snake compromise

1. **Escalate as a targeted intrusion.** Involve organizational incident response, legal and executive contacts, and the relevant national cybersecurity authority where appropriate.
2. **Isolate carefully.** Preserve volatile and network evidence while stopping unauthorized communications. Assume more than one host or tool may be involved.
3. **Collect evidence.** Acquire memory and disk images where feasible, host telemetry, authentication history, network flows, DNS, firewall, proxy, VPN, email, and administrative records.
4. **Scope beyond the named implant.** Search for initial access, keyloggers, credential use, persistence, lateral movement, collection, staging, and exfiltration across all supported platforms.
5. **Protect credentials from clean systems.** Change exposed credentials to entirely new values, revoke sessions and keys, and protect privileged and service accounts with phishing-resistant MFA.
6. **Rebuild confirmed systems.** Use trusted media and baselines rather than relying only on removal of one implant component.
7. **Patch and harden the entry paths.** Update operating systems and applications and correct the weaknesses identified by the investigation.
8. **Assess data exposure.** Determine which documents, mailboxes, credentials, and communications were accessible and meet notification obligations.

06 If the alert is Snake Keylogger

Isolate and rebuild the infected Windows device, then change passwords used or stored there from a clean system. Revoke sessions, protect email and financial accounts first, and search for the phishing message, loader, and other recipients. A keylogger infection is serious but does not by itself establish an FSB Snake intrusion.

07 If the alert is Snake ransomware

Activate the ransomware plan: isolate affected systems and shares, preserve evidence, protect identity and backup infrastructure, determine the intrusion scope, rebuild systems, and restore from protected backups. Do not use Uroburos indicators to assess an EKANS incident.

08 Prevention

- Patch operating systems, internet-facing services, VPNs, and administrative tools.
- Separate user, server, management, backup, and sensitive research or operational networks.
- Use phishing-resistant MFA and dedicated systems for privileged administration.
- Monitor outbound and east-west traffic for unusual peer relationships and long-lived encrypted connections.
- Keep centralized, tamper-resistant logs and tested endpoint response capability for Windows, Linux, and macOS.
- Prepare for credential theft even when the initial malware detection appears to have been remediated.

09 Frequently asked questions

Is Snake malware still active after Operation MEDUSA?

The 2023 action disabled identified implants and disrupted the P2P network. It should not be interpreted as a permanent guarantee against new tools, rebuilt infrastructure, or residual access through stolen credentials.

Is Snake the same as Turla?

Turla is a name used for the threat actor or activity set; Snake/Uroburos is one malware platform associated with it.

Does a Snake Keylogger alert mean a state-sponsored attack?

No. Snake Keylogger is a separate commodity information stealer used by many actors. Validate the exact detection and infection chain.

10 References

- Joint advisory: Hunting Russian Intelligence Snake Malware
- U.S. Department of Justice: Operation MEDUSA
- Australian Cyber Security Centre: Snake advisory
- FortiGuard: Snake Keylogger distinction
- Microsoft: Snake/EKANS ransomware