



NSA/CSS

[HOME](#) > [PRESS ROOM](#) > [PRESS RELEASES & STATEMENTS](#) > [PRESS RELEASE VIEW](#)



PRESS RELEASE | May 9, 2023

U.S. Agencies and Allies Partner to Identify Russian Snake Malware Infrastructure Worldwide

FORT MEADE, Md. - The National Security Agency (NSA) and several partner agencies have identified infrastructure for Snake malware—a sophisticated Russian cyberespionage tool—in over 50 countries worldwide.

To assist network defenders in detecting Snake and any associated activity, the agencies are publicly releasing the joint Cybersecurity Advisory (CSA), “Hunting Russian Intelligence “Snake” Malware” today.

The agencies, which include the NSA, Federal Bureau of Investigation (FBI), Cybersecurity and Infrastructure Security Agency (CISA), Cyber National Mission Force (CNMF), Canadian Cyber Security Centre (CCCS), United Kingdom National Cyber

[Skip to main content \(Press Enter\).](#)

Cyber Security Centre (CSCC), United Kingdom National Cyber Security Centre (NCSC-UK), Australian Cyber Security Centre (ACSC), and New Zealand National Cyber Security Centre (NCSC-NZ) attribute Snake operations to a known unit within Center 16 of Russia's Federal Security Service (FSB). The international coalition has identified Snake malware infrastructure across North America, South America, Europe, Africa, Asia, and Australia, including the United States and Russia.

"Russian government actors have used this tool for years for intelligence collection," said Rob Joyce, NSA Director of Cybersecurity. "Snake infrastructure has spread around the world. The technical details will help many organizations find and shut down the malware globally."

Malicious cyber actors used Snake to access and exfiltrate sensitive international relations documents, as well as other diplomatic communications, through a victim in a North Atlantic Treaty Organization (NATO) country.

In the U.S., the FSB has victimized industries including education institutions, small businesses, and media organizations. Critical infrastructure sectors, such as local government, finance, manufacturing, and telecommunications, have also been impacted.

Typically, Snake malware is deployed to external-facing infrastructure nodes on a network. From there, it uses other tools, and techniques, tactics, and procedures (TTPs) on the internal network to conduct additional exploitation operations.

This CSA focuses on one of the more recent variants of Snake. It provides background on Snake's attribution to the FSB and detailed technical information and mitigation recommendations to assist network defenders in protecting against Snake-associated malicious activity.

[Visit our full library for more cybersecurity information and technical guidance.](#)

NSA Media Relations
MediaRelations@nsa.gov
443-634-0721



SHARE



PRINT

Related Press Advisories

**NCSC-UK, NSA, and Partners Advise about APT28
Exploitation of Cisco Routers**














**CISA, FBI, NSA, and International Partners Issue Advisory on
Demonstrated Threats and Capabilities of Russian State-
Sponsored and Cyber Criminal Actors**

**NSA and FBI Expose Russian Previously Undisclosed
Malware “Drovorub” in Cybersecurity Advisory**

**NSA CISA, FBI, and the UK NCSC further expose Russian
Intelligence Cyber Tactics**

Related Documents

CSA: Hunting Russian Intelligence “Snake” Malware

 cybersecurity  CISA  FBI  csa  FSB  russia  malware
 mitigation  network  Cyber  cyberespionage  tool 
snake