DROVORUB MALWARE | Fact Sheet & FAQs

Fact Sheet

GRU GTsSS facts:

- Malicious cyber activity by Russian General Staff Main Intelligence Directorate (GRU) 85th Main Special Service Center (GTsSS) is sometimes publicly associated with APT28, Fancy Bear, Strontium, and a variety of other identities as tracked by the private sector.
- The GTsSS cyber program uses a wide variety of proprietary and publicly known techniques to target networks and to persist their malware on compromised devices.

Drovorub details:

- Drovorub is a Linux malware developed for use by the GTsSS. When deployed on a victim machine, Drovorub provides the capability for direct communications with actor-controlled command and control infrastructure; file download and upload capabilities; execution of arbitrary commands; port forwarding of network traffic to other hosts on the network; and implements hiding techniques to evade detection.
- As part of NSA's mission to detect threats to National Security Systems (NSS), the Department of Defense (DoD), and the Defense Industrial Base, and to share information about those threats, NSA is sharing details about Drovorub and related detection/mitigation techniques to enable network defenders to identify and degrade malware activity.
- NSA and FBI are sharing this information to counter the capabilities of the GRU

NSA's Cybersecurity Advisories mission:

- NSA releases Cybersecurity Advisories that contain actionable, unique, and timely guidance and information.
- NSA pursues public attribution, in coordination with our USG and FVEYs partners, when it provides the threat intelligence context needed to ensure that system owners will take action.

FBI's mission:

- The FBI has dual responsibilities as a law enforcement and intelligence agency. Our mission is to protect the American people and uphold the Constitution of the United States.
- As we conduct investigations in the cyber space, our aim is to impose risks and consequences on cyber adversaries through our unique authorities, world-class capabilities, and enduring partnerships, building on a century of innovation.
- In fulfilling our mission, attribution is critical to determining how to best impose risks and consequences on cyber adversaries. Unique information gathered and analyzed by the FBI helps attribute malicious cyber activity to the responsible parties, which can in turn trigger additional tools, techniques, and authorities at the disposal of the U.S. Government in stopping these malicious actors.

Frequently Asked Questions (FAQs)

Why did NSA and FBI release this guidance now?

We're sharing this information with our customers and the public to counter the capabilities of the GRU GTsSS, an organization which continues to threaten the United States and its allies. We continuously seek to counter their ability to exploit our Nation's critical networks and systems.

Will the mitigations outlined in the guidance protect my system from exposure?

Implementing SecureBoot in "full" or "thorough" mode should reliably prevent malicious kernel modules, such as the

Drovorub kernel module, from loading. This will prevent Drovorub from being able to hide itself on a system. The other detection and mitigation options, such as Snort and Yara rules, will naturally have a limited lifetime, as they are expected to be the first things changed in future versions of the malware to avoid detection. They should be used as quickly as possible before changes are made.

How did you find out about this malware?

We use a variety of means and methods to acquire information about cyber threats, including our own cybersecurity operations, foreign signals intelligence, U.S. Government partners, engagement with industry, and foreign partners around the world. We don't comment on the source of any particular information so we can continue to fulfil our vital role for the nation. Protecting our sources also allows us to more broadly release the underlying threat information in ways we might not be able to otherwise do.

Can you tell me more about GtsSS? Have you seen indications that they are responsible for other nefarious cyber activities?

The GTsSS cyber program uses a wide variety of proprietary and publicly known techniques to target networks and to persist their malware on commercial devices. For more details, we encourage you to review the CSA.

Have the GTsSS been using this malware for other activities (like for criminal/espionage purposes)?

We are aware that the GTsSS cyber program is a very capable organization that conducts its operations in accordance with GRU mission in the context of the Russian Intelligence Services.

Are there other threat actors using this malware?

We have no reason to believe other threat actors are currently using this malware. That said, now that it is disclosed, you can be sure adversaries will seek to employ similar tools and techniques, so we hope all stakeholders will take action to defend against it.

Are you working with other agencies to prevent this malware from being spread further?

We collaborate closely across the USG and our foreign partners to both raise awareness of cyber threats and provide mitigations guidance as needed. The power of our partnerships is exemplified in the very nature of our dual-seal release, which allows NSA and FBI to bring our unique strengths to bear in a more comprehensive and actionable product.