NSA and FBI warn that new Linux malware threatens national security

reader comments

83 with 55 posters participating, including story author

Share this story

The FBI and NSA have issued a joint report warning that Russian state hackers are using a previously unknown piece of Linux malware to stealthily infiltrate sensitive networks, steal confidential information, and execute malicious commands.

In a report that’s unusual for the depth of technical detail from a government agency, officials said the Drovorub malware is a full-featured tool kit that has gone undetected until recently. The malware connects to command and control servers operated by a hacking group that works for the GRU, Russia’s military intelligence agency that has been tied to more than a decade of brazen and advanced campaigns, many of which have inflicted serious damage to national security.

“Information in this Cybersecurity Advisory is being disclosed publicly to assist National Security System owners and the public to counter the capabilities of the GRU, an organization which continues to threaten the United States and U.S. allies as part of its rogue behavior, including their interference in the 2016 US Presidential Election as described in the 2017 Intelligence Community *Assessment, Assessing Russian*

Activities and Intentions in Recent US Elections (Office of the Director of National Intelligence, 2017)," officials from the agencies wrote.

Stealthy, powerful, and full featured

The Drovorub toolset includes four main components: a client that infects Linux devices; a kernel module that uses rootkit tactics to gain persistence and hide its presence from operating systems and security defenses; a server that runs on attacker-operated infrastructure to control infected machines and receive stolen data; and an agent that uses compromised servers or attacker-control machines to act as an intermediary between infected machines and servers.

A rootkit is a type of malware that burrows deep inside an operating system kernel in a way that prevents the interface from being able to register the malicious files or the processes they spawn. It uses a variety of other techniques as well to make infections invisible to normal forms of antivirus. Drovorub also goes to great lengths to camouflage traffic passing into and out of an infected network.

The malware runs with unfettered root privileges, giving operators complete control of a system. It comes with a full menu of capabilities, making a malware equivalent of a Swiss Army knife.

Security driver slayer

Government officials said Drovorub gets its name from strings unintentionally left behind in the code. "Drovo" roughly translates to "wood" or "firewood," while "rub" translates to "fell" or "chop." Put together, the government said, Drovorub means "woodcutter" or to "split wood." Dmitri Alperovitch, a security researcher who has spent most of his career

investigating Russian hacking campaigns—including the one that targeted the DNC in 2016—offered a different interpretation.

"Re: malware name 'Drovorub,' which as @NSACyber points out translates directly as 'woodcutter,'" Alperovitch, a co-founder and former CTO of security firm CrowdStrike, wrote on Twitter. "However, more importantly, 'Drova' is slang in Russian for 'drivers,' as in kernel drivers. So the name likely was chosen to mean "(security) driver slayer."

> *Re: malware name "Drovorub", which as @NSACyber points out translates directly as "woodcutter"*
>
> *However, more importantly, "Drova" is slang in Russian for "drivers", as in kernel drivers. So the name likely was chosen to mean "(security) driver slayer" https://t.co/yToULwp3xw*
>
> *— Dmitri Alperovitch (@DAlperovitch) August 13, 2020*

Serving Russia's national interests for more than a decade

Drovorub adds to an already abundant cache of previously known tools and tactics used by APT 28, the Russian military hacking group that other researchers call Fancy Bear, Strontium, Pawn Storm, Sofacy, Sednit, and Tsar Team. The group's hacks serve Russian government interests and target countries and organizations the Kremlin considers adversaries.

In August, Microsoft reported that the group had been hacking printers, video decoders, and other so-called Internet-of-things devices and using them as a beachhead to penetrate the computer networks they were connected to. In 2018, researchers from Cisco's Talos group uncovered APT 28's infection of more than 500,000 consumer-grade routers in 54 countries that could

then be used for a range of nefarious purposes.

Other campaigns tied to APT 28 include:

Thursday's advisory didn't identify the organizations Drovorub is targeting or provide even broad descriptions of the targets or geographies where they're located. It also didn't say how long the malware has been in the wild, how many known infections there have been to date, or how the hackers are infecting servers. APT 28 often relies on malicious spam or phishing attacks that either infect computers or steal passwords. The group also exploits vulnerabilities on devices that haven't been patched.

Required reading

Agency officials said that a key defense against Drovorub is to ensure that all security updates are installed. The advisory also urged that, at a minimum, servers run Linux kernel version 3.7 or later so that organizations can use improved code-signing protections, which use cryptographic certificates to ensure that an app, driver, or module comes from a known and trusted source and hasn't been tampered with by anyone else.

"Additionally, system owners are advised to configure systems to load only modules with a valid digital signature making it more difficult for an actor to introduce a malicious kernel module into the system," the advisory stated.

Also included are rules that network administrators can plug in to the Yara and Snort intrusion detection systems to catch and halt network traffic passing to or from control servers or to flag obfuscated Drovorub files or processes already running on a server.

The 45-page document provides a level of technical detail and informed analysis that's on par with some of the best research

from private companies. The advisory is also the first to disclose the existence of this new and advanced malware. Those are things that are rarely available in government advisories. The report should be required reading for anyone managing a network.

https://arstechnica.com/?p=1698939