



NEWS WEATHER TRAFFIC SPORTS THE DAILY J PODCASTS CONNECT LISTEN



NEWS
China launches
high-tech aircraft...



NEWS
Freedom riders' 1947
convictions vacate...



NEWS
Alabama church
shooting kills 2,...



NEWS
GOP, Dem Senate
bargainers divided...

WWJ NEWSRADIO 950 NEWS NATIONAL

US secretly removed malware from networks around the world



Photo credit Getty Images

[View Guide](#)

1:30pm

6:30pm

WWJ Newsradio 950

WWJ Newsradio 950

Aired 1:30pm To 6:30pm GMT+9:30

Live On-Air

[Minimize Player](#)



NEWS

WEATHER

TRAFFIC





SPORTS

THE DAILY J

PODCASTS

CONNECT

LISTEN

 <div>NEWS China launches high-tech aircraft...</div>	 <div>NEWS Freedom riders' 1947 convictions vacate...</div>	 <div>NEWS Alabama church shooting kills 2,...</div>	 <div>NEWS GOP, Dem Senate bargainers divided...</div>
---	--	---	---



Attorney General Merrick Garland on Wednesday said the Justice Department disrupted a global botnet -- a network of computers used to carry out cyberattacks -- controlled by the Russian military intelligence agency, commonly known as the GRU.

"We were able to disrupt this botnet before it could be used. Thanks to our close work with international partners, we were able to detect the infection of thousands of network hardware devices," Garland said in a statement. "We were then able to disable the GRU's control over those devices before the botnet could be weaponized."

While the intended purpose of the malware is unknown, it could have been used for anything from surveillance to destructive attacks, The New York Times reported. The Russian government has reportedly used similar infrastructure recently to attack Ukrainian targets.

Garland said the action, along with numerous sanctions, sends a message to those who continue to enable the Russian regime.

"It does not matter how far you sail your yacht. It does not matter how well you conceal your assets. It does not matter how cleverly you write your malware or hide your online activity. The Justice Department will use every available tool to find you, disrupt your plots, and hold you accountable," he said.

The move comes as U.S. officials warn that Russia could try to strike American critical infrastructure in response to sanctions that the U.S. has imposed on Moscow. Last month, the Biden administration issued new warnings that Russia may be planning a cyberattack. The president urged businesses to invest in cybersecurity measures, saying they have a "patriotic obligation" to defend their systems against such attacks.

The White House said there was no intelligence suggesting a specific Russian cyberattack against U.S. targets, but that there has been increase in "preparatory activity," like scanning websites and hunting for vulnerabilities, that is common among nation-state hackers, the Associated Press reported.

One of the most common ways Russian state actors could access U.S. computer networks by launching so-called "brute force attacks" to decode encryption and gain access to computer networks. Phishing attacks -- emails that convince the computer user to click on malicious links, giving hackers an entrance -- could also be used.

"When you think about how connected our world is and how much rely on the automated systems for our day to day lives to provide us power, to provide us clean water, that's very scary," Johnathan Mell, Operations and Marketing Strategist at St. Louis-based Q-Net Security, told KMOX.

RELATED



What American companies need to know about potential cyberattacks from Russia

RELATED



Russian retreat reveals destruction as Ukraine asks for help

[National News](#)

[Audacy News](#)

[Ukraine](#)

[Russia](#)

[Ukraine Russia Conflict](#)

[Cyberattack](#)

[Cybersecurity](#)

[Malware](#)

1000){r=r.substring(0,r.length-1);return r;})(); var ttDomain = (window==top)?"":(function(){var

1:30pm

View Guide

6:30pm

WWJ Newsradio 950

WWJ Newsradio 950

Aired 1:30pm To 6:30pm GMT+9:30

Live On-Air

Minimize Player