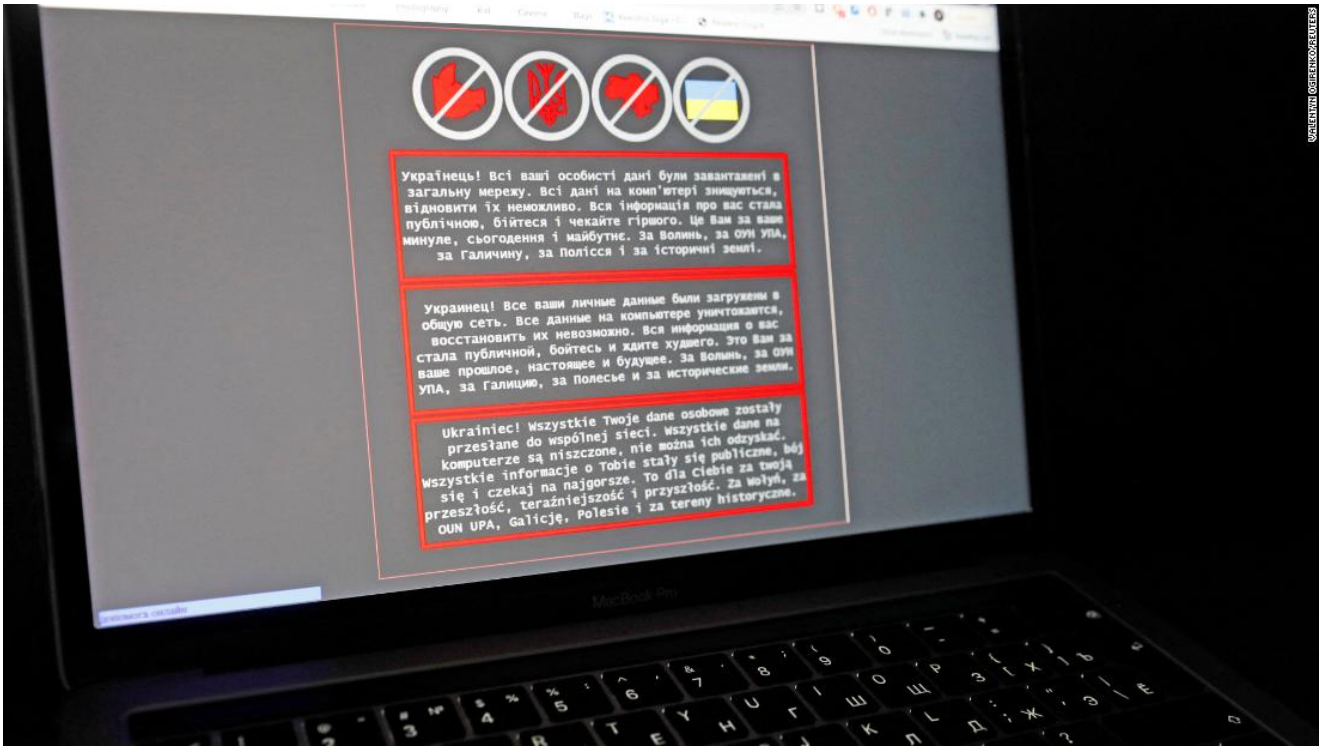
US officials prepare for potential Russian cyberattacks as Ukraine standoff continues

edition.cnn.com/2022/02/02/politics/fbi-ukraine-cyber-russia/index.html

February 2, 2022



*Washington (CNN)*The FBI is asking US businesses to report any uptick in Russian hacking threats -- the latest effort to prepare for potential Russian cyberattacks on US organizations amid Russia's troop buildup on Ukraine's border.

"Have you identified any efforts by known or suspected Russian [hacking groups] to test exploitation capabilities, develop new malware or otherwise prepare for cyber operations?" the FBI asked in a January 21 request for information to US businesses obtained by CNN. The FBI told US firms to email the bureau if they had found "any increased [cyber] activity against Ukraine or US critical infrastructure," including against financial, health care and energy companies.

It's just one of a series of quiet preparations that US officials have made to guard against any potential hacking threats from the Kremlin should the US levy heavy sanctions on Russia for a renewed invasion of Ukraine.

Vladimir Putin says the West has 'ignored' Russia's key concerns over Ukraine

There haven't been any reports of specific, significant Russian hacking threats to US infrastructure. But US officials aren't taking that for granted -- given the history of Russian cyber campaigns against US organizations, including an effort a few years ago to breach energy and water firms.

Read More

At least one previous Russian cyberattack in Ukraine has had global ramifications.

A 2017 cyberattack that the Justice Department blamed on Russian military intelligence began by infecting a Ukrainian software provider, but spread around the world, causing billions of dollars of damage.

Now, US officials are watching closely in case any US response to Russia's military build-up portends an increase in the digital threats facing US organizations.

"We have the weather forecast [of potential Russian cyber threats]," a US official told CNN. "Now we're trying to see if there will be any inclement weather in the form of actual cyber incidents."

In addition, top White House cyber official Anne Neuberger is in Europe this week to talk with US allies about how to support Ukraine in the event of Russian cyberattacks.

Russia knows that "disabling or destroying critical infrastructure" through cyberattacks can pressure another country into "ceding to Russian objectives," Neuberger told reporters Wednesday. "We've been working closely with Ukrainians to harden their defenses and will continue to do so in the days ahead."

Lessons from past Russian hacking

White House and federal agencies charged with cybersecurity have been on heightened alert, with officials checking in with critical infrastructure firms regularly. The departments of Energy and Treasury, and the US Cybersecurity and Infrastructure Security Agency, have in recent weeks held a series of briefings for industry executives on Russian hacking capabilities.

While US officials say they are unaware of any credible and specific Russian hacking threats to the US homeland, they have told US businesses and state and local governments how that could change.

Russia would consider conducting a cyberattack on the US homeland if Moscow perceived that a US or NATO response to a potential Russian invasion of Ukraine "threatened [Russia's] long-term national security," the Department of Homeland Security said in a January 23 intelligence bulletin first reported by CNN.

DHS analysts, however, assessed that Moscow's threshold for conducting disruptive or destructive cyberattacks on the US homeland "probably remains very high."

Call between top US and Russian diplomats doesn't ratchet down Ukraine tensions

The government is, to some degree, reliant on private companies to report emerging hacking threats because those companies own and operate the majority of US critical infrastructure.

The concern among US officials has long been that Russian hackers could gain a foothold into industrial networks that, for example, help distribute electricity or provide other critical services.

In 2018, DHS accused Russian government-backed hackers of engaging in a multi-year effort to infiltrate US energy, water and manufacturing firms. In some case, the hackers took screenshots of sensitive industrial computer systems that help operate machinery.

US critical infrastructure operators have in recent years grown more aware of the threat and invested more in cyber defenses as Russian hacking groups have stayed active around the world.
Rob Joyce, who heads the National Security Agency's Cybersecurity Directorate, said in September that US officials had previously "seen evidence of [Russian] prepositioning against US critical infrastructure."
The FBI and other agencies want to know if anything new on that front is happening right now. The questionnaire the bureau sent US businesses last month asked if they were aware of any industrial control systems that had been recently compromised by Russian hackers.
An FBI spokesperson declined to comment on the request for information.
The intelligence sharing has gone both ways.

Will Vladimir Putin turn the Second Cold War into a hot one?
Robert M. Lee, CEO of Maryland-based cybersecurity firm Dragos, told officials at the National Security Agency and US Cybersecurity and Infrastructure Security Agency in January that a foreign hacking group had probed the computer networks of US electric utilities that operate liquefied natural gas facilities, Lee told CNN.
The activity, detected in December, involved "high-level reconnaissance," and did not lead to any compromises, Lee said.
The hacking group -- known in the cybersecurity industry as Xenotime or Temp.Veles -- developed tools used in an incident that forced a Saudi petrochemical plant to shut down in 2017, according to cybersecurity researchers. The Treasury Department in 2020 sanctioned a Russian government institute for its alleged involvement in that incident.
"Right now, the biggest concern we have are preparations for potential impacts to US utilities and industrial critical infrastructure," Sergio Caltagirone, Dragos' vice president of threat intelligence, told CNN.
An NSA spokesperson said the agency's Cybersecurity Collaboration Center uses it expertise to "proactively engage the defense industrial base and its service providers to disrupt ongoing nation-state threats in real-time."

What happens in Ukraine may not stay there

The US effort to anticipate Russian hacking threats draws on information on the ground in Ukraine, which has had to fend off a string of cyberattacks since mid-January.
One component of the hacks involved destructive malicious code that wiped data from at least two Ukrainian government agencies. The incident has been contained and not widely disruptive, but it had echoes of the 2017 cyberattack in its use of destructive computer code that was disguised as ransomware.
US companies that do business in Ukraine should be wary of spillover from cyberattacks on Ukrainian networks, government and industry executives have warned.
"[D]isruptive and destructive attacks against Ukraine are likely to have broader implications, including potential impacts to organizations based outside the country," US cybersecurity firm CrowdStrike said in an intelligence assessment.

Health care organizations with a presence in Ukraine -- or that work with suppliers there -- are isolating computer networks serving that part of the business to guard against potential hacking threats, according to Errol Weiss, chief security officer of the Health Information Sharing and Analysis Center, a global cyber threat sharing group for health care providers.