https://www.cnn.com/2022/03/21/politics/biden-russia-cyber-activity/index.html

Biden warns business leaders to prepare for Russian cyber attacks

By Maegan Vazquez, Donald Judd, Sean Lyngaas and Zachary Cohen, CNN

Updated 6:52 PM ET, Mon March 21, 2022

Former NATO advisor: Putin won't stop unless he's stopped in Ukraine 12:45

(CNN) President Joe Biden on Monday issued an urgent warning to American business leaders, telling them to strengthen their companies' cyber defenses immediately.

Speaking at the Business Roundtable Quarterly Meeting in Washington, Biden said Russian President Vladimir Putin is likely to use cyber attacks as a form of retaliation against the United States for its actions to counter Russia's incursion on Ukraine.

Biden said, "The magnitude of Russia's cyber capacity is fairly consequential and it's coming."

He added that "one of the tools (Putin's) most likely to use, in my view -- in our view -- is cyber attacks. They have a very sophisticated cyber capability," and later argued, "The point is that he has the capability. He hasn't used it yet, but it's part of his playbook."

The President told business leaders the national interest is at stake, suggesting that it's "a patriotic obligation that you invest as much as you can in making sure -- and we will help in any way -- that you have built up your technological capacity to deal with cyber attacks."

Earlier Monday, Biden issued a statement pointing to "evolving intelligence" to suggest Russia could conduct malicious cyber activity against American companies and critical infrastructure.

While the Biden administration has been warning the nation of the prospect of cyber attacks by Russia for months, most recently as a response to the economic restrictions imposed on Russia over its invasion of Ukraine, the President's statement suggests "evolving intelligence" has heightened the threat.

The details of exactly what that intelligence is remain unclear, but deputy national security adviser Anne Neuberger said during Monday's White House briefing that Russia had been conducting "preparatory activity" for cyber attacks, which she said could include scanning websites and hunting for software vulnerabilities.

Neuberger said the administration is reiterating its warnings "based on evolving threat intelligence that the Russian government is exploring options for potential cyber attacks on critical infrastructure in the United States," but also underscored that "there is no certainty there will be a cyber incident on critical infrastructure."

The administration last week "hosted classified briefings with companies and sectors we felt would be most effective and provided very practical, focused advice," Neuberger told CNN's Phil Mattingly during Monday's briefing.

Biden said in his statement that the administration would "continue to use every tool to deter, disrupt, and if necessary, respond to cyber attacks against critical infrastructure," but acknowledged that "the federal government can't defend against this threat alone."

"Most of America's critical infrastructure is owned and operated by the private sector and critical infrastructure owners and operators must accelerate efforts to lock their digital doors. The Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) has been actively working with organizations across critical infrastructure to rapidly share information and mitigation guidance to help protect their systems and networks," the statement said.

The administration is recommending several steps to help private sector partners prevent against cyber attacks, including using multi-factor authentication, consulting with cyber security professionals to make sure systems are protected against all known vulnerabilities, changing passwords across networks to prevent stolen credentials from being used, backing up and encrypting data and educating employees on cyber security.

Concerns that Putin might lash out

The decision for Biden to issue the warning reflects concerns within the administration about what Putin might be willing to do next as it becomes increasingly clear his invasion of Ukraine is not going as expected, according to a US official familiar with the internal discussions on cyber security.

Biden officials have been discussing how the state of Russia's ground campaign might change Putin's calculus and how options are being considered in Russia as a result, the official said, noting the situation -- in some ways -- is more volatile than ever.

Russia still maintains its cyber capabilities and the administration believes Putin may be more willing to use those tools as he gets more desperate, the official added. The official would not provide details about the kinds of options for potential cyber attacks the US believes Russia may be exploring, but there has been an increase in observed activity, according to a source familiar with the situation.

The official said it is difficult to determine whether this is just noisy Russian activity meant to send a message to the US about what it could do or actual preparation of the environment.

"If you're Russia, disinformation doesn't seem to be working, they're not going to fire a shot at us, and so what's left is something in the middle: cyber," a second official added.

The US departments of Energy, Treasury and Homeland Security, among others, have briefed big electric utilities and banks on Russian hacking capabilities, and urged businesses to lower their thresholds for reporting suspicious activity. The FBI has been wary that Russian speaking ransomware groups could lash out at US businesses.

While the administration has issued warnings about possible Russian hacking activity for months, when the statement comes from the President, "it's generally because [the threat] has taken on additional significance in the eyes of the government," a third US official said.

Ukrainian government agencies have been hit by a series of cyber attacks before and after the Russian invasion but not the level of hacking that some analysts feared.

Cyber attacks have nonetheless played a supporting role in the war. As the Russian military began attacking Ukraine on February 24, satellite modems that provide internet service for tens of thousands of customers in Europe, including some in Ukraine, were taken offline in a cyber attack on US telecommunications provider Viasat.

The US government is investigating the hack of Viasat as a potential Russian state-sponsored cyber attack, a US official familiar with the matter previously told CNN.

Neuberger on Monday did not identify who was responsible for the hack. She said US officials continue to investigate the incident.

Earlier in March, a bipartisan group of senators also shared their concerns with the Biden administration about the potential of widespread Russian cyberattacks in the US as retribution for harsh sanctions against Russia in the wake of President Vladimir Putin's unprovoked invasion of Ukraine.

In a letter to Homeland Security Secretary Alejandro Mayorkas Sunday evening obtained by CNN, 22 senators, led by Nevada Democratic Sen. Jacky Rosen and South Dakota Republican Sen. Mike Rounds, raised questions about America's readiness for Russian cyber and disinformation threats.

Additional correspondence obtained by CNN indicated that DHS responded to the senators on Monday, saying that the CISA's Office of Legislative Affairs will work with the group to prepare a briefing on the matter.

CNN's Eva McKend contributed to this report.