2022-01-21

How the Biden administration is making gains in an uphill battle against Russian hackers

Jasper, Scott

The Conversation

How the Biden administration is making gains in an uphill battle against Russian hackers

theconversation.com/how-the-biden-administration-is-making-gains-in-an-uphill-battle-against-russian-hackers-174199

Scott Jasper

On Jan. 14, 2022, the FSB, Russia's domestic intelligence service, announced that it had broken up the notorious Russia-based REvil ransomware criminal organization. The FSB said the actions were taken in response to a request from U.S. authorities. The move marks a dramatic shift in Russia's response to criminal cyberattacks launched against U.S. targets from within Russia, and comes at a time of heightened tensions between the two countries.

U.S. policy and actions in response to cyberattacks connected to Russia have changed distinctly since the Biden administration took office. President Joe Biden has openly confronted Russian President Vladimir Putin on his responsibility regarding international cyberattacks, and the Biden administration has taken unprecedented steps to impose costs on Russian cyber criminals and frustrate their efforts.

Upon taking office, Biden immediately faced difficult challenges from Russian intelligence operatives and criminals in headline-grabbing cyberattacks on private companies and critical infrastructure. As a scholar of Russian cyber operations, I see that the administration has made significant progress in responding to Russian cyber aggression, but I also have clear expectations about what national cyber defense can and can't do.

Software supply chain compromise

The SolarWinds hack carried out in 2020 was a successful attack on the global software supply chain. The hackers used the access they gained to thousands of computers to spy on nine U.S. federal agencies and about 100 private-sector companies. U.S. security agencies said that a sophisticated hacking group, "likely Russian in origin," was responsible for the intelligence-gathering effort.

The SolarWinds hack explained.

On Feb. 4, 2021, Biden addressed Putin in a statement delivered at the State Department. Biden said that the days of the U.S. rolling over in the face of Russian cyberattacks and interference in U.S. elections "are over."

Biden vowed to "not hesitate to raise the cost on Russia." The U.S. government had not previously issued indictments or imposed sanctions for cyber espionage, in part out of concerns that they could result in reciprocal actions by Moscow against NSA and CIA hackers. Nevertheless, the U.S. Treasury Department issued sanctions against the Russian Foreign Intelligence Service, the SVR, on April 15, 2021.

Biden also signed an executive order to modernize federal government cybersecurity. He directed agencies to deploy systems that detect cyber incursions, like the one that spotted SolarWinds activity at Palo Alto Networks. In parallel, his security agencies published tools and techniques used by the SVR and ransomware gangs to help organizations defend against them.

Economic sanctions and technical barriers, however, did not slow SVR efforts to gather intelligence on U.S. foreign policy. In May 2021, Microsoft revealed that hackers associated with Russia exploited the mass-mailing service Constant Contact. By masquerading as the U.S. Agency for International Development, they sent authentic-looking emails with links to more than 150 organizations, which, when clicked, inserted a malicious file that allowed computer access.

Ransomware attacks

Also in May, the shutdown of the Colonial Pipeline by a ransomware attack by the Russian cyber gang DarkSide halted the flow of nearly half the gas and jet fuel to the Eastern Seaboard. Panicked drivers rushed to fill up tanks while prices soared. A month later, consumers scrambled to find meat alternatives after REvil infected beef and pork processer JBS USA with ransomware.

Ransomware attacks explained.

Biden said Russia has "some responsibility to deal with this." At a summit in Geneva in June, he handed Putin a list of off-limits critical infrastructure that would merit a U.S. response if attacked. It is likely that Russian intelligence services and law enforcement have a tacit understanding with cybercriminals and can shut down their resources.

Though not counting on Putin to exert influence, the White House formed a ransomware task force to go on the offense against the gangs. The first step was using a counterterrorism program to offer rewards of up to US$10 million for information on hackers behind state-sanctioned breaches of critical infrastructure.

In close collaboration with international partners, the Justice Department announced the arrest of a Ukrainian national in Poland, charged with the REvil ransomware attack against Kaseya, an information technology software supplier. The Justice Department also seized $6.1 million in cryptocurrency from another REvil operator. Romanian authorities arrested two others involved in REvil attacks.

U.S. law enforcement seized $2.3 million paid in ransom to DarkSide by Colonial Pipeline by using a private key to unlock bitcoin. And the Treasury Department disrupted the virtual currency exchanges SUEX and Chatex for laundering the proceeds of ransomware. Treasury Department sanctions blocked all of their property in the U.S. and prohibited U.S. citizens from conducting transactions with them.

Gen. Paul Nakasone, Director of the National Security Agency, testifying before the House Intelligence Committee on April 15, 2021. Al Drago/Pool via AP

Additionally, the top U.S. cyberwarrior, Gen. Paul Nakasone, acknowledged for the first time in public that the U.S. military had taken offensive action against ransomware groups. In October, U.S. Cyber Command blocked the REvil website by redirecting traffic, which prevented the group from extorting victims. After REvil realized its server was compromised, it ceased operations.

Limits of US responses

Russia conducts or condones cyberattacks by state and criminal groups that take advantage of gaps in international law and avoid crossing national security lines. In October, the SVR stepped up attempts to break into technology companies to steal sensitive information. U.S. officials considered the operation to be routine spying. The reality that international law does not prohibit espionage per se prevents U.S. responses that could serve as strong deterrents.

Similarly, after cyber gang BlackMatter carried out a ransomwware attack on an Iowa farm cooperative in September, the gang claimed that the cooperative did not count as critical infrastructure. The gang's claim refers to cyberattack targets that would prompt a national response from the U.S. government.

Despite this ambiguity, the administration has unleashed the military to frustrate the efforts of ransomware groups, while law enforcement agencies have gone after their leaders and their money, and organizations in the U.S. have shored up their information systems defenses.

Though government-controlled hackers might persist, and criminal groups might disappear, rebuild and rebrand, in my view the high costs imposed by the Biden administration could hinder their success. Nevertheless, it's important to bear in mind that national cyber defense is an extremely challenging problem and it's unlikely that the U.S. will be able to eliminate the threat.

[*Get The Conversation's most important politics headlines, in our Politics Weekly newsletter.*]