Cyberattack in Ukraine targets government websites

January 14 2022, by Yuras Karmanau, Frank Bajak and Dasha Litvinova

Credit: Pixabay/CC0 Public Domain

A cyberattack left a number of Ukrainian government websites temporarily unavailable Friday, officials said.

While it wasn't immediately clear who was responsible, the disruption came amid heightened tensions with Russia and after talks between Moscow and the West failed to yield any significant progress this week.

Ukrainian Foreign Ministry spokesman Oleg Nikolenko told The Associated Press it was too soon to say who was behind it, "but there is a long record of Russian cyber assaults against Ukraine in the past."

Moscow had previously denied involvement in cyberattacks against Ukraine.

About 70 websites of both national and regional government bodies were targeted in the attack. but no critical infrastructure was affected and no personal data accessed, according to Victor Zhora, deputy chair of the State Service of Special Communication and Information Protection.

The hack amounted to a simple defacement of government websites, said Oleh Derevianko, a leading private sector expert and founder of the ISSP cybersecurity firm. The hackers got into a content management system they all use, but "didn't get access to the websites themselves."

The main question, said Derevianko, is whether this is a standalone hacktivist action—"patriotic" Russian freelancers—or part of a larger state-backed operation.

A message posted by the hackers in Russian, Ukrainian and Polish that claimed Ukrainians' personal data had been placed online and destroyed. Its threatening tone told Ukrainians to "be afraid and expect the worst." In response, Poland's government issued a statement noting that Russia has a long history of such disinformation campaigns and noted that the Polish in the message was error-ridden and clearly not from a native speaker.

Tensions between Ukraine and Russia have been running high in recent months after Moscow amassed an estimated 100,000 troops near Ukraine's border.

NATO Secretary-General Jens Stoltenberg said Friday that the alliance will continue to provide "strong political and practical support" to Ukraine in light of the cyberattacks.

"In the coming days, NATO and Ukraine will sign an agreement on enhanced cyber cooperation," Stoltenberg said in a statement.

Russia has long history of launching cyber operations against Ukraine, including a hack of its voting system ahead of 2014 national elections and an assault the country's power grid in 2015 and 2016. In 2017, Russia unleashed one of most damaging cyberattacks on record with the NotPetya virus that targeted Ukrainian businesses and caused more than $10 billion in damage globally.

Ukrainian cybersecurity professionals have been fortifying the defenses of critical infrastructure ever since. Zhora has told the AP that officials are particularly concerned about Russian attacks on the power grid, rail network and central bank.

Experts have said recently that the threat of another such cyberattack is significant as it would give Russian President Vladimir Putin the ability to destabilize Ukraine and other ex-Soviet countries that wish to join NATO without having to commit troops.

"If you're trying to use it as a stage and a deterrent to stop people from moving forward with NATO consideration or other things, cyber is perfect," Tim Conway, a cybersecurity instructor at the SANS Institute, told the AP in an interview last week.

Conway was in Ukraine last month conducting a simulated cyberattack on the country's energy sector. The U.S. has been helping Ukraine bolster its cyber defenses through agencies including the Department of Energy and USAID.

The White House didn't immediately respond to a request seeking comment.

In a separate development Friday, Russia's Federal Security Service, or FSB, announced the detention of members of the REvil ransomware gang, which was behind last year's Fourth of July weekend supply-chain attack targeting the Florida-based software firm Kaseya that crippled more than 1,000 businesses and public organizations globally.

The FSB claimed to have dismantled the gang, but REvil effectively disbanded in July. Cybersecurity experts say its members largely moved to other ransomware syndicates. They cast doubt Friday on whether the arrests would significantly impact ransomware gangs, whose activities have only moderately eased after a string of high-profile attacks on critical U.S. infrastructure last year including the Colonial Pipeline.

The FSB said it raided the homes of 14 group members and seized over 426 million rubles ($5.6 million), including in cryptocurrency as well as computers, crypto wallets and 20 elite cars "bought with money obtained by criminal means." All those detained have been charged with "illegal circulation of means of payment," a criminal offense punishable by up to six years in prison. The suspects weren't named.

According to the FSB, the operation was conducted at the request of U.S. authorities, who reported the leader of the group to officials in Moscow. It's the first significant public action by Russian authorities since U.S. President Joe Biden warned Putin last year that he needed to crack down on ransomware gangs in his country.

Experts said it was too early to know if the arrests signal a major Kremlin crackdown on ransomware criminals—or if may just have been a piecemeal effort to appease the White House.

Bill Siegel, CEO of the ransomware response firm Coveware, said he'll be watching to see what kind of prison time those arrested get. "The follow-through on sentencing will send the strongest signal one way or another as to IF there has truly been a change in how tolerant Russia will be in the future to cyber criminals," he said via email.

And Yelisey Boguslavskiy, research director at Advanced Intelligence, said that while the arrests do follow a pattern of Kremlin pressure on ransomware criminals—including in some cases prompting them to hand over decryption keys—those arrested could simply be low-level affiliates, not the core group that managed the malware. The REvil syndicate also apparently ripped off some affiliates so it had enemies in the criminal underground, he said.

REvil's attacks crippled tens of thousands of computers worldwide and yielded at least $200 million in ransom payments, Attorney General Merrick Garland said in November when announcing charges against two hackers affiliated with the gang.

Such attacks brought significant attention from law enforcement officials around the world. The U.S. announced charges against two affiliates in November, hours after European law enforcement officials revealed the results of a lengthy, 17-nation operation. As part of that operation, Europol said, a total of seven hackers linked to REvil and another ransomware family have been arrested since February.

The AP reported last year that U.S. officials, meanwhile, shared a small number of names of suspected ransomware operators with Russian officials, who have said they were investigating.

Brett Callow, a ransomware analyst with the cybersecurity firm Emsisoft, said that "whatever Russia's motivations may be, the arrests would "certainly send shockwaves through the cybercrime community.

The gang's former affiliates and business associates will invariably be concerned about the implications."