How the Kremlin provides a safe harbor for ransomware

https://apnews.com/article/business-technology-general-news-government-and-politics-c9dab7eb3841be45dff2d93ed3102999

By FRANK BAJAK | April 16, 2021

1 of 2 FILE - A Russian man identified as Alexander Vinnik, center, is escorted by police officers from the courthouse at the northern Greek city of Thessaloniki, in this Friday, Sept. 29, 2017, file photo. Vinnik, convicted of laundering $160 million in criminal proceeds through a cryptocurrency exchange, is currently imprisoned in France and might yield additional information about the intersection of organized cybercrime and the Russian state. (AP Photo/Giannis Papanikos, File)

BOSTON (AP) — A global epidemic of digital extortion known as ransomware is crippling local governments, hospitals, school districts and businesses by scrambling their data files until they pay up. Law enforcement has been largely powerless to stop it.

One big reason: Ransomware rackets are dominated by Russian-speaking cybercriminals who are shielded — and sometimes employed — by Russian intelligence agencies, according to security researchers, U.S. law enforcement, and now the Biden administration.

On Thursday, as the U.S. slapped sanctions on Russia for malign activities including state-backed hacking, the Treasury Department said Russian intelligence has enabled ransomware attacks by cultivating and co-opting criminal hackers and giving them safe harbor. With ransomware damages now well into the tens of billions of dollars, former British intelligence cyber chief Marcus Willett recently deemed the scourge "arguably more strategically damaging than state cyber-spying."

The value of Kremlin protection isn't lost on the cybercriminals themselves. Earlier this year, a Russian-language dark-web forum lit up with criticism of a ransomware purveyor known only as "Bugatti," whose gang had been caught in a rare U.S.-Europol sting. The assembled posters accused him of inviting the crackdown with technical sloppiness and by recruiting non-Russian affiliates who might be snitches or undercover cops.

Worst of all, in the view of one long-active forum member, Bugatti had allowed Western authorities to seize ransomware servers that could have been sheltered in Russia instead. "Mother Russia will help," that individual wrote. "Love your country and nothing will happen to you." The conversation was captured by the security firm Advanced Intelligence, which shared it with the Associated Press.

"Like almost any major industry in Russia, (cybercriminals) work kind of with the tacit consent and sometimes explicit consent of the security services," said Michael van Landingham, a former CIA analyst who runs the consultancy Active Measures LLC.

Russian authorities have a simple rule, said Karen Kazaryan, CEO of the software industry-supported Internet Research Institute in Moscow: "Just don't ever work against your country and businesses in this country. If you steal something from Americans, that's fine."

Unlike North Korea, there is no indication Russia's government benefits directly from ransomware crime, although Russian President Vladimir Putin may consider the resulting havoc a strategic bonus.

In the U.S. alone last year, ransomware struck more than a hundred federal, state and municipal agencies, upward of 500 hospitals and other health care centers, some 1,680 schools, colleges and universities and hundreds of businesses, according to t he cybersecurity firm Emsisoft.

Damage in the public sector alone is measured in rerouted ambulances, postponed cancer treatments, interrupted municipal bill collection, canceled classes and rising insurance costs – all during the worst public health crisis in more than a century.

The idea behind these attacks is simple: Criminals infiltrate malicious data-scrambling software into computer networks, use it to "kidnap" an organization's data files, then demand huge payments, now as high as $50 million, to restore them. The latest twist: if victims fail to pay up, the criminals may publish their unscrambled data on the open internet.

In recent months, U.S. law enforcement has worked with partners including Ukraine and Bulgaria to bust up these networks. But with the criminal masterminds out of reach, such operations are generally little more than whac-a-mole.

Collusion between criminals and the government is nothing new in Russia, said Adam Hickey, a U.S. deputy assistant attorney general, who noted that cybercrime can provide good cover for espionage.

Back in the 1990s, Russian intelligence frequently recruited hackers for that purpose, said Kazaryan. Now, he said, ransomware criminals are just as likely to be moonlighting state-employed hackers.

The Kremlin sometimes enlists arrested criminal hackers by offering them a choice between prison and working for the state, said Dmitri Alperovitch, former chief technical officer of the cybersecurity firm Crowdstrike. Sometimes the hackers use the same computer systems for state-sanctioned hacking and off-the-clock cybercrime for personal enrichment, he said. They may even mix state with personal business.

That's what happened in a 2014 hack of Yahoo that compromised more than 500 million user accounts, allegedly including those of Russian journalists and U.S. and Russian government officials. A U.S. investigation led to the 2017 indictment of four men, including two officers of Russia's FSB security service – a successor to the KGB. One of them, Dmitry Dokuchaev, worked in the same FSB office that cooperates with the FBI on computer crime. Another defendant, Alexsey Belan, allegedly used the hack for personal gain.

A Russian Embassy spokesman declined to address questions about his government's alleged ties to ransomware criminals and state employees' alleged involvement in cybercrime. "We do not comment on any indictments or rumors," said Anton Azizov, the deputy press attache in Washington.

Proving links between the Russian state and ransomware gangs is not easy. The criminals hide behind pseudonyms and periodically change the names of their malware strains to confuse Western law enforcement.

But at least one ransomware purveyor has been linked to the Kremlin. Maksim Yakubets, 33, is best known as co-leader of a cybergang that cockily calls itself Evil Corp. The Ukraine-born Yakubets lives a flashy lifestyle, He drives a customized Lamborghini supercar with a personalized number plate that translates to 'Thief,' according to Britain's National Crime Agency.

Yakubets started working for the FSB in 2017, tasked with projects including "acquiring confidential documents through cyber-enabled means and conducting cyber-enabled operations on its behalf," according to a December 2019 U.S. indictment. At the same time, the U.S. Treasury Department slapped sanctions on Yakubets and offered a $5 million reward for information leading to his capture. It said he was known to have been "in the process of obtaining a license to work with Russian classified information from the FSB."

The indictment charged Evil Corp. with developing and distributing ransomware used to steal at least $100 million in more than 40 countries over the previous decade, including payrolls pilfered from towns in the American heartland.

By the time Yakubets was indicted, Evil Corp. had become a major ransomware player, security researchers say. By May 2020, the gang was distributing a ransomware strain that was used to attack eight Fortune 500 companies, including the GPS device maker Garmin, whose network was offline for days after an attack, according to Advanced Intelligence.

Yakubets remains at large. Another Russian currently imprisoned in France, however, might offer more insight into the dealings of cybercriminals and the Russian state. Alexander Vinnik was convicted of laundering $160 million in criminal proceeds through a cryptocurrency exchange called BTC-e. A 2017 U.S. indictment charged that “some of the largest known purveyors of ransomware” actually used it to launder $4 billion. But Vinnik can’t be extradited until he completes his 5-year French prison sentence in 2024.

Still, a 2018 study by the nonpartisan think tank Third Way found the odds of successfully prosecuting authors of cyberattacks against U.S. targets — ransomware and online bank theft are the costliest — are no better than three in a thousand. Experts say that those odds have gotten longer.

This week’s sanctions send a strong message, but aren’t likely to deter Putin unless the financial sting hits closer to home, many analysts believe.

That might require the kind of massive multinational coordination that followed the 9/11 terror attacks. For instance, allied countries could identify banking institutions known to launder ransomware proceeds and cut them off from the global financial community.

“If you’re able to follow the money and disrupt the money and take the economic incentive out, that’ll go a long way in stopping ransomware attacks,” said John Riggi, cybersecurity advisor for the American Hospital Association and a former FBI official.

___

This story has been updated to correct the spelling of Alexander Vinnik’s name.

___

Associated Press writer Angela Charlton in Paris contributed to this report.

###