Global war on ransomware? Hurdles hinder the US response

June 5 2021, by Alan Suderman

WANTED BY THE FBI

MAKSIM VIKTOROVICH YAKUBETS

Conspiracy; Conspiracy to Commit Fraud; Wire Fraud; Bank Fraud; Intentional Damage to a Computer




DESCRIPTION

Aliases: Maksim Yakubets, "AQUA"	
Date(s) of Birth Used: May 20, 1987	**Place of Birth:** Ukraine
Hair: Brown	**Eyes:** Brown
Height: Approximately 5'10"	**Weight:** Approximately 170 pounds
Sex: Male	**Race:** White
Citizenship: Russian	

REWARD

The United States Department of State's Transnational Organized Crime Rewards Program is offering a reward of up to $5 million for information leading to the arrest and/or conviction of Maksim Viktorovich Yakubets.

CAUTION

Maksim Viktorovich Yakubets is wanted for his involvement with computer malware that infected tens of thousands of computers in both North America and Europe, resulting in actual financial losses in the tens of millions of dollars.

Specifically, Yakubets was involved in the installation of malicious software known as Zeus, which was disseminated through phishing emails and used to capture victims' online banking credentials. These credentials were then used to steal money from the victims' bank accounts. On August 22, 2012, an individual was charged in a superseding indictment under the moniker "aqua" in the District of Nebraska with conspiracy to participate in racketeering activity, conspiracy to commit computer fraud and identity theft, aggravated identity theft, and multiple counts of bank fraud. On November 14, 2019, a criminal complaint was issued in the District of Nebraska that ties the previously indicted moniker of "aqua" to Yakubets and charges him with conspiracy to commit bank fraud.

Yakubets is also allegedly the leader of the Bugat/Cridex/Dridex malware conspiracy wherein he oversaw and managed the development, maintenance, distribution, and infection of the malware. Yakubets allegedly conspired to disseminate the malware through phishing emails, to use the malware to capture online banking credentials, and to use these captured credentials to steal money from the victims' bank accounts. He, subsequently, used the malware to install ransomware on victims' computers. Yakubets was indicted in the Western District of Pennsylvania, on November 13, 2019, and was charged with Conspiracy, Conspiracy to Commit Fraud, Wire Fraud, Bank Fraud, and Intentional Damage to a Computer.

If you have any information concerning this person, please contact your local FBI office or the nearest American Embassy or Consulate.

Field Offices: Omaha, Pittsburgh

www.fbi.gov

This poster provided by the U.S. Department of Justice shows Maxsim

Yukabets. Yakubets, 33, is best known as co-leader of a cybergang that calls itself Evil Corp. Foreign keyboard criminals with no fear of repercussions have paralyzed U.S. schools and hospitals, leaked highly sensitive police files, triggered US fuel shortages and, most recently, a now could be responsible for a disruption in global food supply chains. Credit: U.S. Department of Justice via AP

Foreign keyboard criminals with scant fear of repercussions have paralyzed U.S. schools and hospitals, leaked highly sensitive police files, triggered fuel shortages and, most recently, threatened global food supply chains.

The escalating havoc caused by ransomware gangs raises an obvious question: Why has the United States, believed to have the world's greatest cyber capabilities, looked so powerless to protect its citizens from these kind of criminals operating with near impunity out of Russia and allied countries?

The answer is that there are numerous technological, legal and diplomatic hurdles to going after ransomware gangs. Until recently, it just hasn't been a high priority for the U.S. government.

That has changed as the problem has grown well beyond an economic nuisance. President Joe Biden intends to confront Russia's leader, Vladimir Putin, about Moscow's harboring of ransomware criminals when the two men meet in Europe later this month. The Biden administration has also promised to boost defenses against attacks, improve efforts to prosecute those responsible and build diplomatic alliances to pressure countries that harbor ransomware gangs.

Calls are growing for the administration to direct U.S. intelligence

agencies and the military to attack ransomware gangs' technical infrastructure used for hacking, posting sensitive victim data on the dark web and storing digital currency payouts.

Fighting ransomware requires the nonlethal equivalent of the "global war on terrorism" launched after the Sept. 11 attacks, said John Riggi, a former FBI agent and senior adviser for cybersecurity and risk for the America Hospital Association. Its members have been hard hit by ransomware gangs during the coronavirus pandemic.

"It should include a combination of diplomatic, financial, law enforcement, intelligence operations, of course, and military operations," Riggi said.

A public-private task force including Microsoft and Amazon made similar suggestions in an 81-page report that called for intelligence agencies and the Pentagon's U.S. Cyber Command to work with other agencies to "prioritize ransomware disruption operations."

"Take their infrastructure away, go after their wallets, their ability to cash out," said Philip Reiner, a lead author of the report. He worked at the National Security Council during the Obama presidency and is now CEO at The Institute for Security and Technology.

But the difficulties of taking down ransomware gangs and other cybercriminals have long been clear. The FBI's list of most-wanted cyber fugitives has grown at a rapid clip and now has more than 100 entries, many of whom are not exactly hiding. Evgeniy Bogachev, indicted nearly a decade ago for what prosecutors say was a wave of cyber bank thefts, lives in a Russian resort town and "is known to enjoy boating" on the Black Sea, according to the FBI's wanted listing.

Ransomware gangs can move around, do not need much infrastructure to

operate and can shield their identities. They also operate in a decentralized network. For instance, DarkSide, the group responsible for the Colonial Pipeline attack that led to fuel shortages in the South, rents out its ransomware software to partners to carry out attacks.

Katie Nickels, director of intelligence at the cybersecurity firm Red Canary, said identifying and disrupting ransomware criminals takes time and serious effort.

"A lot of people misunderstand that the government can't just willy-nilly go out and press a button and say, well, nuke that computer," she said. "Trying to attribute to a person in cyberspace is not an easy task, even for intelligence communities."

Reiner said those limits do not mean the United States cannot still make progress against defeating ransomware, comparing it with America's ability to degrade the terrorist group al-Qaida while not capturing its leader, Ayman al-Zawahiri, who took over after U.S. troops killed Osama bin Laden.

"We can fairly easily make the argument that al-Qaida no longer poses a threat to the homeland," Reiner said. "So short of getting al-Zawahiri, you destroy his ability to actually operate. That's what you can do to these (ransomware) guys."

The White House has been vague about whether it plans to use offensive cyber measures against ransomware gangs. Press secretary Jen Psaki said Wednesday that "we're not going to take options off the table," but she did not elaborate. Her comments followed a ransomware attack by a Russian gang that caused outages at Brazil's JBS SA, the second-largest producer of beef, pork and chicken in the United States.

Gen. Paul Nakasone, who leads U.S. Cyber Command and the National

Security Agency, said at a recent symposium that he believes the U.S. will be "bringing the weight of our nation," including the Defense Department, "to take down this (ransomware) infrastructure outside the United States."

Sen. Angus King, an independent from Maine who is a legislative leader on cybersecurity issues, said the debate in Congress over how aggressive the U.S. needs to be against ransomware gangs, as well as state adversaries, will be "front and center of the next month or two."

"To be honest, it's complicated because you're talking about using government agencies, government capabilities to go after private citizens in another country," he said.

The U.S. is widely believed to have the best offensive cyber capabilities in the world, though details about such highly classified activities are scant. Documents leaked by former NSA contractor Edward Snowden show the U.S. conducted 231 offensive cyber operations in 2011. More than a decade ago a virus called Stuxnet attacked control units for centrifuges in an underground site in Iran, causing the sensitive devices to spin out of control and destroy themselves. The cyberattack was attributed to America and Israel.

U.S. policy called "persistent engagement" already authorizes cyberwarriors to engage hostile hackers in cyberspace and disrupt their operations with code. U.S. Cyber Command has launched offensive operations related to election security, including against Russian misinformation officials during U.S. midterm elections in 2018.

After the Colonial Pipeline attack, Biden promised that his administration was committed to bringing foreign cybercriminals to justice. Yet even as he was speaking from the White House, a different Russian-linked ransomware gang was leaking thousands of highly

sensitive internal files—including deeply personal background checks—belonging to the police department in the nation's capital. Experts believe it's the worst ransomware attack against a U.S.-based law enforcement agency.

"We are not afraid of anyone," the hackers wrote in a follow-up post.