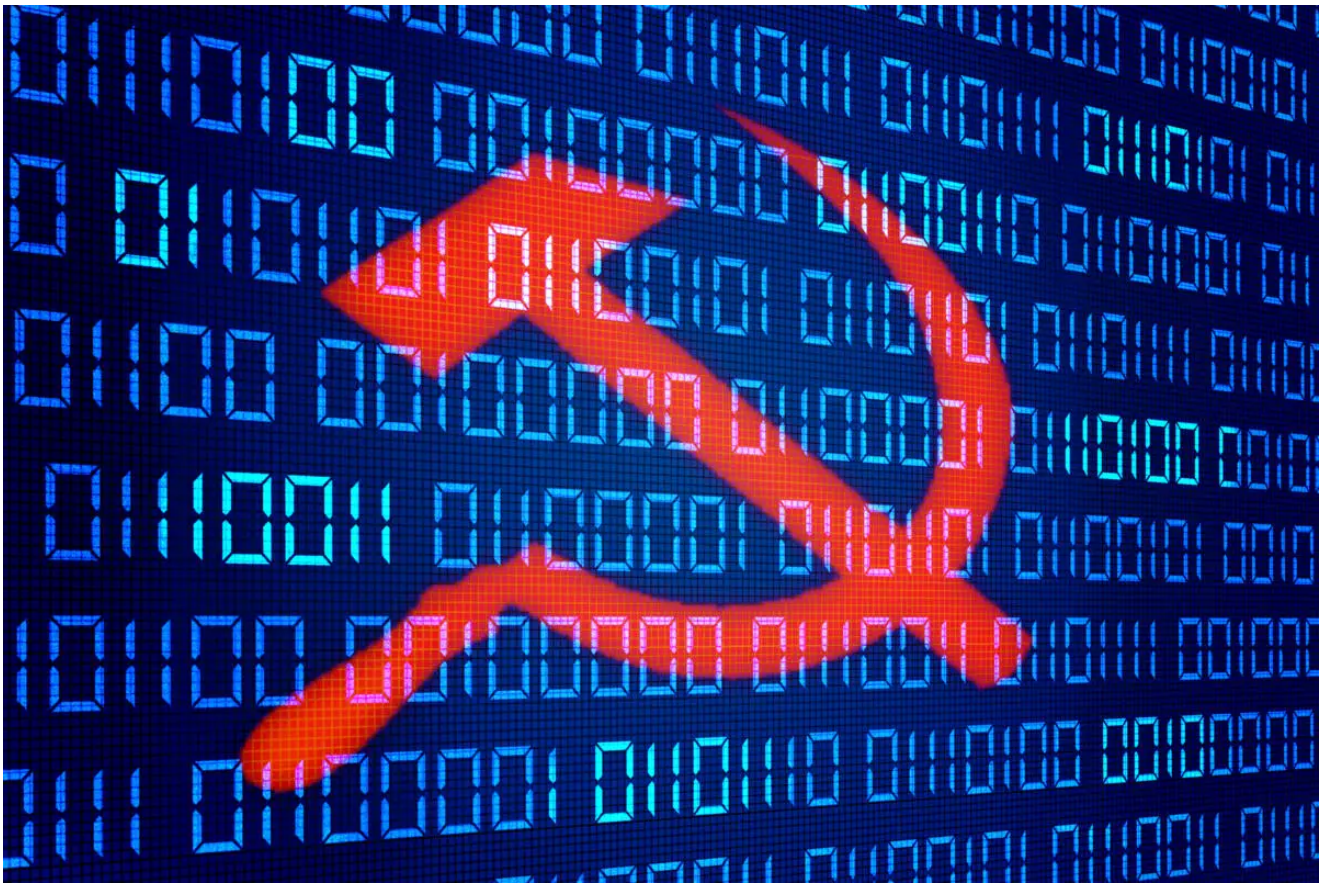
# Russia is fully capable of shutting down cybercrime

csoonline.com/article/3632943/russia-is-fully-capable-of-shutting-down-cybercrime.html

Christopher Burgess



It is no secret the locus for a great deal of the world's cybercriminal activity lays within the boundaries of The Russian Federation. The  onslaught of ransomware attacks directed at non-Russian entities is evidence of that.

Last week, Recorded Future's Insikt Group published a report shedding more light on the connection between the Russian state and criminal actors, a connection that Insikt Group posits is "well established yet highly diffused."

The key judgments from the Insikt Groups analysis are:

- It is highly likely that Russian intelligence services and law enforcement have a longstanding, tacit understanding with criminal threat actors.
- This association will continue, though efforts to put space between the government and criminal entities may increase to provide greater plausible deniability to the government
- US President Joe Biden's assertion that Russian cybercriminals are protected by the Russian government has placed Russian President Vladimir Putin on the defensive.

- Russian cybercriminals are reforming their operations and targeting vectors implying that the Biden administration's actions have been modestly successful.

Is this much of a surprise to those who invest their professional life watching things Russia? Not really, says Monique Camarra, co-host of the Kremlin File who explains, "We know the KGB was present in all aspects of Soviet life, so it's no surprise that they would have relations and dealings with criminal groups. Important hubs were controlled by the KGB in cooperation with criminal elements." She continued how, for example, "the Tambov crime group, during privatization of state assets, regained control of the port, fuel and energy business. The fact that the new cadre of criminals, the cybercriminals, are attached at the hip to the Russian security apparatus should surprise no one."

## US sanctions have consequences

As a result of a flurry of ransomware attacks that impacted the United States infrastructure, the United States hit Russia in April 2021 with both sanctions and the expulsion of diplomatic/intelligence personnel from the United States, tying the diplomatic actions to the criminal actions in a clear and unambiguous signal: the tolerance of the United States was approaching its end point.

In June, at the summit referenced in Insikt Group's analysis and then again in July 2021 when Biden held a telephone conference call with Putin, a similar message was delivered, unambiguously, by Biden. Biden commented to reporters, "I made it very clear to him that the United States expects, when a ransomware operation is coming from his soil even though it's not sponsored by the state, we expect them to act if we give them enough information to act on who that is."

It isn't as if Russia can't control their internet gateways across which these cyber crimes are being committed. To wit: On September 2, 2021, with the Russian election fast approaching and the efforts of Putin to silence dissent in overdrive, Roskomnadzor blocked six providers of virtual private networks to the Russian market (Hola! VPN, ExpressVPN, KeepSolid VPN Unlimited, Nord VPN, Speedify VPN, IPVanish VPN); the organization had previously excluded two others, VyprVPN and OperaVPN. Roskomnadzor claims they blocked the VPN services due to "illegal activities, including those related to the distribution of drugs, child pornography, extremism and suicidal tendencies."

## Dmitry Dokuchaev—a key individual

Interestingly, the Insikt analysis draws on actions that occurred over the last decade to create their mosaic of interconnectivity between the Russian government and cybercriminals. The analysis hangs its hat on Dmitry Dokuchaev, among others, a major in the Russian interior ministry (FSB), who is a unique individual in that he was simultaneously under indictment by the United States for cybercrimes and by Russia for treason associated with cybercrimes while an officer of the FSB in 2016. He pleaded guilty in Russia and went to prison.

The circumstances of Dokuchaev's arrest further cement the connection between the Russian government and the criminal cyber world and illustrate what Russia is capable of doing to cybercriminals if it is in their interests.

The FSB cyber operations group, Information Security Center, of which Dokuchaev was a member, imploded in December 2016 through January 2017, with the arrests of multiple leadership personnel.

The initial arrests included Colonel Sergey Mikhailov, deputy director of the center, and Ruslan Stoyanov, a manager at Kaspersky Labs. They are alleged to have feathered their nest by sharing with the West (the FBI and others) data that had been harvested from Russian companies which they engaged to investigate… wait for it… cybercrimes.

The arrest of Mikhailov was full of drama and seemed straight out of a 1950s Russian crime film: He reportedly was present at an FSB staff meeting when he was dragged unceremoniously out the of the building with a bag over his head. The next arrests included Dokuchaev, who served as Mikhailov's deputy within the center, and the director of the center, Andrei Gerasimov. In 2019, Mikhailov was sentenced to 22 years in prison by the Russian courts.

Much to the chagrin of the FSB, their dirty laundry was being aired for all to see, as the internal catfight between the FSB's Information Security Center, which just had its leadership arrested for cybercrimes, and the FSB's Special Communications Group (previously known to western intelligence as FAPSI, the group in charge of Russian cryptographic standards, security of Russian elections, signals intelligence, and a multitude of other activities) culminated in the Special Communications Group assimilating the Information Security Center.

## Russia's action to take

The FSB saga is evidence that Russia is fully capable of arresting and prosecuting cyber criminals operating within their geographic and virtual internet footprint. The bar is high for instances of cybercrime that will cause the Russian government to take action. But clearly, two officers facilitating the West's investigation into Russian cybercriminals off the record and allegedly for millions of dollars, met that bar.

The choice of words is always important and therefore one reading between the lines will note the subtlety of Biden's messaging to Putin: It is in the Russian Federation's interest to act because, regardless of whether entities operate with or without the tacit acknowledgement of the Russian government, the United States had provided fair warning that lack of action by Russia will result in the United States acting in its own interest.

Time will tell if the relationship between Russian cybercriminals and the Russian Federation cyber entities will evolve in a manner that quiets the former and their criminal activities. If not, the potential for action by U.S.  government entities should be expected.