RUSSIA IS STRUGGLING TO KEEP ITS CYBERCRIME GROUPS ON A TIGHT LEASH

-

07.06.2017

The Rehister (06 Jun 2017)
Russia's control of cybercrime groups that have come to play a part in its espionage activity is crumbling, according to Cybereason.

The security intelligence outfit reached this conclusion after reviewing the latest tactics and procedures associated with high-profile cyber-espionage pops blamed on the Kremlin. Russia has made use of contractors to run intelligence operations for many years. These criminals-turned-spies offer a resource to the state while enjoying a cloak of semi-protected "status" for their extracurricular malicious activities, providing they are directed against foreign targets.

Ross Rustici, senior manager of intelligence research at Cybereason, said that what the FSB is doing now is an "outgrowth of what the KGB was doing in the 80s".

"With the collapse of the USSR, the Russian government had a problem of recruiting technology talent to accomplish their goals. Through necessity they turned to outsourcing and contractors to cover the work they weren't able to handle in-house. This gave them deniability about subsequent cyber-operations."

Red (Army) Teaming
The Russian security services (formerly arms of the KGB) have longstanding ties to national criminal and hacktivist communities, according to Cybereason. A decade ago, the state demonstrated its reach into these informal communities with the large scale DDoSing of Estonia in 2007, which came to be known as the first cyber-conflict.

Cybercriminals are recruited to Russia's national cause through a mix of coercion, payments and appeals to patriotic sentiment. "There's a grab bag of motives", according to Rustici.

"Patriot hackers" have played a part in Russian cy-ops for at least six years, according to Cybereason. "The hybridisation that results in the use of an open-source malware kit to attack the Ukrainian power grid or patriotic hackers taking part in attacking a foreign government's networks as part of a kinetic attack demonstrates the extent to which outsourcing can empower and obfuscate nation-state actions."

Russia's hybridisation of tools, actors and missions has created one of the most "potent and ill-defined advanced threats that the cybersecurity community faces", Cybereason claims. Russia's use of private contractors also has other benefits in helping to decrease overall operational costs, mitigating the risk of detection and gaining technical expertise that they cannot recruit directly into the government. Combining a cyber-militia with official state-sponsored hacking teams has

"created the most technically advanced and bold cybercriminal community in the world".

The maturity of the Russian approach allows for considerable advances in oversight for these types of operations in addition to more creative uses of the outsourced labor. Unlike in China, where this small industry is an evolution of a permissive and unregulated environment or North Korea where all actions are highly regulated and the state attempts to control every facet of online activity, the Kremlin has actively sought to create operating procedures and create a decision framework for how to employ their underground elements.

For example, the US Justice Department recently unsealed an indictment alleging that the FSB (Russian Federal Security Service the country's main investigative spy agency) officer defendants, Dmitry Dokuchaev and Igor Sushchin, protected, directed, facilitated and paid criminal hackers to collect information through computer intrusions in the US and elsewhere. Prosecutors alleged that FSB officers worked with criminal co-defendants Alexsey Belan and Karim Baratov to obtain access to the email accounts of thousands of individuals.

But Russia's longstanding strategy of using criminal and hacktivist groups to launch attacks on nation states is starting to collapse, according to Cybereason. This is more to do with longer-term economic trends rather than individual law enforcement actions.

The advent of cryptocurrencies and globalisation of hacking has loosened the Kremlin's grip on these groups as they no longer need to rely on Russian banks to launder their payments. Russia sometimes employs hackers who reside beyond its geographical borders making it harder to "apply coercive force should the actors cross one of the many ambiguous lines that governs these relationships". Appeals to patriotism alone are not enough. The threat of "hack for us or end up in Siberia" only works against residents hackers.

This eroding control is impacting security around the world, as nation-state actors use the skills they honed with Russia for their own agendas such as the Carbanak Gang. This has repercussions for international cybersecurity as former state operatives are becoming mercenaries or hackers for hire. "The capabilities that were once indicative of a nation-state actor are now an affordable commodity for the private sector," reports Cybereason.

Other countries looking to emulate the Russian model in their own cyber operations are likely to run into trouble. For one thing, mistakes by non-state actors can escalate quickly. In addition, cybercriminals will "occasionally bite the hand that feeds them", quite aside from the difficulty for a state in controlling any operation that involves maverick hackers. Lastly there's the issue that bringing in independent hackers makes it more likely that any military-grade hacking tools they get hold of will leak, creating an arms control proliferation problem in the process.

Kaynak/Source: