How the Russia-Ukraine conflict is impacting cybercrime

intel471.com/blog/russia-ukraine-conflict-cybercrime-underground

Intel 471 has been monitoring how the ongoing tension between Russia and Ukraine is impacting the cybercrime underground. While financially-motivated actors have yet to show their inclination to leverage the conflict for personal gain, the recent change of course from Russian law enforcement in the form of arrests and takedowns show that the country will leverage the underground for diplomatic advantage in the same way it does for its intelligence purposes.

While there have been cyberattacks on Ukrainian entities over the past month, Intel 471 has not observed any evidence that these attacks have been carried out by financially-motivated actors. An attack carried out in January, in which Ukrainian websites were defaced as a cover to launch destructive malware known as WhisperGate, has not attracted much attention from underground actors. Of the discussions we observed, a low volume of actors elaborated on how the attacks were committed and spoke on what they believed to be weaknesses in Ukrainian critical infrastructure. The lack of discussion fits the methodology of financially-motivated actors: attacks like WhisperGate are difficult to monetize. Additionally, a good portion of these forums are pro-Russian in nature, with forum moderators frequently discouraging or outright banning discussion threads that discuss politics.

Aside from the attack mentioned above, we also observed a small concentration of advertisements and offers related to data tied to Ukrainian government organizations. While the timing of the offers might suggest the actors used the current Russia-Ukraine tensions as a motivator, or perhaps nation-state affiliated actors were at the helm in some way, we assess these reasons were likely not the case. This assessment comes as the volume of Ukrainian government data mirrors other instances we've observed over the past five years, when geopolitical tensions were calm.

Conversely, there has been a lot of action in the form of Russian law enforcement arresting various alleged cybercriminals over the past three months. Most recently, three underground stores trading in compromised payment card data – Ferum shop, Trump Dumps and UAS Shop – along with the Sky Fraud forum went offline, with a note indicating they allegedly were seized by Russia's Ministry of Internal Affairs (MVD). Later the same day, the Russian TASS press agency reported six individuals were arrested in Russia on cybercrime charges.

While it's unclear how everyone arrested is tied to the affected forums, one of those men — Andrey Novak — has been linked to UNICC, another carding forum that "closed" last month. Novak was also among those charged in absentia in 2018 by the U.S. Department of Justice for allegedly working with notorious malware and carding forum Infraud.

These arrests, combined with the actions taken against the REvil ransomware gang, are an unprecedented development in how Russian law enforcement deals with cybercriminals within its own borders. For decades, Russia has been extremely lenient with cybercriminals that have shown ties to Russia and a modus operandi of targeting countries that don't belong to the Commonwealth of Independent States (CIS), an intergovernmental organization which includes Russia and former Soviet states. Cybercriminals have long developed their techniques, tactics, and procedures (TTPs) in order to purposely avoid targeting CIS countries and businesses that operate within them, while forum admins and other organized groups have banned any activity aimed at these countries.

It is possible that the Russian administration has authorized these law enforcement actions as a diplomatic gesture to Western governments, given that Russia's domestic security agency, the Federal Security Service (FSB), has publicly said some of the arrests were conducted in conjunction with U.S. law enforcement. Russia's desire to publicize these actions through domestic and international mainstream outlets and social media platforms suggests the administration is pushing a message of cooperation and resolution. Should tensions cool between Ukraine and Russia, we assess it is possible that Russian law enforcement will return to status quo leniency for these cybercriminals. Until then, Russian-based threat actors could see their country's law enforcement's recent actions as a deterrent to conducting cybercrime activities, which would prove a worthy cause benefiting organizations around the world.

It's also likely that as the situation progresses, advantageous financially-motivated threat actors may seek to target entities in Ukraine that may be more vulnerable due to understaffed organizations or overburdened network infrastructure. Criminal actors may seek to purchase access credentials, personally identifiable information (PII) or intellectual property to capitalize on the distractions, and financially motivated actors could act as suppliers to fill that gap.

Intel 471 will continue to monitor, analyze and report on the underground response as the Russia-Ukraine conflict develops.