The Moscow Times
30 YEARS
INDEPENDENT NEWS FROM RUSSIA

‘Hacktivist’ Cyber Disruption Could Spread to Russia, Experts Believe

An attack on the Belarusian railway system shows cyberspace may have become the safest place for activists to reside.

By James Beardsworth

February 01, 2022

A cyber attack briefly halted Belarusian railway systems. **Eugene Pashkovsky (CC BY-SA 4.0).**

A cyber attack carried out by a group called the Belarusian Cyber Partisans (BCP) on Jan. 24 briefly halted Belarusian railway systems, threatening to paralyze trains moving Russian troops and artillery into the country.

The attack, which was part of a wider project by the group to target state-run institutions and longtime leader Alexander Lukashenko’s regime, could be a sign of more cyber tactics to come by activists in the wider region, including Russia, experts said.

"The BCP have been so spectacular and effective that I could definitely see a few other groups

popping up in the region," Gabriella Coleman, professor of Anthropology at Harvard University and author of two books on computer hacking, told The Moscow Times.

The number of hacktivist groups — activists who use technology to effect social change — has been on the rise across Russia in the last few years, and with brutal crackdowns on public protests sweeping across the post-Soviet region, cyberspace may be the safest place for collective discord.

'In Russia there is clearly a highly trained technical class of people, and there is disaffection, so you would expect to find at least a small pocket of hacktivism," Coleman added.

Related article: Russian SolarWinds Hackers Target 150 Organizations in New Attack

Hacktivists' tactics, which were popularized by the group Anonymous over the past decade, have been responsible for a series of high-profile attacks across Russia, including a series of "hack and leaks" by cyber group Shaltai Boltai — meaning humpty dumpty in English — which exposed Kremlin tactics in the 2014 annexation of Crimea.

A glut of technical specialists in Russia, and the absence of a significant tech sector to employ them tends to attract those feeling disenfranchised to the world of hacktivism, experts say. But many more potential hacktivists end up becoming hackers.

"There is just so much money to be made in illegal hacking," Coleman said.

Additionally, an alleged tacit agreement between cybercriminals and the state has historically allowed hackers to work with relative impunity in Russia providing they don't operate in the .ru domain.

A Times of London report last year detailed how two of Russia's most notorious hackers, Maksim Yakubets and Igor Turashev of the Evil Corp group, live a lavish lifestyle in Russia despite being behind the creation and distribution of malware used to steal over $100 million from banks, charities and financial institutions in the last decade.

As a spate of cyber attacks including one that targeted 70 Ukrainian government websites last week suggests that cyber attacks are becoming an ever increasing part of Putin's playbook, the move to institutionalize these skills means captured hackers are seen as a potential asset to state security as opposed to a threat.

"It could be the case that potential hacktivists end up working for the state," said Coleman, adding that it is also worth noting that Russia is better equipped than Belarus to deal with cyber threats.

BCP set out to expose the outdated institutions Lukashenko presides over, said Yulia Shemetovets, a spokeswoman for the group.

"Many entities are not even using licensed software; they use old computers, and the regime doesn't invest enough money into these infrastructures," she told The Moscow Times.

In contrast, Russia pledged 28 billion rubles ($362 million) to cybersecurity in 2020, building a number of “cyber polygons” across the country to expand its cybersecurity training and educational programs.

However, as Coleman pointed out, "security across the board is still not good enough. There are so many weak links."

Government institutions

An October report in the Vedomosti business daily found that 16% of cyberattacks in Russia are carried out by hacktivists with one in five cyberattacks being carried out against government institutions.

While many of these are quickly thwarted, Oleg Skulkin, head of the digital forensics and incident response team at cybersecurity company Group-IB, told The Moscow Times that the threat of hacktivism should not be overlooked.

"The threat of hacktivism should not be underestimated. They are also cybercriminals, it’s just that their motivation is different. Their actions can cause as much damage as the attacks carried out by traditional cybercrime. As we can see, they can use the same methods and employ the exact same tools," Skulkin said.

Although hacktivism does not pose as large a threat to the cyber community as financially motivated hackers, organizations have a greater chance of regaining control of the server when money can be used as a bargaining chip. If hacktivists target you, there is little you can do other than to submit to their demands, he said.

“The high risk nature of hacktivism, and the fact you need skills, means you will never see a truly mass movement in hacking,” Coleman said. That does not mean though that it cannot be used as an important tool for political opposition, she added.

"This is something that has recently entered the cultural imagination," Coleman said, "the BCP are not the first to use sabotage, but they're the first to be well organized and execute it in a very deliberate way. I think they do genuinely believe these tactics can be successfully deployed."

Original url:
https://www.themoscowtimes.com/2022/02/01/hacktivist-cyber-disruption-could-spread-to-russia-experts-believe-a76154