Russian hackers target cash before politics

November 8 2016, by Thibault Marchand

Moscow-based internet security giant Kaspersky has estimated that there are over 1,000 hackers in Russia specialising in financial crime

Just as the scandal over alleged Russian hacking of the US Democratic Party erupted in June, police in Russia were rounding up a group known as Lurk.

In the underground world of Russian hackers, a shadowland of anonymous internet forums where users exchange the latest malware, Lurk was legendary.

The group, active since 2011, was accused of stealing some three billion rubles ($47 million, 42.5 million euros) from Russian banks and aspiring hackers were keen to join.

Then more than 50 members, most of whom hailed from the Urals city of Ekaterinburg, were arrested in a sweeping raid that entailed 86 probes in 15 regions across the vast country.

But despite the eye-catching operation, the crackdown on Lurk only touched the tip of the iceberg of a lucrative criminal industry.

Moscow-based internet security giant Kaspersky has estimated that there are over 1,000 hackers in Russia specialising in financial crimes.

Between 2012 and 2015, by the company's conservative estimate, Russian-speaking hackers stole at least $790 million across the globe.

Meanwhile, this type of illegal activity is flourishing.

"The number of financial cyber criminals is growing as the use of online banking rises," explained Yury Namestnikov, the head of Kaspersky's Russia research and analysis department.

Adding to security woes are also the prevalence of smartphones—which are less well protected than computers—and the rise in "ransomware", a technique that allows hackers to steal data and then ransom it back to the owner.

A picture taken on October 17, 2016 shows employees working at the headquarters of Internet security giant Kaspersky in Moscow

"It is no secret that most of today's crypto-ransomware has Russian roots, both in terms of the authors of the malicious code and of the actors who spread the malware and demand the ransom," Kaspersky noted in a report.

Soviet-style education

For industry experts Russia's dubious honour as a major power in the hacking world is no accident.

"We have good mathematics schools and Russians know how to code properly," said Namestnikov. "What is special about the Russian hackers is that they have been active for so long."

Artem Sychev is in charge of cyber security at Russia's Central Bank and concurs that "Russian-speaking hackers were educated in the Soviet-style system," whose emphasis on high-level maths and science continues today.

"They are most creative people, including unfortunately in the area of fraud," he said.

'Patriot hackers?'

The furore over the US election hacks has shone a spotlight on alleged ties between hackers and the Russian government.

Authorities in Washington have accused top-ranking Russian officials of directing attacks on the US aimed at undermining the election.

CrowdStrike, the security firm that uncovered the hacking of the Democratic National Committee, said that the group behind it, Cozy Bears, was linked to Russian military intelligence.

Authorities in Washington have accused top-ranking Russian officials of directing cyber attacks on the US to undermine the election

Another group, Fancy Bears—which has hacked targets including the World Anti-Doping Agency—meanwhile has ties to the FSB spy agency, according to Crowdstrike.

Russia has dismissed the allegations and said US politicians are blaming Moscow in a bid to drum up their polling numbers.

Local experts insist the vast majority of hacking in Russia is aimed at thieving cash—not interfering in politics.

"99 percent of internet pirates are looking to steal money," said Ilya Sachkov, founder of Russian security firm IB-Group.

"There are no patriotic hackers."

Even while the Kremlin is adamant in denying a role in any of the hacking scandals, the authorities are certainly struggling to tackle the issue—and often appear to turn a blind eye.

"Unfortunately, for Russian-speaking cybercriminals current conditions are more than favourable: the risk of prosecution is low while the potential rewards are high," wrote Kaspersky.

As an example, Russian hacker Yevgeny Bogachev has a $3 million price on his head from the FBI.

His network of hackers—which operated from Ukraine and Russia before being dismantled in 2014—stole more than $80 million from victims mainly in the US.

Despite being wanted, Bogachev reportedly lives freely in the southern Russian city of Krasnodar.

© 2016 AFP

Citation: Russian hackers target cash before politics (2016, November 8) retrieved 29 April 2024 from https://phys.org/news/2016-11-russian-hackers-cash-politics.html