The Moscow Times
30 YEARS
INDEPENDENT NEWS FROM RUSSIA

Hacker Attacks on Russia Gain Attention But Cause Little Damage

By Olexandra Zelenaya

April 29, 2022

Alexei Smyshlyaev / TASS

Two days after the start of Russia's invasion of Ukraine, a group of hackers managed to get access to several Russian state-owned television channels and broadcast anti-war videos.

But the attack ended after a few minutes and regular programming resumed.

This type of fleeting hacking operation has been repeated many times in Russia in recent weeks in apparent retaliation for the Kremlin's decision to attack Ukraine.

But despite the scale of this global cyber-offensive, IT experts told The Moscow Times that its successes have been short-lived and caused little real political or economic damage.

The online offensive against Russia appears to have been carried out by shadowy hacking groups, and it has included data leaks, distributed denial-of-service (DDoS) attacks, anti-war posts on state-owned websites, and even making printers in Russia spew out anti-war messages.

"[Worldwide hacking collective] Anonymous is pursuing a policy of '1,000 pinpricks' with its hacker attacks," said Dennis-Kenji Kipker, an expert on IT security at the University of Bremen. "Although these actions are regularly celebrated as successes, the sustainability of the cyber-attacks is doubtful."

One of the most common forms of online intrusion has been the hacking of major state-owned entities and subsequent data dumps.

Anonymous-affiliated hackers announced last month that they had managed to get access to almost a million emails from VGTRK, a powerful state-run media corporation that operates television channels including Rossia 24. They also leaked the personal data of 120,000 Russian servicemen apparently fighting in Ukraine as well as data from the Culture Ministry, Central Bank and communications regulator Roskomnadzor.

Related article: Russia-Linked Hacking Groups Targeting the U.S.: What You Need to Know

Some of the emails in the leaked VGTRK database revealed details of the media corporation's internal workings, according to Aric Toler, a researcher at investigative outlet Bellingcat.

Toler flagged how VGTRK keeps a watchful eye on foreign media coverage of its own broadcasts, and how Nikolai Patrushev, the secretary of the powerful Security Council, sends physical telegrams to VGTRK on formal occasions.

But while interesting for researchers, the emails have yet to turn up anything politically significant. And the size of the VGTRK leak means it will likely take journalists and investigators many months to comb through all the data.

In addition, it is often unclear whether the leaks are genuine.

Despite Anonymous claiming a successful attack on the Russian Central Bank on March 24, the Bank denied its data had been compromised.

Just 10% of the data breaches claimed by the Anonymous group are likely to be new, according to Igor Bederov, the head of the Internet Rozysk cybersecurity firm.

Another popular tactic has been DDoS attacks on Russian websites, causing shut-downs or delays. DDoS attacks grew fourfold last month, the state-run TASS news agency reported.

"More and more users have been involved in these DDoS attacks," said Bederov. "On the one hand, it was a systematic effort, but on the other, these were very low-quality attacks. Their main strength is in the number of users taking part in them."

In most cases, such attacks are easily stopped by competent IT security teams. However, many have partly succeeded because of the incompetence of developers who didn't properly protect their websites, according to Bederov.

In other cyber-intrusions, Russian web services have been flooded with anti-war ads. Two days after the start of the invasion, viewers on Ivi, a Russian streaming service, saw pictures of war damaged Ukrainian towns and crying children instead of their favorite sitcoms.

The online assault has not gone unnoticed by Russian officials.

Related article: The Battle to Keep Russia's Internet Free

The online assault has not gone unnoticed by Russian officials.

“The scale of the cyberattacks is unprecedented, up to hundreds of thousands a week,” Russian Foreign Ministry spokeswoman Maria Zakharova said earlier this month. “Russia has a lot of reasons to blame the Western countries for funding cyber-criminals.”

However, identifying the culprits is not always straightforward.

One perpetrator is likely to be hacking group Anonymous, which has repeatedly claimed responsibility.

“Russia may be using bombs to drop on innocent people, but Anonymous uses lasers to kill Russian government websites,” one of the hackivist movement’s accounts tweeted two days after the outbreak of war.

“Anonymous is behind the attacks,” said Alexander Lyamin, founder of cybersecurity firm Qrator Labs. “Even the geographic location of servers used for organizing attacks confirms this.”

But other experts are not convinced.

“For sure, Anonymous will be responsible for some of the incidents,” said expert Kipker. “But since anyone can theoretically speak for Anonymous, there will just as certainly be free riders who make mere claims to create political uncertainty.”

Some have also pointed the finger at a “Ukrainian IT Army” that the government in Kyiv set up shortly after the start of the Russian invasion.

Despite their ineffectiveness, the wave of cyber-attacks on Russia marks a shift in hacker tactics, according to analysts.

“The hackers’ actions are dangerous because ultimately what we are witnessing here is interference by private individuals in key global political issues,” Kipker said.

Original url:
https://www.themoscowtimes.com/2022/04/29/hacker-attacks-on-russia-gain-attention-but-cause-little-damage-a77428