TECH

Hacktivist group Anonymous is using six top techniques to 'embarrass' Russia

PUBLISHED THU, JUL 28 2022•6:00 PM EDT UPDATED FRI, JUL 29 2022•4:09 AM EDT

Monica Pitrelli
@MONICAPITRELLI

KEY POINTS

Anonymous uses many strategies in its digital fight against Russia, the most effective being hacking into databases and leaking the information online, according to cybersecurity specialist Jeremiah Fowler.

The size of the leaked data will take years to process.

The hacks have also exposed Russia's cybersecurity defenses to be far weaker than previously believed, say cybersecurity researchers.

In this article

NES.N-CH +0.94 (+0.97%)

Members of the loosely connected collective known as Anonymous are known for wearing Guy Fawkes masks in public.
Jakub Porzycki | Nurphoto | Getty Images

Ongoing efforts by the underground hacktivists known as Anonymous are "embarrassing" Russia and its cybersecurity technology.

That's according to Jeremiah Fowler, co-founder of the cybersecurity company Security Discovery, who has been monitoring the hacker collective since it declared a "cyber war" on Russia for invading Ukraine.

"Anonymous has made Russia's governmental and civilian cyber defenses appear weak," he told CNBC. "The group has demystified Russia's cyber capabilities and successfully embarrassed Russian companies, government agencies, energy companies and others."

"The country may have been the 'Iron Curtain,'" he said, "but with the scale of these attacks by a hacker army online, it appears more to be a 'paper curtain.'"

The Russian embassies in Singapore and London did not immediately respond to CNBC's request for comment.

Ranking Anonymous' claims

Though missile strikes are making more headlines these days, Anonymous and its affiliate groups aren't losing steam, said Fowler, who summarized many of the collective's claims

CNBC grouped Anonymous' claims into six categories, which Fowler helped rank in order of effectiveness:

1. Hacking into databases

Claims:

- Posting leaked information about Russian military members, the Central Bank of Russia, the space agency Roscosmos, oil and gas companies (Gazregion, Gazprom, Technotec), the property management company Sawatzky, the broadcaster VGTRK, the IT company NPO VS, law firms and more
- Defacing and deleting hacked files

Anonymous has claimed to have hacked over 2,500 Russian and Belarusian sites, said Fowler. In some instances, stolen data was leaked online, he said, in amounts so large it will take years to review.

"The biggest development would be the overall massive number of records taken, encrypted or dumped online," said Fowler.

VIDEO 02:55

Anonymous has 'embarrassed' Russian companies and government agencies

Shmuel Gihon, a security researcher at the threat intelligence company Cyberint, agreed that amount of leaked data is "massive."

"We currently don't even know what to do with all this information, because it's something

2. Targeting companies that continue to do business in Russia

Claims:

- Blocking websites of companies identified as continuing to do business in Russia
- Dumping 10GB of emails, passwords and other data belonging to the Swiss food company Nestle. Nestle said these claims have "no foundation."

In late March, a Twitter account named @YourAnonTV began posting logos of companies that were purportedly still doing business in Russia, with one post issuing an ultimatum to pull out of Russia in 48 hours "or else you will be under our target."

By targeting these companies, the hacktivists are upping the financial stakes of continuing to operate in Russia.

"By going after their data or causing disruption to their business, [companies] risk much more than the loss of sales and some negative PR," said Fowler.

3. Blocking websites

Claims:

- Blocking Russian and Belarusian websites
- Disrupting internet connectivity at the St. Petersburg International Economic Forum which delayed Vladimir Putin's keynote speech by some 100 minutes

Distributed denial of service (DDoS) attacks work by flooding a website with enough traffic to knock it offline. A basic way to defend against them is by "geolocation blocking" of foreign IP addresses. By hacking into Russian servers, Anonymous purportedly circumvented those defense mechanisms, said Fowler.

VIDEO 09:15

Could Russia's war on Ukraine escalate into a global cyberwar?

"The owners of the hacked servers often have no idea their resources are being used to launch attacks on other servers [and] websites," he said.

Contrary to popular opinion, DDoS attacks are more than minor inconveniences, said Fowler.

"During the attack, critical applications become unavailable [and] operations and productivity come to a complete stop," he said. "There is a financial and operational impact when services that government and the general public rely on are unavailable."

4. Training new recruits

Claims:

- Training people how to launch DDoS attacks and mask their identities
- Providing cybersecurity assistance to Ukraine

Training new recruits allowed Anonymous to expand its reach, brand name and capabilities, said Fowler.

People wanted to be involved, but didn't know how, he said. Anonymous filled the gap by training low-level actors to do basic tasks, he said.

This allowed skilled hackers to launch more advanced attacks, like those of NB65, a hacking group affiliated with Anonymous which claimed this month on Twitter to have used "Russian ransomware" to take control of the domain, email servers and workstations of a

manufacturing plant operated by the Russian power company Leningradsky Metallichesky Zavod.

LMZ did not immediately respond to CNBC's request for comment.

"Just like in sports," said Fowler, "the pros get the World Cup and the amateurs get the smaller fields, but everyone plays."

5. Hijacking media and streaming services

Claims:

- Showing censored images and messages on television broadcasts, such as Russia-24, Channel One, Moscow 24, Wink and Ivi
- Heightened attacks on national holidays, including hacking into Russian video platform RuTube and smart TV channel listings on Russia's "Victory Day" (May 9) and Russia's real estate federal agency Rosreestr on Ukraine's "Constitution Day" (June 28)

The website for Rosreestr is down, as of today's publication date. Jeremiah Fowler said it was likely pulled offline by Russia to protect internal data after it was hacked. "Russian journalists have often used data from Rosreestr to track down officials' luxury properties."
CNBC

This tactic aims to directly undermine Russian censorship of the war, but Fowler said the messages only resonate with "those that want to hear it."

Those Russian citizens may already be using VPNs to bypass Russian censors; others have

Among those leaving Russia are the "uber rich" — some of whom are departing for Dubai — along with professionals working in journalism, tech, legal and consulting.

6. Directly reaching out to Russians

Claims:

- Hacking into printers and altering grocery store receipts to print anti-war and pro-Ukrainian messages
- Sending millions of calls, emails and text messages to Russian citizens
- Sending messages to users on the Russian social networking site VK

Of all the strategies, "this one sticks out as the most creative," said Fowler, though he said he believes these efforts are winding down.

Fowler said his research has not uncovered any reason to doubt Anonymous' claims thus far.

How effective is Anonymous?

"The methods Anonymous have used against Russia have not only been highly disruptive and effective, they have also rewritten the rules of how a crowdsourced modern cyberwar is conducted," said Fowler.

Information collected from the database breaches may show criminal activity as well as "who pulls the strings and where the money goes," he said.

However, most of the information is in Russian, said Gihon. He said cyber specialists, governments, hacktivists and everyday enthusiasts will likely pore through the data, but it won't be as many people as one might think.

Bill Hinton | Moment Mobile | Getty Images

Gihon also said he doesn't believe criminal prosecutions are likely.

"A lot of the people that they've compromised are sponsored by the Russian government," he said. "I don't see how these people are going to be arrested anytime soon."

However, leaks do build on one another, said Gihon.

Fowler echoed that sentiment, saying that once a network is infiltrated, systems can "fall like dominoes."

Hackers often piggyback off one another's leaks too, a situation Gihon called "the bread and butter" of the way they work.

"This might be a beginning of massive campaigns that will come later on," he said.

The more immediate outcome of the hacks, Fowler and Gihon agreed, is that Russia's cybersecurity defenses have been revealed as being far weaker than previously thought. However, Gihon added that Russia's offensive cyber capabilities are strong.

"We expected to see more strength from the Russian government," said Gihon, "at least when it comes to their strategic assets, such as banks and TV channels, and especially the government entities."

Anonymous pulled the veil off Russia's cybersecurity practices, said Fowler, which is "both

In this article

NES.N-CH +0.94 (+0.97%)

TRENDING NOW

1 **Stocks making the biggest moves premarket: Goldman Sachs, Morgan Stanley, Apple, Boeing and more**

2 **Iowa caucus results: Trump wins, DeSantis edges Haley for second place, Ramaswamy ends campaign**

3 **Burger King owner Restaurant Brands buys chain's largest U.S. franchisee**

4 **The No. 1 in-demand remote job companies are hiring for—it can pay over $100,000 a year**

5 **5 things to know before the stock market opens Tuesday**

Contact

News Tips

Got a confidential news tip? We want to hear from you.

GET IN TOUCH

Advertise With Us

PLEASE CONTACT US

CNBC Newsletters

Sign up for free newsletters and get more CNBC delivered to your inbox

SIGN UP NOW

Get this delivered to your inbox, and more info about our products and services.