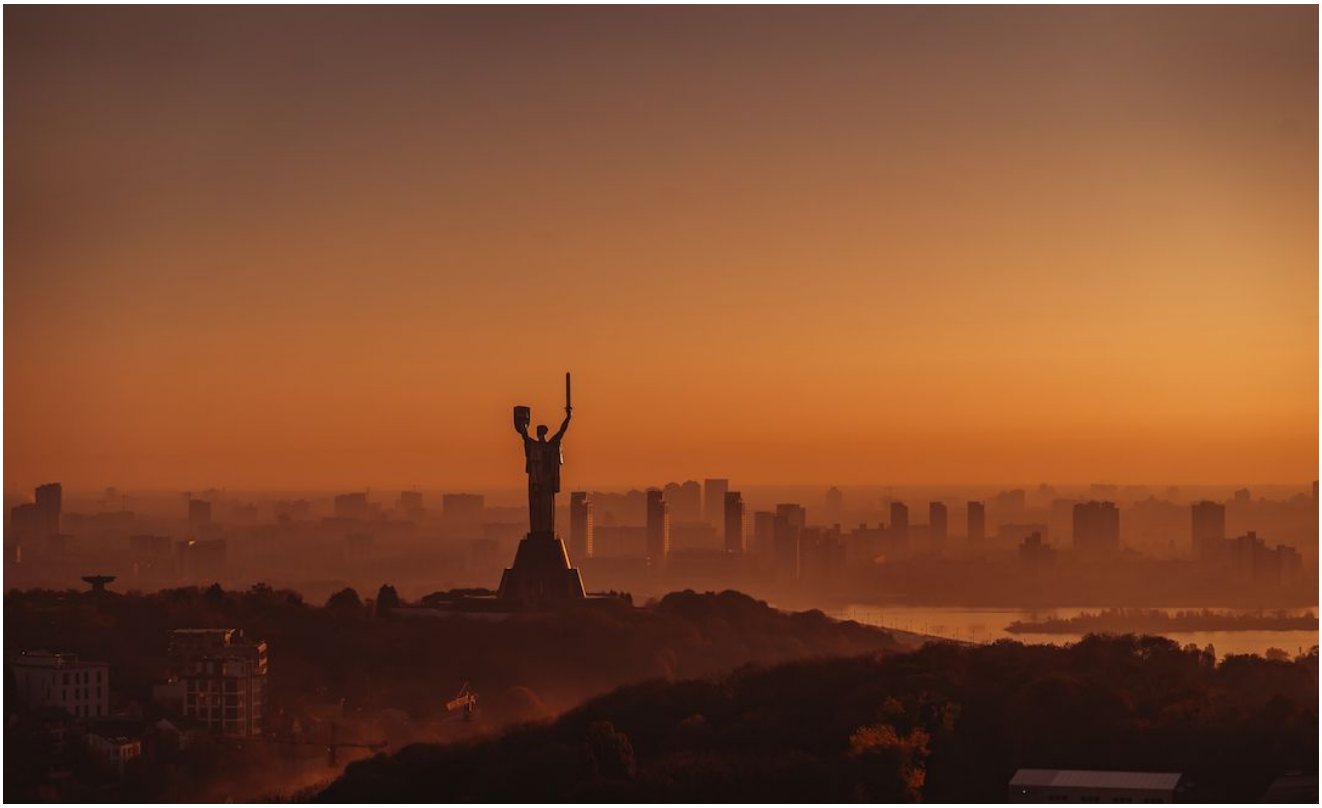
Pro-Ukraine hackers leak Russian data in hopes someone will make sense of it

therecord.media/pro-ukraine-hackers-leak-russian-data-in-hopes-someone-will-make-sense-of-it/



Daryna Antoniuk
January 10th, 2023

In October, investigative journalists at Bellingcat identified a secretive group of Russian military engineers responsible for programming the flight paths of high-precision cruise missiles. Their attacks on Ukraine's critical and civilian infrastructure had left millions of Ukrainians without electricity and heating and caused hundreds of civilian deaths and injuries.

Bellingcat used open-source intelligence and leaked information from Russia's underground data markets to identify people in this group.

Such leaks have proven useful for investigative journalism groups – although it isn't obvious what to do with terabytes of unstructured data, which is extremely difficult to analyze and verify, according to Aric Toler, director of training and research at Bellingcat.

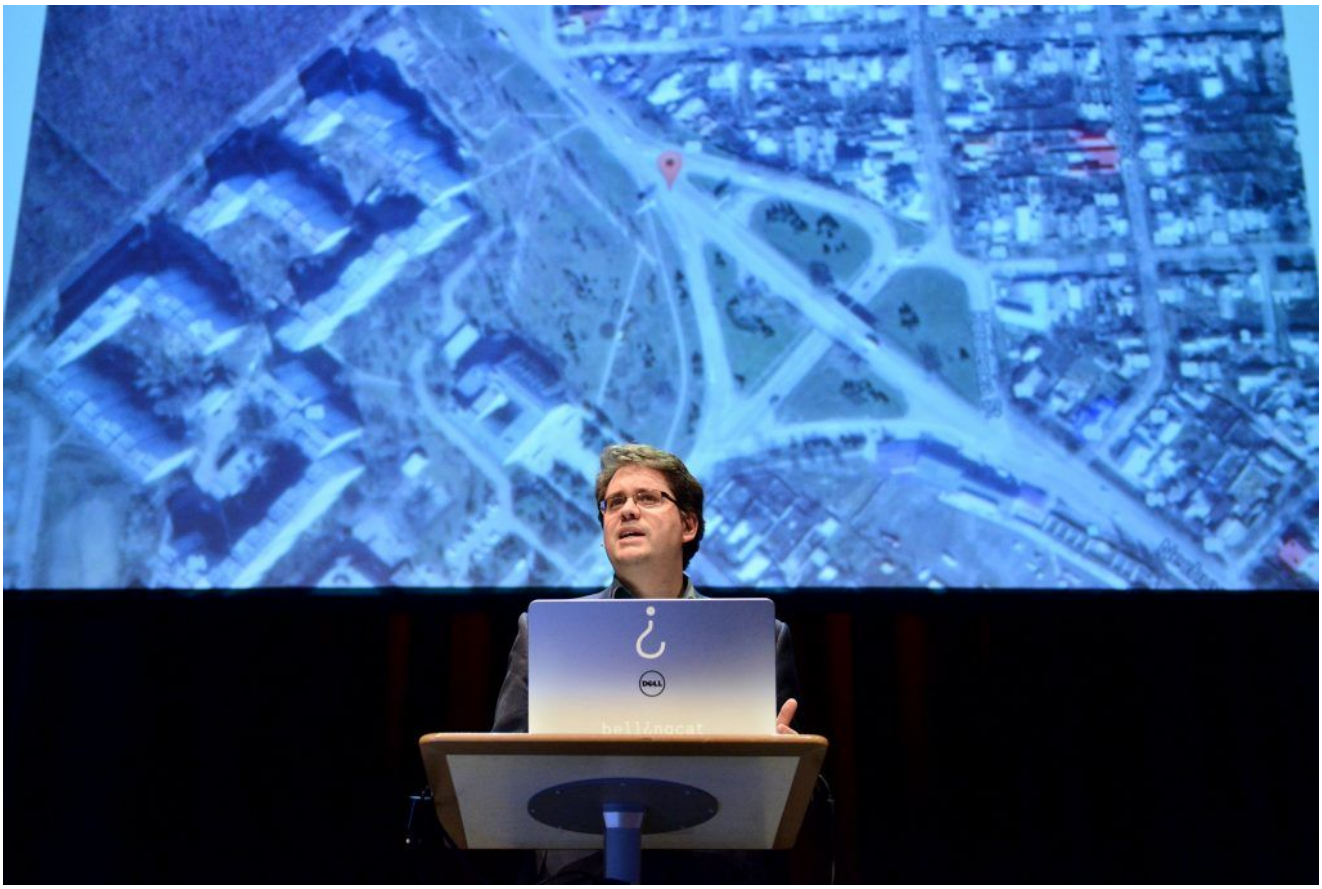
"Most big data dumps have a few interesting nuggets for every hundred or thousand boring, mundane, useless data points," Toler told The Record.

Since the start of the war in Ukraine, Bellingcat has seen a "gigantic surge" of new leaks from pro-Ukrainian hackers against Russia, according to Toler. American investigative reporter Emma Best, a founder of the whistleblower site Distributed Denial of Secrets (DDoSecrets), told The Record in July that hackers had leaked over 12 million Russian documents to the organization since February.

“Ukrainian hackers have data on almost every resident of Russia, even those who do not use a computer,” said Sean Townsend, spokesperson at the Ukrainian Cyber Alliance.

Ukrainian hackers and their allies publish Russian data leaks almost daily. Among their targets are state agencies, such as the Central Bank of Russia and the media monitoring service Roskomnadzor, as well as civil companies such as the taxi aggregator Citymobil or the service for tour operators Level Travel.

Russian hackers also leak data from Ukrainian networks, but these operations often have little strategic value to either side and are primarily useful from a propaganda perspective, said Gavin Wilde, an expert on Russia and information warfare.



Eliot Higgins, the founder of Bellingcat. Image: The Norwegian Foundation for a Free and Investigative Press

“The apparently opportunistic and uncoordinated nature of these operations also creates difficulty in separating potentially valuable insights from useless chaff,” he told The Record.

For Ukrainian hackers, the value and practicality of leaked data are not necessarily the most important thing — they leak data to anger the Kremlin, draw attention to their activities, attract new members and distract their adversaries from more disruptive operations.

Hackers usually leave it up to journalists and intelligence agencies to decide what to do with troves of leaked documents.

“Successful hacking and exfiltration is often the easy part,” said Wilde. “Making sense of mountains of unstructured data is an entirely different ballgame — these collectives seem content to simply pass that burden onto anyone else.”

Regardless of their effect, hack-and-leak operations are a central component of this cyberwar. "These cyberattacks draw out actors driven by everything from pure ego to sincere patriotism, who might have otherwise been reluctant to engage in hacktivism,” Wilde said.

Some of these data leaks can be valuable for journalists or intelligence services down the road.

“Not all of the data is immediately helpful, but it adds to the huge repository of data that already exists in Russia, linking together addresses, names, and phone numbers,” Toler said.

Angry hackers

For many Ukrainian tech specialists, hacking Russia is an emotional thing — they do it out of anger or despair when other ways to fight the enemy are not available.

When Russia launched a massive missile attack on Ukrainian cities on New Year's Eve, Ukrainian hackers wrote on Telegram that they would attack Russian digital infrastructure in response.

The most common types of cyberattacks among Ukrainian hackers and hacktivists are distributed denial-of-service, defacements, and data leaks — these attacks don't require as much skill as more destructive operations, several cybersecurity experts said.

Despite the lack of noticeable influence, hacktivists’ attacks can annoy the Russian government. The Kremlin said in December that it intends to impose fines of up to $7 million on companies affected by data breaches, as well as develop a system that will detect leaked data published on Telegram.

In 2022, hackers leaked more than 1.5 billion lines of personal data of Russian citizens, according to Moscow-based cybersecurity company Kaspersky Lab.

Instead of selling the leaked data on darknet forums, pro-Ukrainian hackers publish it in Telegram channels, such as NLB, DumpForums, or Data1eaks. The most common response from the Russian government to these leaks is to dismiss them – claiming they contain outdated information or data that was already in the public domain.

This is not always true. For example, after hackers from the pro-Ukrainian group NLB published 17 million lines of data leaked from Moscow's e-schooling service earlier in December, the Russian government denied that the database contained data of real users. However, BBC Russia wrote that its reporters looked through the database and found information about their own children inside.

Legitimate targets

The data of Russian schoolchildren is unlikely to help Ukraine win the war, but pro-Ukrainian hackers told The Record that when it comes to Russia, all their targets are “legitimate.”

“Why are the Russians' data hacked? This is because their compatriots came to Ukraine to kill and steal,” Townsend, from the Ukrainian Cyber Alliance, wrote on Telegram. “Anything ending in *.ru* is a legitimate target.”

A hacktivist group from Belarus called the Cyber Partisans also follows this rule when they pass on Russian data to journalists.

“Russia provoked a war that is supported by the majority of the population, so from a moral point of view, we are not worried about the privacy of the data of Russian citizens,” the group’s spokesperson Yuliana Shemetovets told The Record.

When Cyber Partisans leaks the data of Belarusian citizens, they are more careful. “We do not share highly sensitive information, such as passport data of Belarusians, with journalists. Even most Cyber Partisans do not have access to this information,” Shemetovets said.

And while government and intelligence services are a priority for hackers, sometimes the information they get from civilian companies also turns out to be useful.

For example, among the many users affected by a data leak from Yandex Food, a popular food delivery service in Russia, are agents of Russia’s security services and military, who in several cases ordered food to their workplaces using their official email addresses, according to Bellingcat.

> I took a look at the Yandex Food (basically Russian Doordash) leak to see what investigative leads could be found within. Turns out: a lot of FSB officers like to have food delivered to their work, with detailed delivery instructions.
>
> New on @bellingcat: https://t.co/I97rtYNvL6
>
> — Aric Toler (@AricToler) April 1, 2022

To verify the authenticity of this leak, Bellingcat cross-referenced data points to independent sources including social media profiles and other leaked databases. Bellingcat's staff and contributors in more than 20 countries use publicly-available data, social media posts, and leaked documents to investigate a variety of subjects – war crimes, human rights abuses, and organized crime. One of its high-profile investigations helped to identify a key suspect in the Malaysian Airlines Flight 17 accident in 2014.

“A successful data leak is not about hacking one big target, it is about the amount of data obtained,” Townsend told The Record. “With a lot of data, you can find anyone.”

Ukraine’s government uses data obtained from hackers to assemble the so-called “Book of Executioners,” listing Russian soldiers who kill and allegedly torture Ukrainians. Ukraine-based OSINT company Molfar cooperates with hackers to obtain leaked Russian databases, such as those of FSB employees, which it then verifies and sends to journalists.

Analyzing data

When hackers leak data, they rarely care what happens to it next.

“My main task is to gather data and give it to those who know what to do with it,” said Yaroslav Garaguts, founder of the Clarity Project open database. Leaked data is usually used by journalists to conduct investigations or law enforcement agencies to identify suspects, he said.

According to Shemetovets from Cyber Partisans, hacktivists don't have the time or resources to investigate all the data, so they give it to journalists they trust.

“Hacking large databases is a big responsibility,” she said. “This data should be protected by the government, but it fell on the shoulders of Cyber Partisans. We were just lucky that it got into the hands of people with the right values.”

Not all hackers can handle leaked data responsibly. With large data dumps, hackers usually have “a very loose idea of what is in there due to the sheer amount of data (hundreds of gigabytes, at times), along with a possible lack of language and cultural understanding of the content,” Toler said.

Some leaks, on the other hand, are over-curated. “You have to be really careful about verification and considering what the objective of the leakers may be,” Toler told The Record.

Verification of leaked data is a laborious process, according to him. It's not really possible for the giant-mega-ultra dumps of information to be entirely fabricated, but it is possible to sneak a fake bit of data into it.

Destructive attacks

The fact that both Russian and Ukrainian hacktivists are mostly involved in DDoS, defacement, and hack-and-leak operations suggests the limits of both their capabilities and risk tolerance, according to Wilde. “More sophisticated offensive cyber operations are hard to pull off and might draw too much of the wrong kind of attention,” he said.

Some experts believe that these operations are only the tip of the iceberg and that hackers simply do not talk about more serious cyberattacks.

The transition from espionage and data leaks to destructive attacks requires time and sufficient skills, according to Townsend.

“There are many hackers behind Ukraine and they will become more organized and move on to more serious operations that will cause more damage to the Russian IT infrastructure. But this is a slow process,” he said.

- Nation-state News
- News

No previous article

No new articles

Daryna Antoniuk


is a reporter for Recorded Future News based in Ukraine. She writes about cybersecurity startups, cyberattacks in Eastern Europe and the state of the cyberwar between Ukraine and Russia. She previously was a tech reporter for Forbes Ukraine. Her work has also been

published at Sifted, The Kyiv Independent and The Kyiv Post.