Anonymous Challenges Russia's Supposed Cyber Prowess With Repeat Rosatom Breach

By Nica Osorio

Published: 2022-05-13 · Archived: 2026-04-02 12:07:07 UTC

KEY POINTS

- Anonymous hits Russia's nuclear energy behemoth with repeat attack
- This is the second breach of Rosatom in less than 3 months
- Initial set of 10,000 documents from hack to be released
- Leaked information contains contracts with clients, customers' personal information

Apart from vodka, Matryoshka dolls and Vladimir Putin, Russia is also famous — even feared — for its army of hackers. But since Kremlin's invasion of Ukraine in February, Russian government agencies, financial institutions, oil and gas companies and even close circuit cameras across the country have come under relentless cyber attacks from Anonymous, the international decentralized hacking collective and movement.

Anonymous' campaign has been highly effective: it hacked and defaced Russian websites and pried out sensitive information and data from Russia's business and government entities. The collective has promised it will not stop its crusade until the Kremlin ends its war against Ukraine and its latest exploit has been to hack none other than Russia's state-run nuclear energy behemoth Rosatom. Interestingly, it is the second time in less than three months Anonymous has breached Rosatom. The latest attack is bigger than the first one carried out in March, and despite the Kremlin's supposed prowess in the cyber realm, it has not been able to prevent this repeat intrusion into one of its most valued companies.

Anonymous' KelvinSecurity — the same group that hacked Nestle and leaked crucial data of the multinational company and its clients — was also behind the latest Rosatom breach, which scooped out 800,000 documents. Most of the documents are about the nuclear energy company's affiliates and clients.

Rosatom, with a 2020 revenue of $1.2 trillion, specializes in nuclear energy and supplies a fifth of the transcontinental country's electricity. It is also one of the largest exporters of nuclear technology and products in the world.

Hacker man typing on laptop with flag of Russia overlay Jernej Furman/flickr.com

This time, the hacking collective leaked 5.63 GB of data from the Rosatom Customer System. The KelvinSecurity team told *International Business Times* that the breach this time is more damaging to Rosatom than the March hack.

A key KelvinSecurity member who uses the Twitter handle @Ksecureteamlab said this the exploit this time "directly affects (Rosatom's) clients." A different team from the collective had leaked 15.3 gigabytes of data from Rosatom in March, which included an email address hosted on ProtonMail, a free encrypted email provider.

The KelvinSecurity team plans to initially release "about 10,000" documents from the latest hack "to expose the Russian company." This first set of documents, according to the group, impacts the company's clients as it includes contracts with clients and even its customers' personal information and passport details.

The team shared documents from the breach with IBT as proof of their exploit (screenshots below).

Муниципальное унитарное предприятие города Апатиты "Апатитская электросетевая компания"

АКТ

КОНТРОЛЬНОГО СНЯТИЯ ПОКАЗАНИЙ ПРИБОРА УЧЁТА ЭЛЕКТРОЭНЕРГИИ

От 31.03.2022

ящий акт составили:
ставитель МУП "АЭСК" контролер СЭИ
ставитель МУП "АЭСК"
сутствии потребителя, его представителя:

(должность, Ф.И.О.) Телефон: 9646851717, 96468

ор энергоснабжения **5120121026**

Чуркина Наталья Дмитриевна ИП

, что **31.03.2022** в 12 часов 00 минут произведено контрольное снятие заний прибора учёта электроэнергии

объекта Жемчужная ул, д.20, кв.1
ние объекта: Нежилое помещение

альный осмотр:
о установки электросчётчика: В эл. щитке в торговом зале
а подключения прибора учёта: непосредственного/трансформаторного (нужное подчеркнуть)
ические характеристики:

Приборы учета:		Заводской №	Класс точности	Расчётный коэффициент	Государственная поверка	
ид	Марка				от	до
чик	СЕ-101	007805050000306	1.0	-	01.01.2012	01.01.2028

дность счётчика: 5 Нагрузка по фазам каб. линии: "А"_____А, "В"_____А, "С"___

еднее показание РПУ, представленное потребителем 28.02.2022г.	01825
азание прибора учёта при контрольном снятии: 31.03.22г.	04414

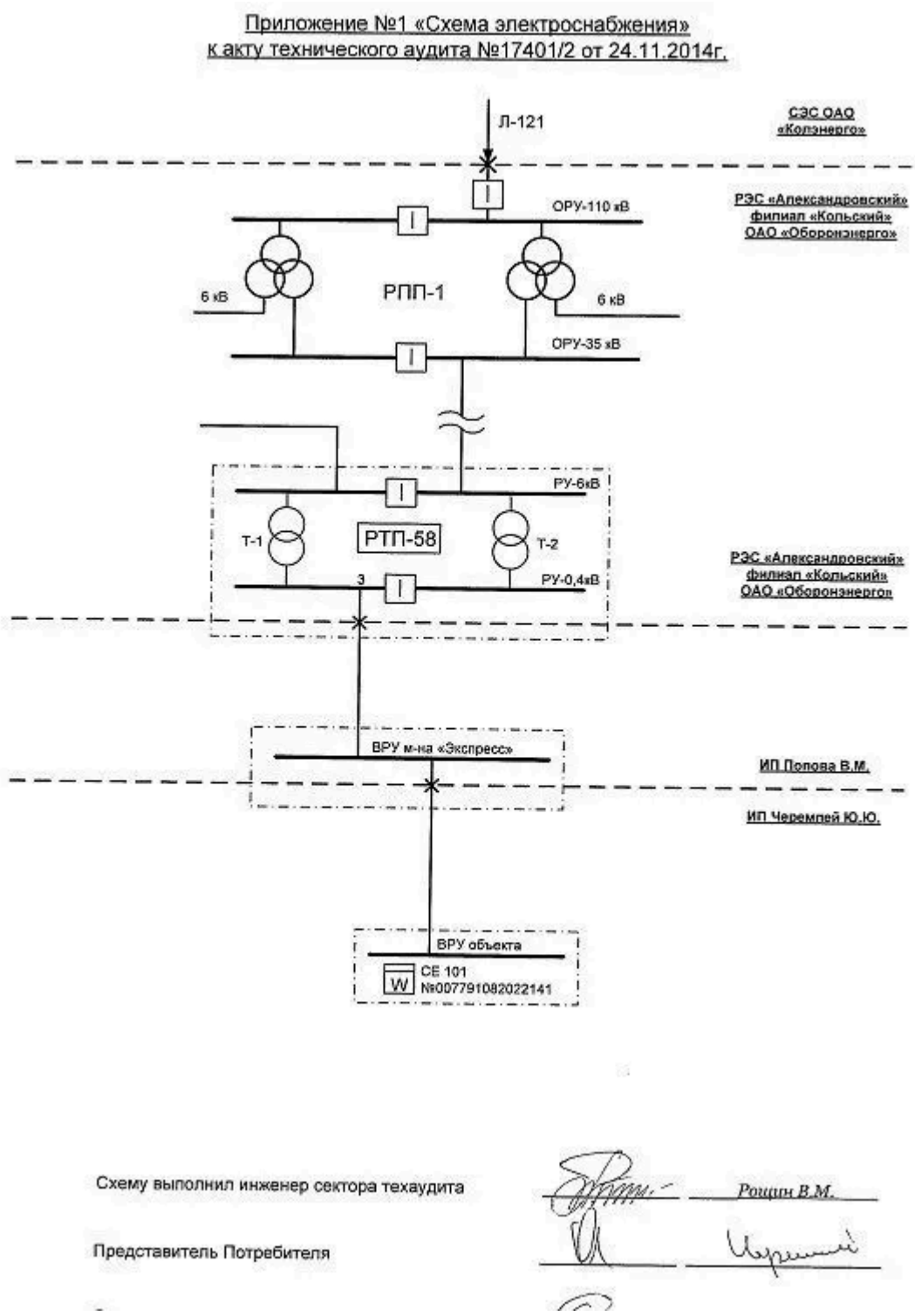
ичие пломб: присутствуют/отсутствуют (нужное подчеркнуть)

ера пломб: РПУ *MP0235479,MP1104592*
аружено безучётное потребление: да/нет (нужное подчеркнуть)
ючение: На момент осмотра зафиксирован и
Конец. показ. на 31.03.22г. - 04414,0

ставитель МУП "АЭСК": **Представитель потребителя:**

33-83, 2-05-44, 2-20-63

Leaked Rosatom document sent by @Ksecureteamlab in Twitter DM



Leaked Rosatom document sent by @Ksecureteamlab in Twitter DM

Among the leaked documents is a passport issued in Uzbekistan (not shown here), while another appears to be a copy of the "Apatity Electric Grid Act (Google translation; Apatity is a town in Murmansk Oblast, Russia). The last one shared with IBT looks like a power supply scheme diagram. The Rosatom leak is now available and those interested can check out this link.

The Anonymous group said it does not have a list of Russian targets to hack, but that it swiftly targets any technology that it identifies as a threat to Ukraine's physical infrastructure — and that it will eventually target any

such Russian technology even if the said tech has not been used to attack any structure in Ukraine.

KelvinSecurity team said that they already have information on the infrastructure and technology Russia is using and businesses that help the Russian army, but the collective has not yet attacked them.

Russia, many analysts think, had prepared to invade Ukraine long before it started what the Kremlin calls a "special military operation." However, it may have failed to anticipate the cyberattacks unleashed on it by Anonymous as part of the group's effort to support Ukraine's fightback.

The West has feared Russia would turn to more destructive cyber attacks as its military attack stalls in Ukraine, and Russian hackers have stepped up their attacks, but the collective was largely dismissive of that effort.

"There are Russian hackers [who] want to attack [using] Conti ransomware in their affiliate program; now they want to increase their capacity but in reality, these hackers do not have political purposes, only financial," Anonymous said. Conti ransomware, believed to be distributed by Russia-based hackers, is considered as an extremely damaging exploit because of its speed in encrypting data and spreading to other systems.

These "pro-Russian hacktivists perform simple attacks like web platform misconfiguration and low-level hacks," @Ksecureteamlab said. "I consider lamers are launching DDoS attack[s] only and some malware infection methods."

logo of KelvinSecurityTeam sent by @@Ksecureteamlab on Twitter DM

"Russian media like Russia Today are launching the campaign that I can personally qualify as an act of revenge since Anonymous attacked the Russian media," @Ksecureteamlab said when asked if Anonymous' actions had triggered the pro-Russian hackers.

@Ksecureteamlab alleged that the Russian media is working with "digital pirates" to falsify images, attack platforms and make their exploits "trend."

Anonymous shared that these actors are either people who identified with Russia and were deeply immersed in the country's brainwashing and propaganda, or "mass media seeking acts of revenge" because they were dismissed, including those who "resigned from these media [outlets], due to their new campaign to support Russia."

Another group, according to Anonymous, is composed of "government actors and intelligence agencies, who want to carry out espionage and malware development to interfere with the physical infrastructure system."

@Ksecureteamlab also shared that these actors have (always) launched ransomware attacks in the U.S. and "their participation, in my opinion, is the same as their daily routine model."

© Copyright IBTimes 2026. All rights reserved.

Source: https://www.ibtimes.com/anonymous-challenges-russias-supposed-cyber-prowess-repeat-rosatom-breach-leaks-data-3505131