



**| Flash |**

# Temporary BreachForums Disruption Claimed by Hacking Group

F-2024-04-17a

Classification: TLP:CLEAR

Criticality: Medium

Intelligence Requirements: Deep and Dark Web, Threat Actor

**April 17, 2024**

**Scope Note:** ZeroFox Intelligence is derived from a variety of sources, including—but not limited to—curated open-source accesses, vetted social media, proprietary data sources, and direct access to threat actors and groups through covert communication channels. Information relied upon to complete any report cannot always be independently verified. As such, ZeroFox applies rigorous analytic standards and tradecraft in accordance with best practices and includes caveat language and source citations to clearly identify the veracity of our Intelligence reporting and substantiate our assessments and recommendations. All sources used in this particular Intelligence product were **identified prior to 9:00 AM (EDT) on April 17, 2024**; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

# Flash | Temporary BreachForums Disruption Claimed by Hacking Group

## › Key Findings

- On April 15, 2024, threat actor “R00TKIT”—in alleged coordination with the “CyberArmyofRussia”—claimed to have taken down BreachForums’ surface web domain. R00TKIT also alluded that it would imminently publish information related to the forum’s users.
- R00TKIT’s involvement was quickly disputed by “Baphomet”, BreachForum’s moderator, who instead blamed “the five eyes network, and various other large nations.” Baphomet also announced the resumption of the forum on a new [.]st top level domain (TLD). As of the time of writing, this site is fully functional.
- BreachForum’s short downtime and R00TKIT’s failure to publish subsequent information as had been threatened indicates there is an unlikely chance R00TKIT was involved.
- There is a roughly even chance that the events were initiated by Law Enforcement (LE) entities as Baphomet claimed. Prior to the disruption, a well-regarded threat actor advertised a data breach composed of allegedly sensitive information, which had a high chance of spurring LE scrutiny.

## Details

On April 15, 2024, BreachForums' surface web domain was taken down. The site's administrator, Baphomet, posted a subsequent PGP-encrypted message to the forum's Telegram channel announcing the suspension of BreachForums[.]cx and added that the forum's [.]onion domain was still functioning. ZeroFox can confirm that the deep and dark web (DDW) domain was not disrupted.

- BreachForums is an illicit hacking forum that hosts discussion surrounding malicious network access and exploitation, as well as the trading of associated goods such as personally identifying information and personal financial information.
- The forum has experienced significant disruption on numerous occasions, including the April 2022 LE takedown of its predecessor Raidforums and the March 2023 LE takedown of BreachForums following the arrest of the site's creator, known as "Pompompurin."<sup>1</sup>

```
BaphometOfficial
copy
-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA512

The domain is currently suspended. We're working on it. We apologise for any inconvenience. We will update you when we know more. :)

Feel free to use tor until this is sorted.

http://breachedu76kdyavc6szj6ppbplfqoz3pgrk3zw57my4vybgbplpfeayd.onion/
-----BEGIN PGP SIGNATURE-----
Version: GnuPG v1

iQIcBAEBCgAGBQJmHZFWAAoJEH1GZpLvDMTIkqEP/0caIKMbeytHX3NUdDmLIFIE
vZoy7yUwbBhBcUR02mGmTyClqPU4xILLCWJCwto6tV2o8hXvzj9/WS8LtDE0+FkM
sxPlD7E0fb4/GPr+LwEmYbQuiWnIUANTfGUT0FbedDqZU955I4igtsUfWESPKY0q
tbjA/GXzR3syIIcYAwFawpBeTchVwYR7N8spQQus7//R5s4lwCttYlr+jH6YJdp+
ojfJF3yt8FI18krVacjFw0Z7BqucqBa9zQG0JVN/dvLf3RgIw4yP0L0Iwy7gwX0
KUnicFrTc8T0CVpLSaU9kd0veQPVGabDU8RnpqgAIKhJt72z3aXNuInBH8fM1e
c/cWv0pQVs8PZKZjRt9wVTMLCtdnWU+5s9ewjqKQ1Iw72fktrr7GRj2/d3xX6eJN
pwRfBXVNNziuxwGtY2qhl0icRKtzQGwQQsiz80ydEve6PX1+t3WifFEK8eNS0nuX
7oN0pfT5zWBDNiH+HputNHKoyd97IKA192ZcfhB9y0Y13NYWd0JtR3JUQpzMEDCnX
V0iyE26stp6aJR24CKTeaYAkmdORDZnBmf6ZWafN3V8WwFEK56MluJU137Jdu44
r07f/k2UI8CQ/iHhoqitD70AV5IRW6eb4zV2uBfw0WItdt0ZXJ3SN7JvJ4y5WnUD
QFP220GN4Wf0vSq/3wx2
=q+gW
-----END PGP SIGNATURE-----
```

### Telegram post by Baphomet announcing the site's suspension

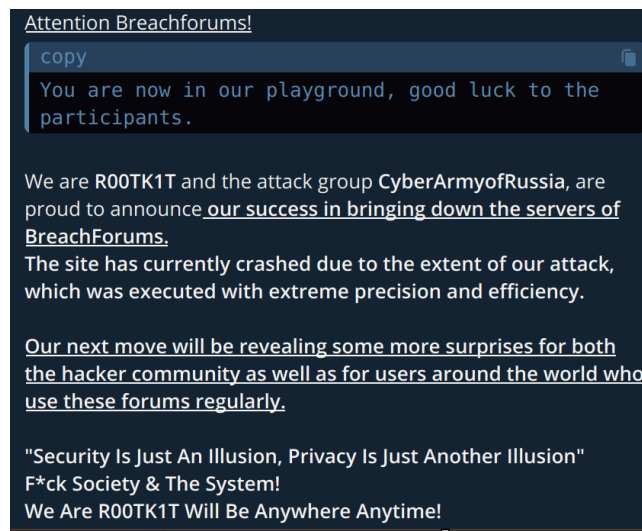
Source: ZeroFox Intelligence

<sup>1</sup>

hXXps://www.justice[.]gov/opa/pr/justice-department-announces-arrest-founder-one-world-s-largest-hacker-for-ums-and-disruption

Threat actor R00TK1T, in alleged coordination with the CyberArmyofRussia, declared responsibility for the site's disruption several hours later in a Telegram post. The group also alluded it would imminently reveal "surprises" aimed at the "hacker community." There is a roughly even chance that this will not take place, however, it could allude to the planned unveiling of a new campaign, motives, or the leaking of doxing information aimed at the forum's users.

- R00TK1T is a financially and ideologically-motivated hacking outfit that has been responsible for data theft and denial-of-service (DoS) attacks against organizations globally, often leveraging vulnerability exploitation and allegedly disgruntled employees.<sup>2</sup>
- The CyberArmyofRussia—which did not comment on the attack except to copy R00TK1T's statement on to its own Telegram page—is a hacking group that is frequently implicated in DoS attacks against Ukrainian targets and the dissemination of pro-Russia propaganda.



## Telegram post by R00TK1T claiming responsibility for the disruption

Source: ZeroFox Intelligence

R00TK1T's involvement was quickly disputed by Baphomet, who instead blamed "the five eyes network, and various other large nations." Baphomet also announced the resumption of the forum on the [. ]st TLD. As of the time of writing, this site is fully functional.

---

<sup>2</sup> [hXXps://www.sangfor\[.\]com/blog/cybersecurity/r00tk1t-hacking-group-malaysia-needs-stronger-cybersecurity](https://www.sangfor[.]com/blog/cybersecurity/r00tk1t-hacking-group-malaysia-needs-stronger-cybersecurity)

- “The five eyes network” almost certainly alludes to an international intelligence-sharing alliance comprising the United States, the United Kingdom, Canada, Australia, and New Zealand.

```
-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA256

Another day, another domain suspension.

Hello everyone.

New Domain: breachforums.st

As you've noticed, our cx domain was suspended. After thorough investigation we've determined this activity as part of not only the "five eyes" network, but various other large nations as well working together to silence our forums.

But not really. Our domain (.cx) was suspended - which is not really new when it comes to running a forum like ours. We currently have a temporary domain available to all users - breachforums.st . As with anytime we experience downtime or a domain suspension, groups of morons take credit for it despite doing literally nothing but smashing their little pig fingers on a keyboard the second any issues happen on our forum. It never helps that various media outlets and Internet personalities quickly post this information as fact without verifying literally anything - great job as always.

This will be the domain for the time being, but we are working on some protections over the next week that'll make these one-time suspensions less effective. Also be aware that with our recent ddos protections in place on the tor site, there should typically be availability at all times for our tor site - if not just refresh your identity within the tor browser and attempt to reconnect.

At this point nothing has been seized, hacked, or even reasonably attacked. There is a chance that we are going to experience DDoS attacks like every other time we come back after any downtime/suspension so just be patient with us. I appreciate the community being patient for the situation as always, so please enjoy our forum.

- - Baph
-----BEGIN PGP SIGNATURE-----
```

## Telegram post by Baphomet announcing the site's suspension

Source: ZeroFox Intelligence

R00TKIT claims to support Russia and Israel, while opposing Iran. This is an unorthodox stance rarely seen amongst Russian-speaking threat groups, highlighted by inconsistencies such as friendly Russian-Iranian relations.

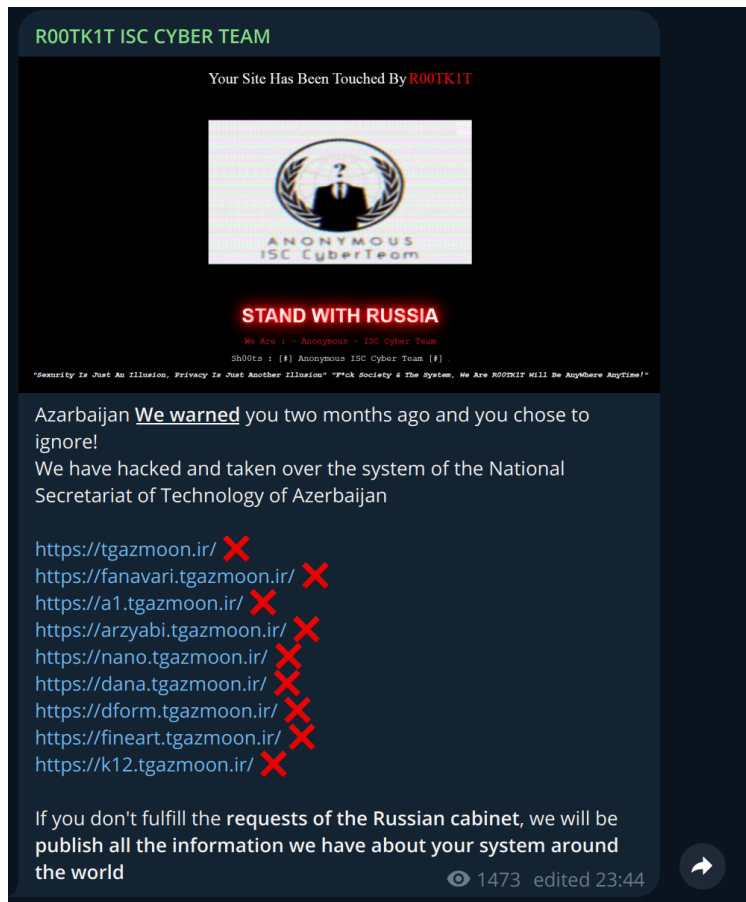
Many of R00TKIT's historical targets are those perceived to be acting against the interests of Russia and Israel.

- R00TKIT has claimed to target numerous Iran-based entities, including a financial exchange system, an educational institution, a hospital, and an overseas logistical company. In early 2024, the group also announced its intent to target Malaysian government entities due to their involvement in the Middle East.<sup>3</sup>
- Entities perceived as being anti-Russia have been targeted, with R00TKIT claiming to have attacked a Chinese drone manufacturer whose products are allegedly being used by the Armed Forces of Ukraine in the ongoing Ukraine-Russia conflict.

---

<sup>3</sup> [hXtps://izologic\[.\]com/region/central-asia/r00tkit-hacking-group-threatens-malaysia-in-its-latest-post/](https://izologic[.]com/region/central-asia/r00tkit-hacking-group-threatens-malaysia-in-its-latest-post/)

The group also claimed credit for defacing an Azerbaijani state website, following a disagreement with the Russian government in October 2023.



### Telegram post by R00TK1T claiming responsibility for defacing an Azerbaijani state website

Source: ZeroFox Intelligence

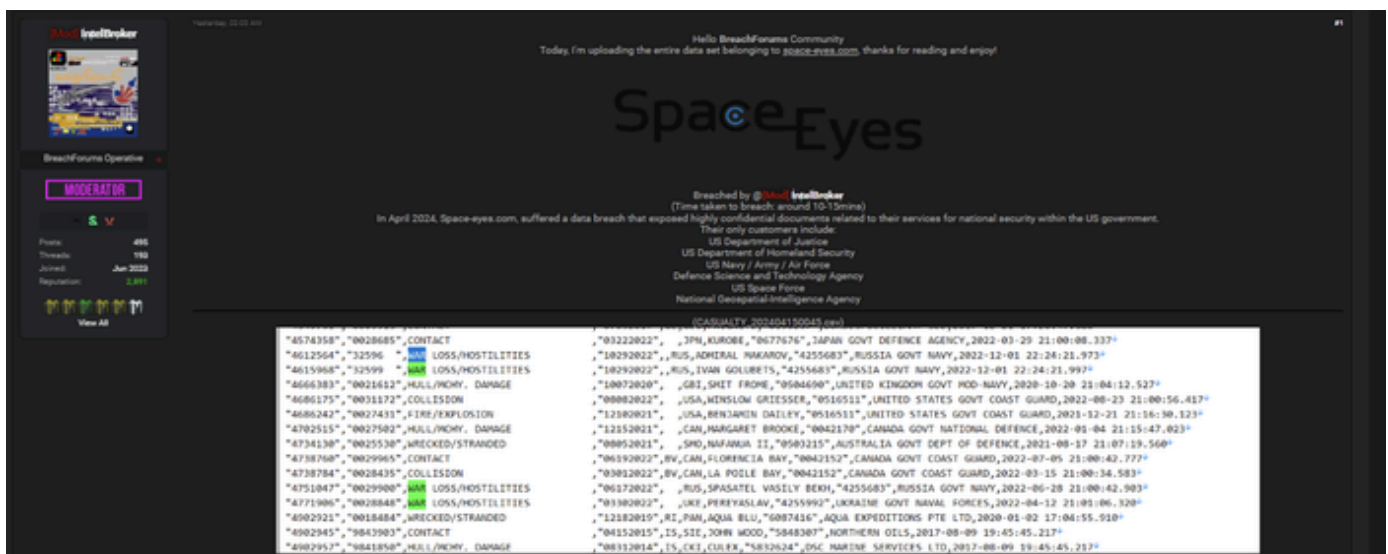
There is a likely chance that the basis for this alignment stems from deeming both the Iranian and Ukrainian governments terrorists; R00TK1T has alluded to the latter on multiple occasions. There is also a roughly even chance that R00TK1T's alleged allegiances are an attempt to generate "non-Russian" support for Russia by routinely undermining the current geopolitical status quo.

As a primarily-English speaking forum, BreachForums is regularly frequented by actors discussing cyberattacks against both Russia and Israel, which R00TK1T almost certainly perceives as justification for its alleged involvement. However, given the forum's short

downtime and the lack of subsequent information posted by R00TKIT as threatened, it is unlikely that R00TKIT was involved in the site's disruption.

This is supported further by a BreachForums post made prior to the disruption by well-regarded threat actor "IntelBroker", who claimed to advertise a leaked database associated with "Space Eyes"—a geospatial intelligence company that almost certainly works with the U.S. government.

Posts of this nature are not uncommon from IntelBroker; however, they are not usually advertised in clear web forums such as BreachForums[.]cx. There is roughly even chance that the sensitivity of this alleged data breach encouraged and facilitated LE activity that resulted in the forum's disruption.



## BreachForums post by IntelBroker

Source: ZeroFox Intelligence

## **Recommendations**

- Organizations should implement training for employees focusing on awareness of contemporary threats, phishing vigilance, social engineering resilience, and basic cybersecurity hygiene.
- Organizations should ensure their web pages and other online content are protected by using secure coding practices and updated security plugins and subjecting them to regular website security audits.
- Websites should be monitored to prevent irrelevant keywords or hidden data from being inserted.
- Implement secure password policies with phishing-resistant multi-factor authentication, complex passwords, and unique credentials.
- Proactively monitor for compromised accounts being brokered in DDW forums.
- Leverage cyber threat intelligence to inform the detection of ransomware and digital extortion (R&DE) threats; their associated tactics, techniques, and procedures (TTPs); and Indicators of Compromise (IOCs).
- Ensure critical, proprietary, or sensitive data is always backed up to secure, off-site, or cloud servers at least once per year—and ideally more frequently.
- Adopt a Zero-Trust cybersecurity posture based upon a principle of least privilege, and implement network segmentation to separate resources.
- Configure email servers to block emails with malicious indicators, and deploy authentication protocols to prevent spoofed emails.
- Deploy a holistic patch management system, and ensure all business IT assets are updated with the latest software as quickly as possible.

## **| Appendix A: Traffic Light Protocol for Information Dissemination**

|                                | <b>Red</b>                                                                                                                                                                                             | <b>Amber</b>                                                                                                                                                                                                                                                                                                                 |
|--------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>WHEN SHOULD IT BE USED?</b> | <b>Sources may use</b><br><b>TLP:RED</b> when information cannot be effectively acted upon by additional parties and could lead to impacts on a party's privacy, reputation, or operations if misused. | <b>Sources may use</b><br><b>TLP:AMBER</b> when information requires support to be effectively acted upon but carries risks to privacy, reputation, or operations if shared outside of the organizations involved.                                                                                                           |
| <b>HOW MAY IT BE SHARED?</b>   | <b>Recipients may NOT share</b><br><b>TLP:RED</b> with any parties outside of the specific exchange, meeting, or conversation in which it is originally disclosed.                                     | <b>Recipients may ONLY share</b><br><b>TLP:AMBER</b> information with members of their own organization and its clients, but only on a need-to-know basis to protect their organization and its clients and prevent further harm.<br><b>Note that</b><br><b>TLP:AMBER+STRICT</b> restricts sharing to the organization only. |
|                                | <b>Green</b>                                                                                                                                                                                           | <b>Clear</b>                                                                                                                                                                                                                                                                                                                 |
| <b>WHEN SHOULD IT BE USED?</b> | <b>Sources may use</b><br><b>TLP:GREEN</b> when information is useful for the awareness of all participating organizations, as well as with peers within the broader community or sector.              | <b>Sources may use</b><br><b>TLP:CLEAR</b> when information carries minimal or no risk of misuse in accordance with applicable rules and procedures for public release.                                                                                                                                                      |
| <b>HOW MAY IT BE SHARED?</b>   | <b>Recipients may share</b><br><b>TLP:GREEN</b> information with peers and partner organizations within their sector or community but not via publicly accessible channels.                            | <b>Recipients may share</b><br><b>TLP:CLEAR</b> information without restriction, subject to copyright controls.                                                                                                                                                                                                              |

## Appendix B: ZeroFox Intelligence Probability Scale

All ZeroFox intelligence products leverage probabilistic assessment language in analytic judgments. Qualitative statements used in these judgments refer to associated probability ranges, which state the likelihood of occurrence of an event or development. Ranges are used to avoid a false impression of accuracy. This scale is a standard that aligns with how readers should interpret such terms.

| Almost No Chance | Very Unlikely | Unlikely | Roughly Even Chance | Likely | Very Likely | Almost Certain |
|------------------|---------------|----------|---------------------|--------|-------------|----------------|
| 1-5%             | 5-20%         | 20-45%   | 45-55%              | 55-80% | 80-95%      | 95-99%         |