



| Brief |

The Underground Economist: Volume 4, Issue 8

B-2024-04-18b

Classification: TLP:CLEAR

Criticality: Medium

Intelligence Requirements: Deep and Dark Web, Phishing

April 18, 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 18, 2024**; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

Brief | The Underground Economist: Volume 4, Issue 8

| Temporary BreachForums Disruption Claimed by Hacking Group

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 identifiable information (PII) and personal financial information (PFI).
- The forum has experienced significant disruption on numerous occasions, including the April 2022 LE takedown of its predecessor Raidforums and the March 2023 law enforcement (LE) takedown of BreachForums following the arrest of the site's creator, known as "Pompompurin."¹

¹

[hXXps://www.justice\[.\]gov/opa/pr/justice-department-announces-arrest-founder-one-world-s-largest-hacker-forums-and-disruption](https://www.justice.gov/opa/pr/justice-department-announces-arrest-founder-one-world-s-largest-hacker-forums-and-disruption)

```
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://breachedu76kdyavc6szj6ppbplfqoz3pgrk3zw57my4vybglpfeayd.onion/
-----BEGIN PGP SIGNATURE-----
Version: GnuPG v1

iQIcBAEBCgAGBQJmHZFWAAoJEH1GZpLvDMTIkqEP/0caIKMbeytHX3NudDmLIFIE
vZoy7yUwbBhBcUR02mGMTyClqPU4xILlCWJCwto6tV2o8hXvzj9/WS8LtDE0+FkM
sxPld7E0fb4/GPr+LwEmYbQuiWnIUANTfGUT0FbedDqZU955I4igtsUfWESPKY0q
tbjA/GXzR3syIicYAwFawpBeTchVwYR7N8spQQus7//R5s4lwCttYlr+jH6YJdp+
ojfJF3yt8FI18krVacjFrw0Z7BqucqBa9zQGDJVn/dvLf3RgIw4yP0L0Iwy7gwX0
KUinicFrTc8T0CvPlSaU9kd0veQPVGabDU8RnpqgAIKhJt72z32aXNuInBH8fM1e
c/cWv0pQVs8PZKZjRt9wVTMLCtdnWU+5s9ewjqKQ1Iw72fktrr7GRj2/d3xX6ejN
pwRfBXVNNziuxwGtY2qhLoicRKtzQGw0Qsiz80ydEve6PX1+t3Wi fFEK8eNS0nuX
7oN0pfT5zWBDNih+HputNHKoyd97IKA192Zc fhB9y0Y13NYWd0JtRJUQpzMEDCnX
V0iyE26stp6aJR24CKTeEaYAkmdORDZnBmf6ZWafN3V8WwFEK56MLujU137Jdu44
r07f/k2UI8CQ/iHhoqitD70AV5IRW6eb4zV2uBfw0WIdt0ZXJ3SN7JvJ4y5WnUD
QFP220GN4Wf0vSq/3wx2
=q+gW
-----END PGP SIGNATURE-----
```

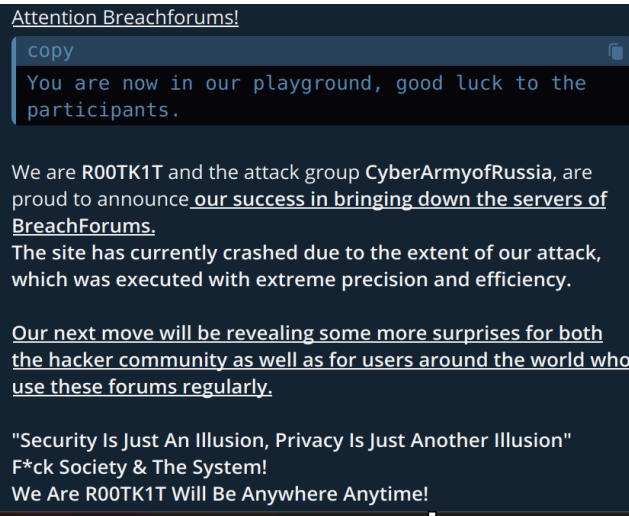
Telegram post by Baphomet announcing the site's suspension

Source: ZeroFox Intelligence

Threat actor "R00TK1T", in alleged coordination with "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 doxxing 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.²
- 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.

² [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)



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 top-level domain (TLD). As of the time of writing, this site is fully functional.

- "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

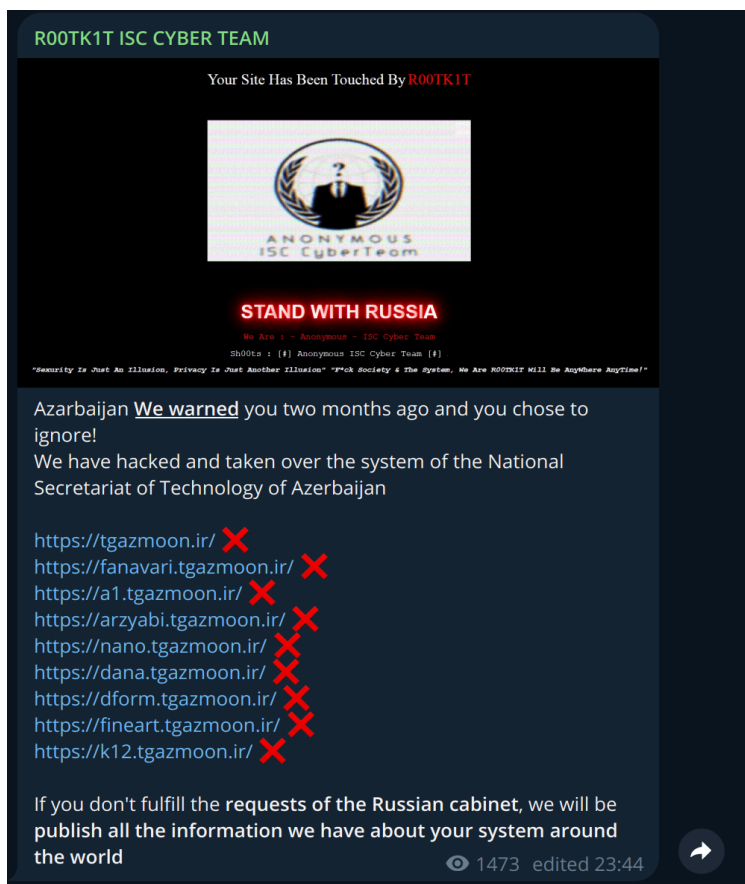
Source: ZeroFox Intelligence

R00TK1T 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 R00TK1T's historical targets are those perceived to be acting against the interests of Russia and Israel.

- R00TK1T 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.³
- Entities perceived as being anti-Russia have been targeted, with R00TK1T 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. The group also claimed credit for defacing an Azerbaijani state website, following a disagreement with the Russian government in October 2023.

³ [hxxps://izoologic\[.\]com/region/central-asia/r00tk1t-hacking-group-threatens-malaysia-in-its-latest-post/](https://hxxps://izoologic[.]com/region/central-asia/r00tk1t-hacking-group-threatens-malaysia-in-its-latest-post/)

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

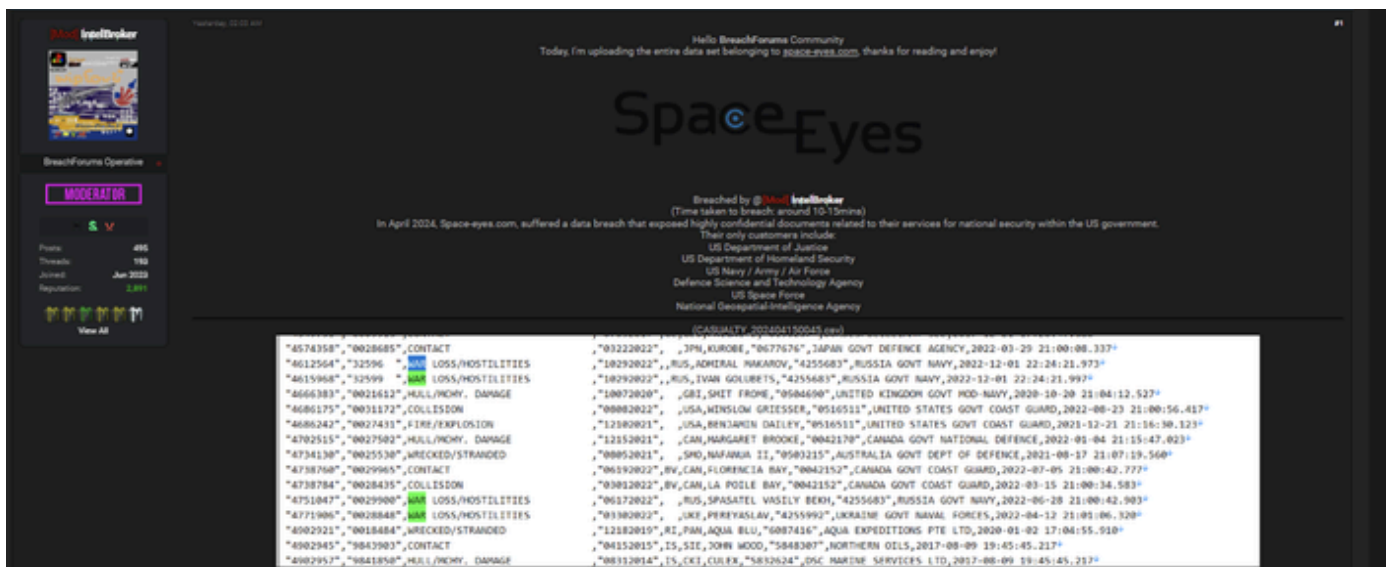
Source: ZeroFox Intelligence

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 R00TK1T as threatened, it is unlikely that R00TK1T 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

Hacktivist Group SiegedSec Announces New Campaign

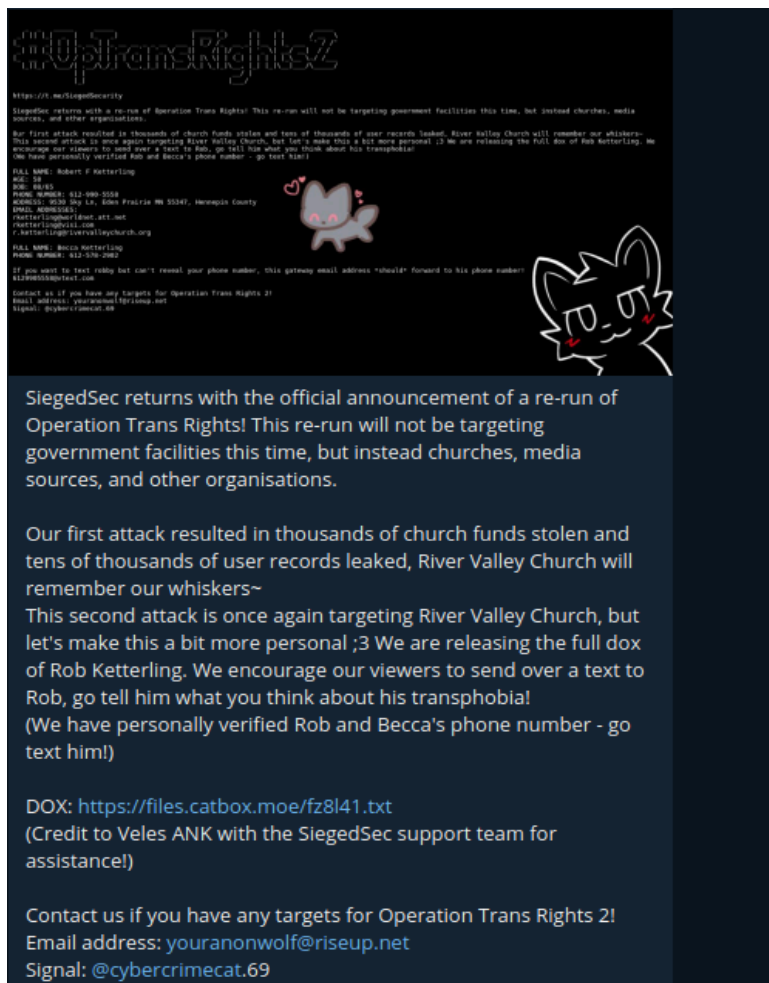
On April 8, 2024, hacktivist group SiegedSec posted on its Telegram channel announcing the start of a new campaign dubbed “Operation Trans Rights 2.” The post claims that SiegedSec intends to target churches, media companies, and other organizations perceived to be infringing on the rights of transexual individuals and communities.

- SiegedSec is a hacktivist group that was first observed in approximately April 2022, and often refer to themselves as the “gay furry hackers.”

- The group was initially a member of the “The Five Families”, a unified hacker collective that has conducted financially, ideologically and politically motivated attacks against organizations across the globe. Aside from SiegedSec, The Five Families collective consists of hacktivist groups ThreatSec, Stormous, and GhostSec as well as Blackforums, a DDW forum used for illicit discussion and trading.
- In December 2023, Sieged Sec was removed from The Five Families following the post of a statement appearing to promote paedophilia. The group subsequently claimed that its page was defaced, denying any involvement.

During 2023, SiegedSec conducted data theft and disruption attacks against organizations deemed to be promoting an anti-transsexual, or right wing political agenda. Targets included several U.S. state governments as well as legal, scientific, and religious institutions. The group also conducted data theft attacks against the Community of Interest Cooperation Portal and The Lessons Learned Portal belonging to the North Atlantic Treaty Alliance (NATO).

Over the coming months, it is almost certain that SiegedSec will attempt to conduct attacks against similar institutions. Attacks will very likely be aimed most often at causing disruption, defacing digital property, undermining, and the doxxing of associated individuals—particularly those who are outspoken regarding beliefs that could be perceived as anti-transsexual. Stolen information is very likely to be leaked or sold in DDW marketplaces, with an unlikely chance that the victim may be extorted first.



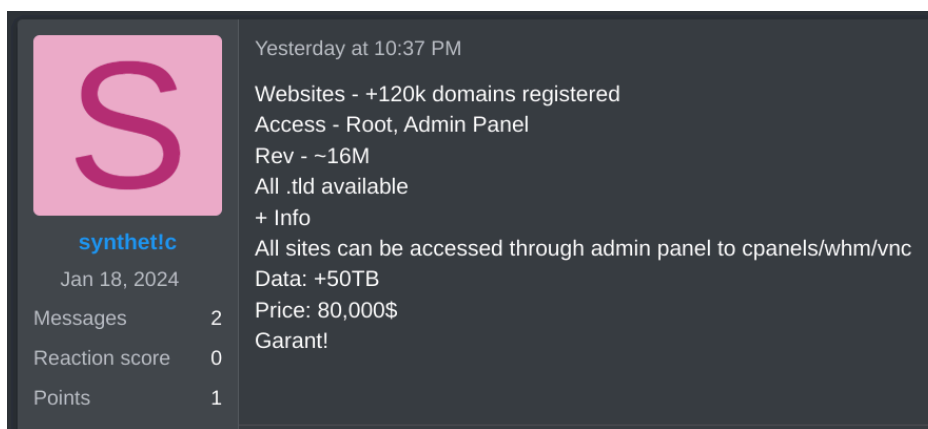
SiegedSec Telegram post announcing Operation Trans Rights 2

Source: ZeroFox Intelligence

Access to U.S. Web Hosting Organization Advertised in Deep and Dark Web Forum

On April 8, 2024, untested threat actor “synthetic” posted in the DDW platform RAMP advertising access to a U.S.-based web hosting organization that has an annual revenue of approximately USD 16 million. According to the post, the victim organization is in the “General Telecommunications Hosting” industry and currently hosts over 120,000 web domains.

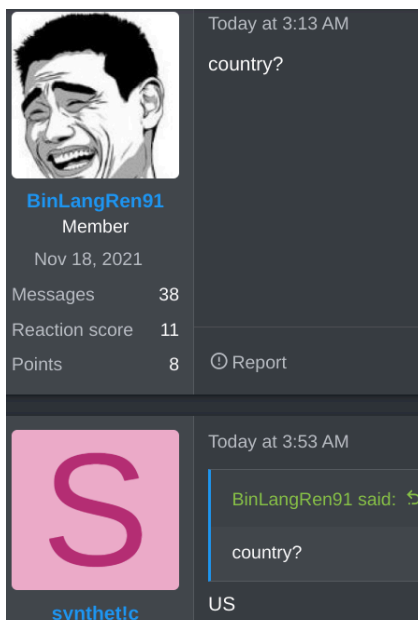
Synthetic claims that the buyer will receive administrative access to all hosted web pages, which could number in the hundreds of thousands and belong to hundreds to thousands of separate organizations. The access is enabled through web hosting tools cPanel, WebHost manager (WHM), and Virtual Network Computing (VNC).



RAMP post advertising initial access sale

Source: ZeroFox Intelligence

Fifty terabytes of data are also included in the sale, which very likely includes PII and PFI of employees and customers extracted from the hosted web pages.

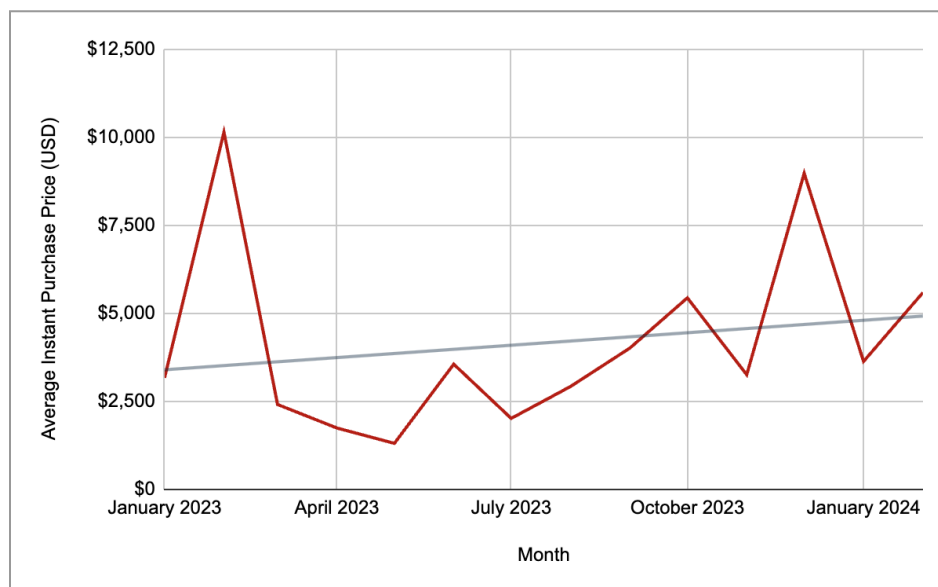


RAMP post specifying the victim region

Source: ZeroFox Intelligence

The asking price for the initial access is USD 80,000, which is significantly higher than the typical price tag for initial access to an organizational network. This is almost certainly due to the notably high potential financial return for the successful exploitation of such significant access.

- Between January 2023 and April 2024, the average asking price for illicit initial access sales publicized in DDW forums xss, Exploit, and RAMP was approximately USD 8,000.
- The requested asking price of initial access is a reflection of the potential lucrativeness of the network access. This almost certainly takes into account factors such as the victim organization's annual revenue, the type of access (virtual private network, remote desktop protocol, etc.), and any associated privileges that enable faster exploitation.



Average instant purchase price of initial access sales

Source: ZeroFox Intelligence

The description included in the advertisement suggests there is a likely chance that the victim is a web or cloud hosting organization with access to significant quantities of customer data.

Privileged access to the web hosting tools of an organization's website can enable a threat actor to conduct an array of subsequent malicious activity.

- The victim organization could be targeted in a digital extortion attack, whereby the buyer leverages ransomware to extract significant payment in exchange for the alleged deletion of the data. This would likely cause financial, operational, and reputational damage.
- The threat actor may target the victim's clients and associates by leveraging techniques such as cross-site scripting or SQL injection against their hosted web pages. The attacker could then move laterally toward the organizations' own servers, putting them at risk of data theft or phishing attacks.
- The end users of the compromised web pages' services could also be targeted, resulting in phishing, impersonation attacks, or fraudulent activity. Their stolen information could also be used to extort the web page owners in large-scale ransomware attacks, leveraging techniques similar to those enacted by threat group CI0p during 2023 campaigns.⁴

Synthetic is not an active user in RAMP, but the advertisement indicates that sales will take place using the forum's escrow service—significantly increasing the credibility of both the sale and the actor. Due to their limited exposure and the nature of the advertised access, there is a roughly even chance that synthetic is an insider and selling information gained through implicit access and trust.

| Bassterlord Returns to Sell Third Malicious Publication

On April 7, 2024, username "mazzon" (almost certainly an account associated with the threat actor "Bassterlord") posted in the the DDW forum xss. The thread addressed multiple topics and was locked shortly after it was posted following a request from the author.

Bassterlord is a positive-reputation threat actor that has been active in DDW forums since approximately 2019 and has been involved in various nefarious activities.

- The actor has previously described themselves as an "Access Broker" and has published two separate manuals titled "Nobody will tell you this" (versions 1.0 and 2.0). The documents, which were leaked in Q2 2023, provide guidance such as how

⁴ [hXXps://zf-dashboard-media.s3.amazonaws.com/intel/d4545937-a245-4dcd-ad06-1b2dc46860e8](https://zf-dashboard-media.s3.amazonaws.com/intel/d4545937-a245-4dcd-ad06-1b2dc46860e8)

to breach the networks of organizations and were generally well-received and highly regarded by their target audience.

- Bassterlord has almost certainly been heavily involved with prominent threat groups LockBit, REvil, and Avadon, including leveraging their malware in ransomware and digital extortion (R&DE) attacks.⁵
- Since 2020, Bassterlord has authored periodic threads and blog posts both in DDW forums and on open source social media platforms, as well as conducted interviews with cybersecurity researchers.⁶

v.3.0 Мануал по работе с сетями "Этого вам никто не расскажет!"
mazon · Yesterday at 12:53 PM · bassterlord · nationalhazardagency · доступы · мануал

ESCROW AVAILABLE IN THIS THREAD!

New deal



mazon
HDD-drive
User
Joined: Sep 4, 2023
Messages: 25
Reaction score: 5

Yesterday at 12:53 PM

Price: 2000-150000
Contacts: 35BD565F38BD0DC0DF6DD7C3BA8648B015B7ACA1CC263A12B8737F406B3B2A118B6264C48AAA

"Long post", "many", "too lazy to read"
So, a little bit of history about the NHA
After the well-known events and the publication of sanctions
<https://xss.is/threads/108621/>
[Sanctions List Search](#)

Exploit post by mazon

Source: ZeroFox Intelligence

The recent thread provides a general update covering the threat actor and their affiliated group, the NHA. Bassterlord claims that, following the February 2024 LE disruption of LockBit, the NHA was under close surveillance by the Federal Bureau of Investigations (FBI). This led to the seizure of all of NHA's funds (including those stored in Monero, referred to as XMR).

The NHA subsequently destroyed "everything they could", which very likely refers to the disbanding of its associated digital infrastructure and the cessation of operations.

⁵

[hXXps://www.bleepingcomputer.com/news/security/tsmc-denies-lockbit-hack-as-ransomware-gang-demands-70-million/](https://www.bleepingcomputer.com/news/security/tsmc-denies-lockbit-hack-as-ransomware-gang-demands-70-million/)

⁶ [hXXps://therecord.media/bassterlord-interview-hacker-initial-access-broker](https://therecord.media/bassterlord-interview-hacker-initial-access-broker)

- Following the LE operation, an indictment was issued by the U.S. District Court that gives an overview of Bassterlord's suspected malicious activity.⁷
- Bassterlord outlines some of the techniques, tactics, and procedures (TTPs) leveraged by the FBI during the operation, alluding to the fault lying with the insufficient practices of affiliates.

ZeroFox has observed two previous instances in which Bassterlord claims to be ceasing activities and quitting the R&DE marketplace.

- There is a roughly even chance that recent LE scrutiny resulted in a genuine attempt by Bassterlord to "retire." It is likely, however, that these statements are intended as disinformation aimed at LE and security researchers.

The thread also sought to advertise the release of Bassterlord's most recent publication, "Nobody will tell you this V3.0." The new manual allegedly assists R&DE operatives in mass brute force targeting of corporations, including how to "organize" attacks, and also allegedly includes "the latest developments of the access mining team."

- Previous iterations of the manual are widely considered as educational and designed for those that are "new to the subject." In a 2023 interview, Bassterlord reportedly claimed that even an individual with minimal experience could conduct a ransomware attack if in possession of V1.0 and V2.0.⁸
- The publication is very likely aimed at educating malicious actors in the targeting of organizational VPN portals. During 2023, ZeroFox Intelligence observed an increase in DDW announcements pertaining to the sale of various checkers and brute force tools designed to compromise corporate VPN networks.

⁷ [hXXps://www.justice\[.\]gov/usao-nj/media/1338926/dl?inline](https://www.justice.gov/usao-nj/media/1338926/dl?inline)

⁸ [hXXps://therecord\[.\]media/bassterlord-interview-hacker-initial-access-broker](https://therecord[.]media/bassterlord-interview-hacker-initial-access-broker)

As for the 3rd part, it will be very short, but informative with software for work and self-written scripts for processing, and all this for the price of 1 good access - \$2000 AT THE MOMENT, WE ARE CONSIDERING PEOPLE SELLING TO ONE PERSON FOR \$150,000 If there are a lot of people, we will sell in parts of 2 to

1 The manual gave an opportunity and shed light on the topic of rans in general

2 The manual showed how careless sysadmins can be and caused a certain trend for brute corp networks, which led to the sale of checkers and brute corp accesses.

After the method was published on the forum in the open, the mana was available in the public, since there was no point in hiding the method itself. Everyone who provided correspondence with me to TOX was refunded.

(There was no scammer)

3 The manual will show you how to assemble the necessary companies and how to organize a targeted attack on them. It contains the latest developments of the access mining team.

"The theme of the manual is mass targeted brute force of corporations"

I have a premonition of another buhurt on the forum on this occasion =D

We will go through any checks and provide the manual personally to the XSS ADMIN if necessary

PRIORITY! I will consider a one-person sale with a large price tag of \$150,000 strictly through the guarantor of the forum at your expense.

This post was created by the NHA

team And last but not least, the old TOXS NHA and Busterre can sit FBI, however, the information is not accurate For safety, a new toks has been created for contacts in the P.M.

ALL TRANSACTIONS ARE CARRIED OUT THROUGH THE GUARANTOR OF THE FORUM AT YOUR EXPENSE!

I remind you that the topic is strictly commercial and if you have any questions, you can ask them in the tox

35BD565F38BD0DC0DF6DD7C3BAB648B015B7ACA1CC263A12B8737F406B3B2A118B6264C48AAA

Advertisement of "Nobody will tell you this V3.0"

Source: ZeroFox Intelligence

The asking price for V3.0 is advertised as USD 2,000, though a buyer may remove the product from the market for USD 200,000. Transactions use the forum's guarantor.

- There is a roughly even chance that Bassterlord's recent claim they are ceasing activities is an attempt to boost sales of their new publication.
- There is a roughly even chance that the subsequent locking of the thread is indicative of a single buyer making an exclusive purchase. It may also have been purchased by a competing threat actor seeking to remove it from the marketplace and gain exclusive access to the information.

| Recommendations

- Adopt a Zero-Trust cybersecurity architecture based upon a principle of least privilege.
- Implement network segmentation to separate resources by sensitivity and/or function.
- Implement secure password policies with phishing-resistant multi-factor authentication (MFA), complex passwords, and unique credentials.
- Leverage cyber threat intelligence to inform the detection of relevant cyber threats and associated TTPs.
- 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.
- Develop a comprehensive incident response strategy.
- Configure email servers to block emails with malicious indicators and deploy authentication protocols to prevent spoofed emails.
- Deploy a holistic patch management process and ensure all IT assets are updated with the latest software updates as quickly as possible.
- Proactively monitor for compromised accounts being brokered in deep and dark web forums.
- Configure ongoing monitoring for Compromised Account Credentials.

| Appendix A: Traffic Light Protocol for Information Dissemination

WHEN SHOULD IT BE USED?

Red

Sources may use

TLP:RED 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.

Amber

Sources may use

TLP:AMBER when information requires support to be effectively acted upon but carries risks to privacy, reputation, or operations if shared outside of the organizations involved.

HOW MAY IT BE SHARED?

Recipients may NOT share

TLP:RED with any parties outside of the specific exchange, meeting, or conversation in which it is originally disclosed.

Recipients may ONLY share

TLP:AMBER 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.

Note that

TLP:AMBER+STRICT restricts sharing to the organization only.

Green

WHEN SHOULD IT BE USED?

Sources may use

TLP:GREEN when information is useful for the awareness of all participating organizations, as well as with peers within the broader community or sector.

Clear

Sources may use

TLP:CLEAR when information carries minimal or no risk of misuse in accordance with applicable rules and procedures for public release.

HOW MAY IT BE SHARED?

Recipients may share

TLP:GREEN information with peers and partner organizations within their sector or community but not via publicly accessible channels.

Recipients may share

TLP:CLEAR 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%