



| Flash |

Bassterlord Returns to Sell Third Malicious Publication

F-2024-04-12a

Classification: TLP:CLEAR

Criticality: Medium

Intelligence Requirements: Deep and Dark Web, Threat Actor, Ransomware and Digital Extortion

April 12, 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 12, 2024**; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

| Flash | Bassterlord Returns to Sell Third Malicious Publication

> Key Findings

- On April 7, 2024, threat actor “Bassterlord” posted in the the deep and dark web (DDW) forum xss. The thread addresses multiple topics but was locked shortly after upon the author’s request.
- Bassterlord claims that following the February 2024 law enforcement (LE) disruption of LockBit, their associated group, the National Hazard Agency (NHA), was under close surveillance by the Federal Bureau of Investigation (FBI). This led to the seizure of all of NHA’s funds (including those stored in XMR) and the cessation of NHA’s operations.
- A new educational manual was also advertised for sale, which allegedly assists threat actors in mass brute force targeting of corporations, including how to “organize” attacks.

| Details

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 different 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 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.¹
- 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.²

v.3.0 Мануал по работе с сетями "Этого вам никто не расскажет!"

mazzon · Yesterday at 12:53 PM · bassterlord · nationalhazardagency · доступны · мануал

ESCROW AVAILABLE IN THIS THREAD!

New deal



mazzon
HDD-drive
User

Joined: Sep 4, 2023
Messages: 25
Reaction score: 5

Yesterday at 12:53 PM

Price: 2000-150000
Contacts: 35BD565F38BD0DC0DF6DD7C3BAB648B015B7ACA1CC263A12B8737F406B3B2A118B6264C48AAA

"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

Xss post by mazzon

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

¹

[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/)

² [hXXps://therecord.media/bassterlord-interview-hacker-initial-access-broker](https://therecord.media/bassterlord-interview-hacker-initial-access-broker)

disruption of LockBit, the NHA was under close surveillance by the FBI. This led to the seizure of all of NHA's funds (including those stored in 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.

- Following the LE operation, an indictment was issued by the U.S. District Court that gives an overview of Bassterlord's suspected malicious activity.³
- 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 V2.0.⁴
- 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.

³ [hXXps://www.justice\[.\]gov/usao-nj/media/1338926/dl?inline](https://www.justice.gov/usao-nj/media/1338926/dl?inline)

⁴ [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

- Implement secure password policies with phishing-resistant multi-factor authentication, complex passwords, and unique credentials.
- Configure ongoing monitoring for Compromised Account Credentials.
- Proactively monitor for compromised accounts being brokered in DDW forums.
- Leverage cyber threat intelligence to inform the detection of R&DE threats, their associated 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.
- Implement network segmentation to separate resources.
- 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 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

	Red	Amber
WHEN SHOULD IT BE USED?	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.	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	Clear
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.	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	Recipients may share TLP:CLEAR information without restriction, subject

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%