



| Profile |

IntelBroker

P-2024-01-24a

Classification: TLP:GREEN

Criticality: Medium

Intelligence Requirements: Deep and Dark Web & Criminal Underground, Ransomware, Threat Actor Targeting

ZeroFox disclaimer: This threat actor appears to espouse views, be involved with groups, and use speech and terms that are offensive and do not in any way represent the views of ZeroFox. In an effort to maintain accuracy in reporting, we have not redacted or altered these offensive names in our report.

January 24, 2024



Profile | IntelBroker

Created on: January 17, 2024

Intelligence Cut-off: 12:00 PM (EST) on
January 17, 2024

First Observed	October 2022
Possible Origin	Serbia
Aliases	ClamAV, ATF, Nationalist, IntelCN, Zoran, mr.bumpkin, leetacro, wezlk, TheKilob
Motivation	Financial, Ideological, Information Theft, Sabotage
Targeted Industries	All Industries
Targeted Nations	United States, India, United Kingdom, Indonesia, Japan, Netherlands, Vietnam, Russia, France, Australia, Canada, United Arab Emirates, Lithuania, Guatemala, Luxembourg, Singapore, Sweden, Côte d'Ivoire
Tools	Endurance ransomware

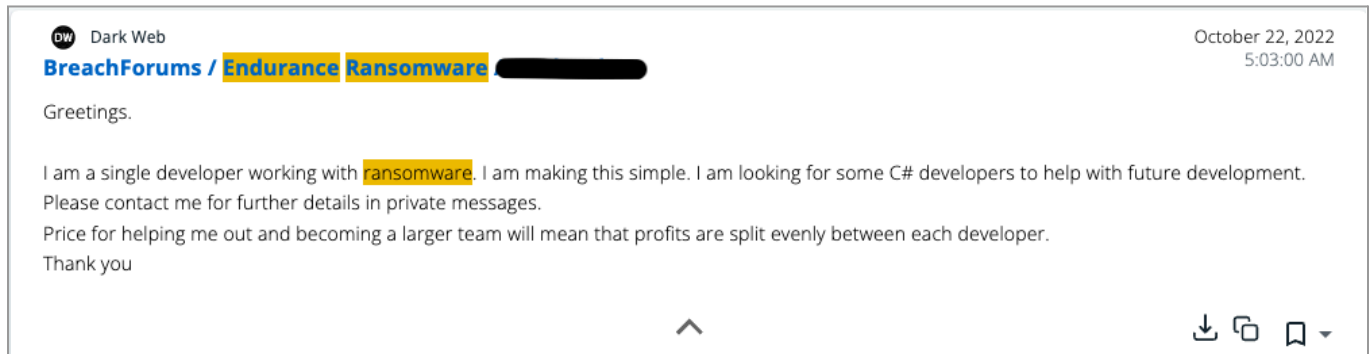
Actor Background

Well-regarded and established threat actor IntelBroker is a hacker and malware developer that has recently increased their targeting of U.S. government entities. They emerged in October 2022 on the predominantly English-language dark web forum BreachForums. On October 22, 2022, IntelBroker claimed they were the developer of Endurance ransomware on BreachForums and were looking for other developers to join the team.¹ The actor posted alleged victims of Endurance ransomware on the forum before it was seized in June 2023 (see Actor Targeting).

[Analyst note: This threat actor appears to espouse views and be involved with groups that are offensive and do not in any way represent the views of ZeroFox. In the interest of full disclosure

¹ ZeroFox Intelligence

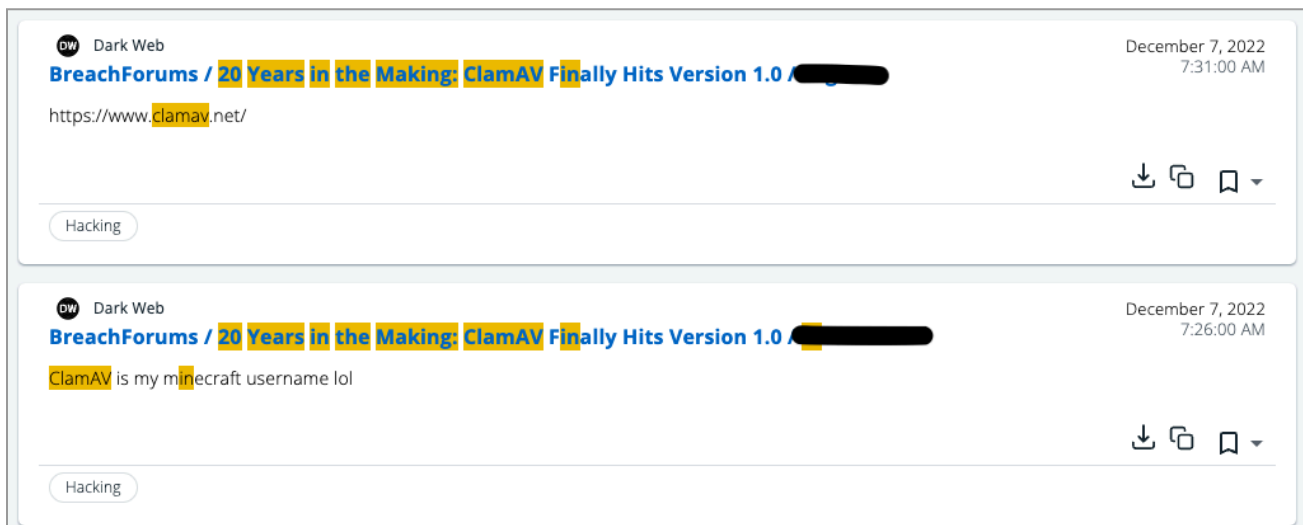
regarding the actor's connections and affiliations, we have not redacted or altered these offensive names in our report.]



IntelBroker States They Are Developers of Endurance Ransomware

Source: ZeroFox Intelligence

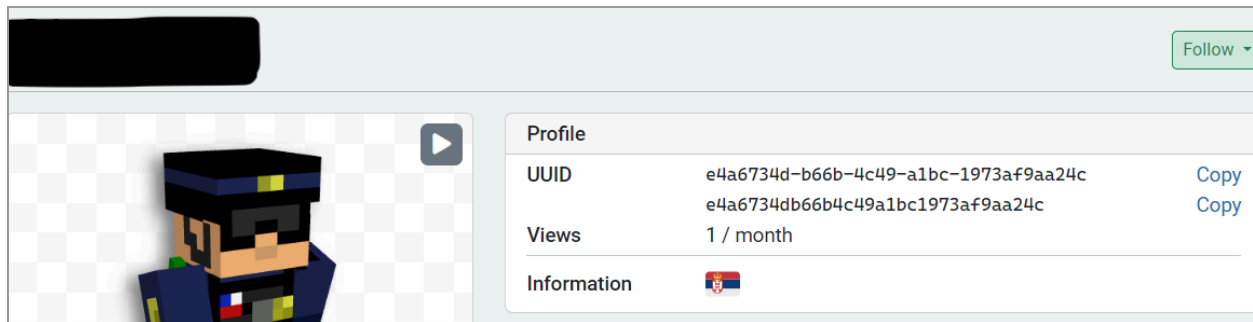
On December 7, 2022, IntelBroker replied to a thread on BreachForums about the release of an updated version of ClamAV open-source antivirus software and claimed that ClamAV was their Minecraft username.



IntelBroker States ClamAV is Their Username

Source: ZeroFox Intelligence

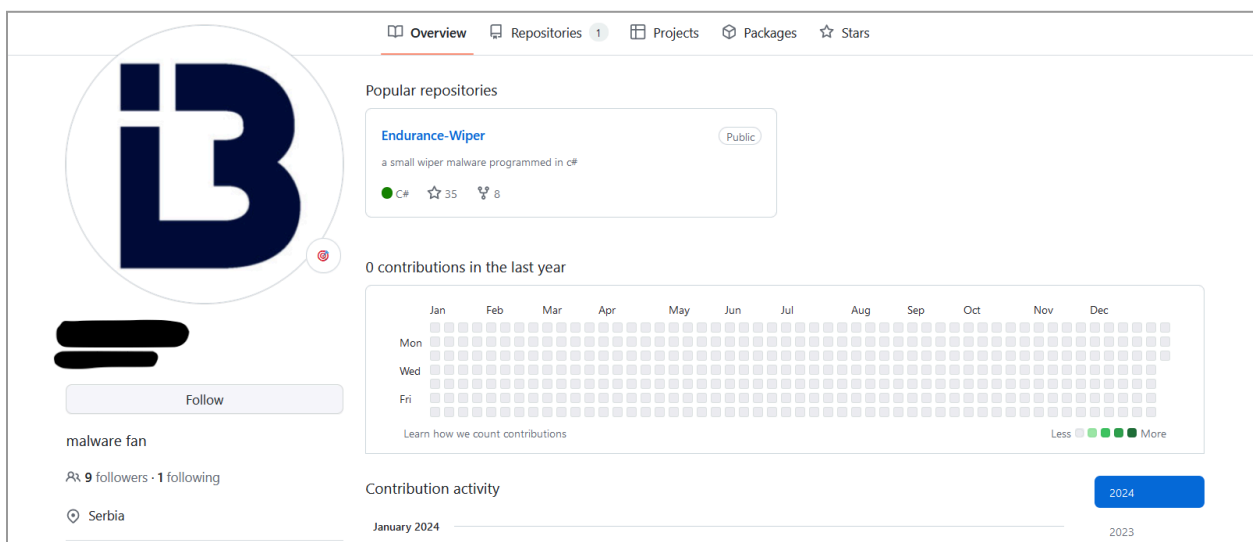
A search of Minecraft users did reveal a ClamAV username. There is minimal information on this page, but it does include a Serbian flag, suggesting a potential location for the actor.



ClamAV Minecraft Profile

Source: [hXXps://namemc\[.\]com/profile/ClamAV.1](https://namemc.com/profile/ClamAV.1)

A GitHub page for the username IntelBroker was located that includes an Endurance wiper repository and location of Serbia as well.



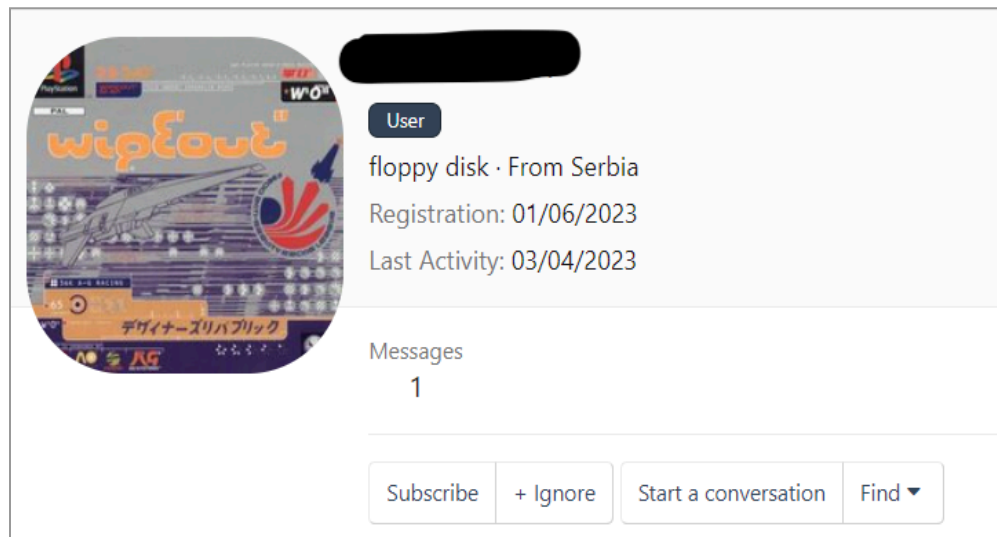
IntelBroker's GitHub Profile

Source: [hXXps://github\[.\]com/IntelBroker](https://github.com/IntelBroker)

In January 2023, a DoxBin post was created about IntelBroker alleging they are a ransomware operator and a racist.² This dox also suggests that the actor's location is Serbia and includes a Jabber account of [ib@darknet\[.\]im](mailto:ib@darknet[.]im). Also, in January 2023, IntelBroker joined the primarily Russian-language deep and dark web forum Xss in

² [hXXps://doxbin\[.\]com/upload/INTELBROKER](https://doxbin.com/upload/INTELBROKER); screenshot not included due to including possible personally identifiable information (PII) of the actor.

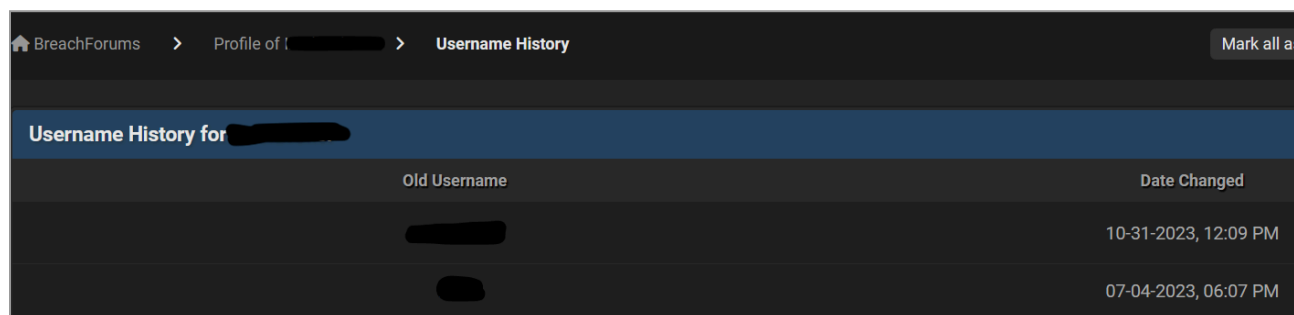
January 2023, listing Serbia on their profile. The actor has been inactive on this forum since March 2023.



IntelBroker's Xss Profile

Source: [xss\[.\]is/members/289553](https://xss[.]is/members/289553)

Once the original BreachForums was seized in June 2023, a new BreachForums was launched, which the actor joined as well. Their initial username was ATF and changed to Nationalist for a few months before the actor started using IntelBroker again.



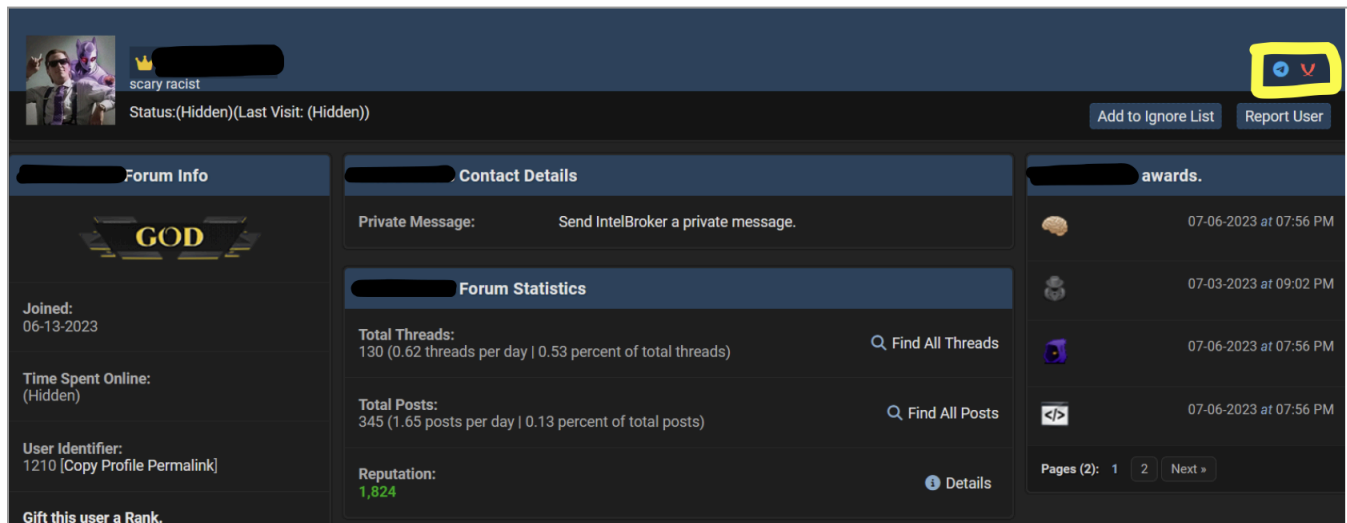
Old Username	Date Changed
[REDACTED]	10-31-2023, 12:09 PM
[REDACTED]	07-04-2023, 06:07 PM

IntelBroker's Username History on New BreachForums

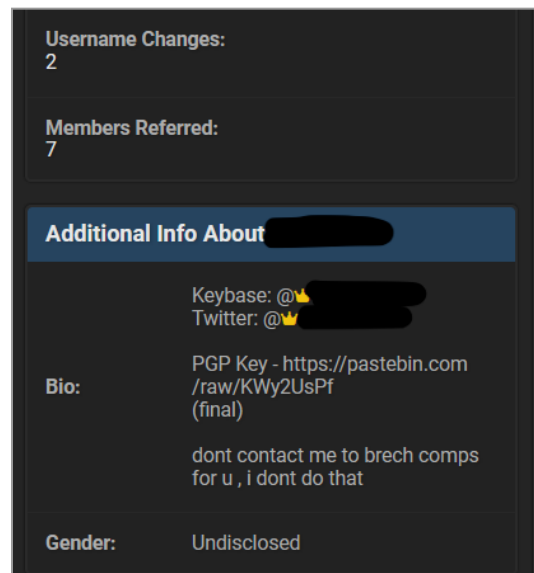
Source: [hXXps://breachforums\[.\]is/User-IntelBroker](https://breachforums[.]is/User-IntelBroker)

In the actor's profile's top right corner are links to the Telegram profile @IntelCN and an XMPP contact of IntelBroker@darknet[.]im. The profile also includes a link to the actor's PGP Key and their username on Keybase and X (formerly Twitter), which is also

IntelBroker. The actor's Keybase profile reveals Bitcoin and Zcash addresses for payment. The actor's PGP key was decoded to reveal the user ID Zoran and the fake email address intelbroker@national.shitposting[.]agency.



The screenshot shows the BreachForum profile of a user named 'scary racist'. The profile includes a header with a crown icon, a status of '(Hidden)', and a last visit of '(Hidden)'. There are buttons for 'Add to Ignore List' and 'Report User'. The main content area is divided into three sections: 'Forum Info', 'Contact Details', and 'awards.'. The 'Forum Info' section shows the user's joined date (06-13-2023), time spent online (hidden), and user identifier (1210). The 'Contact Details' section includes a private message button and forum statistics: 130 threads (0.62 threads per day) and 345 posts (1.65 posts per day). The 'awards.' section shows a list of awards with dates and times. A yellow box highlights the user's profile picture and the 'Report User' button.



This section provides additional information about the user. It includes 'Username Changes: 2' and 'Members Referred: 7'. The 'Additional Info About' section contains the following details:

- Keybase: @ [redacted]
- Twitter: @ [redacted]
- Bio: PGP Key - <https://pastebin.com/raw/KWy2UsPf> (final)
dont contact me to brech comps for u , i dont do that
- Gender: Undisclosed

IntelBroker's BreachForum Profile

Source: [hXXps://breachforums\[.\]is/User-IntelBroker](https://breachforums[.]is/User-IntelBroker)



Supreme Racist God King

The racist. 5 eyes are my fanbase
<https://breachforums.is/User->

Serbia

Teams



cybernegros

- 7 devices
- FEA0 ADC1 DB5F 3BFB
- bc1q6uzzurelqx348t6cr775yv9v4x43m88x7djqlf
- t1RPB1hdgSntRFYigC9jgAvqS816gzTo3us

Chat with 

Your conversation will be end-to-end encrypted.

IntelBroker's Keybase Profile

Source: [hXXps://keybase\[.\]io/intelbroker](https://keybase.io/intelbroker)

```

b4 2f 5a 6f 72 61 6e 20 3c 69 6e 74 65 6c 62 72
6f 6b 65 72 40 6e 61 74 69 6f 6e 61 6c 2e 73 68
69 74 70 6f 73 74 69 6e 67 2e 61 67 65 6e 63 79
3e

```

User ID Packet (0xd)

```

cipherTypeByte: "180"
length: "47"
userId: "national.shitposting.agency>"

```

IntelBroker's PGP Key Decoded

Source: [hXXps://cirw\[.\]in/gpg-decoder/](https://cirw[.]in/gpg-decoder/)

IntelBroker is a somewhat credible actor in the new BreachForums with a high reputation score. They frequently post threads related to company access or databases for sale. The actor has also shared exploits and malware code. IntelBroker typically shares a small sample of proof of access or data, but it appears that some of their claims are exaggerated.

On August 13, 2023, IntelBroker confirmed that they were a part of a hacktivist group called "CyberNiggers." The actor has the group's logo in their signature and has been posting victims on the group's behalf on BreachForums as well.

CyberNiggers - We are recruiting

by [redacted] Sunday August 13, 2023 at 01:04 PM

08-13-2023, 01:04 PM (This post was last modified: 08-13-2023, 08:13 PM by [redacted])



CyberNiggers

Posts: 77

Threads: 35

Joined: Aug 2023

Reputation: 516

Previously, the name Cyber Niggers was involved in several high profile leaks and threads that eventually set the previous BF to be attacked by all sides by the several US alphabet agencies. It was disbanded by its leading members. Since then, it has now been restarted.

If you are serious about bringing a wrath to the multiple glowing agencies that threaten our community and existence online, then you'll be curious about it.

Requirements:

1. Must have amazing OPSEC.

2. A care for the community. I.E, Want to punish the evil alphabet agencies that are threatening our community.

3. Be racist

4. Have an experienced understanding of hacking

Please be aware that being a part of this group will either cause the following:

1. You get nuked by the NSA and Five Eyes Intelligence Group

Or

2. The forum gets shut down (again)

If you're interested, send me a private message on the forums via privnote.

This forum account is currently banned. Ban Length: (Permanent)

Ban Reason: Self-Ban

Find

08-13-2023, 06:23 PM

good to be part of cn again !



IntelBroker Confirms Affiliation with CyberNiggers Group

Source: hXXps:

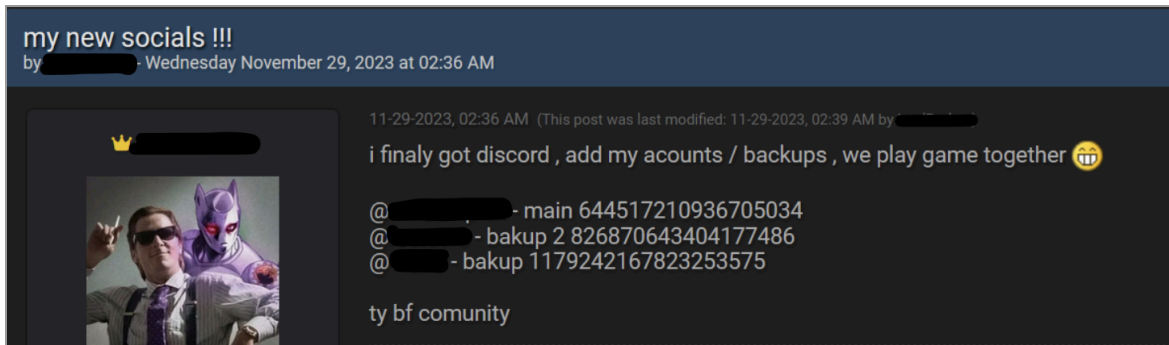
[hXXps://breachforums\[.\]is/Thread-CyberNiggers-We-are-recruiting?recordIsolationId=85ba4932-f4c4-6483-37d6-c0d05d7acbb7](https://breachforums[.]is/Thread-CyberNiggers-We-are-recruiting?recordIsolationId=85ba4932-f4c4-6483-37d6-c0d05d7acbb7)

According to the text within the screenshot, the CyberNiggers group was involved in several high-profile leaks that resulted in the original BreachForums being targeted by government agencies for shutdown. This caused the group to disband for a period, but it has restarted and is recruiting on the new BreachForums. The post claims that prospective members should want to target law enforcement agencies to protect their underground community, have experience hacking, have a high level of OPSEC, and be racist.

On November 29, 2023, IntelBroker shared Discord accounts they had recently created on BreachForums. They had a main account under the username @mr.bumpkin with backup accounts under @leetacro and @wezlk.

© 2024 ZeroFox, Inc. All rights reserved.

7

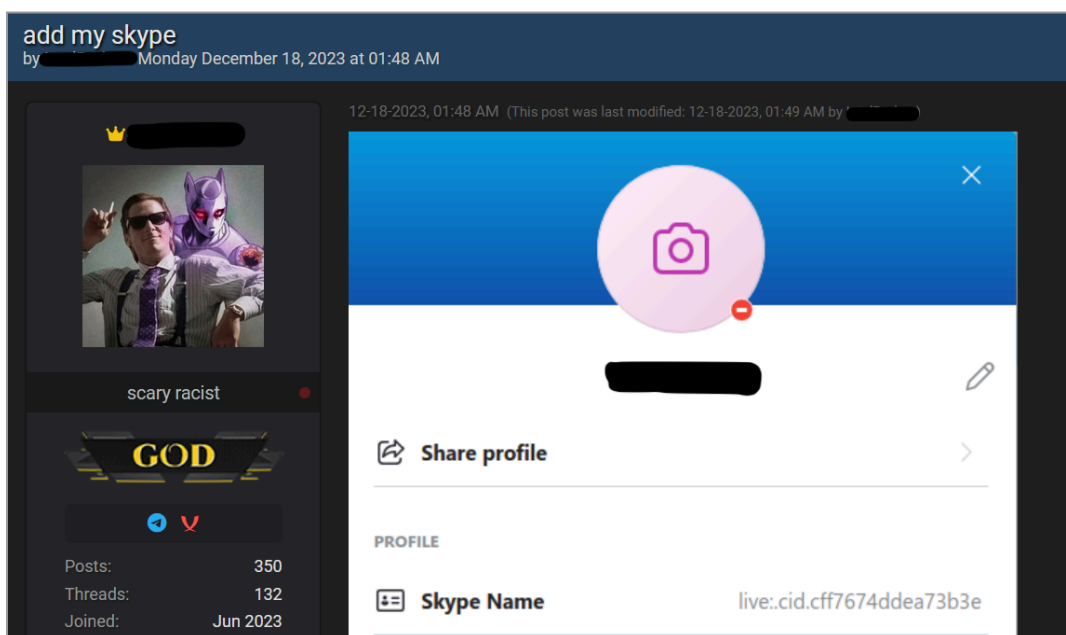


IntelBroker Posting Discord Accounts on BreachForums

Source:

[hXXps://breachforums\[.\]is/Thread-my-new-socials?recordIsolationId=5c2cc7e8-1e94-2134-fdb1-9f23b422a33a](https://breachforums[.]is/Thread-my-new-socials?recordIsolationId=5c2cc7e8-1e94-2134-fdb1-9f23b422a33a)

On December 18, 2023, the actor posted a thread regarding adding them on Skype that showed the username TheKilob. It is likely that this Skype username was used to impersonate another actor with the same username. In November 2022, IntelBroker claimed that “thekilob” had accused them of scamming on the original BreachForums.



IntelBroker Skype Username

[hXXps://breachforums\[.\]is/Thread-add-my-skype?recordIsolationId=fc0e14c6-25a2-658e-2b53-c361c559e158](https://breachforums[.]is/Thread-add-my-skype?recordIsolationId=fc0e14c6-25a2-658e-2b53-c361c559e158)



TheKilob Scamming Accusation

Source: ZeroFox Intelligence

There has been some dark web chatter that the two actors may have worked together since this accusation, and they do follow each other on Keybase.³⁴ The actor thekilob has been banned on several forums, was doxxed in August 2022, and does not appear to have any personal connection to information associated with IntelBroker.⁵

Actor Targeting

ZeroFox analyzed available data of alleged Endurance ransomware victims that IntelBroker posted prior to the original BreachForums seizure, as well as current posts the actor has shared on the new BreachForums on their own or on behalf of the CyberNiggers group to highlight their sector and region victim-targeting.⁶ Since the actor first became active in October 2022, IntelBroker has targeted approximately 150 victims with the majority being in the government, financial services, and technology sectors.

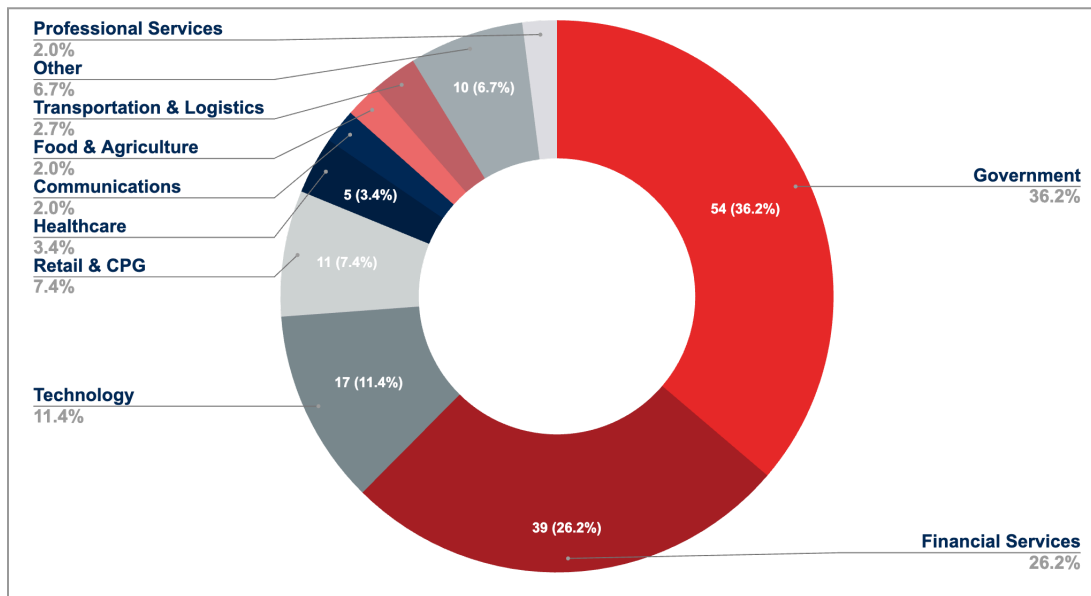
³ hXXps://keybase[.]io/intelbroker

⁴ hXXps://keybase[.]io/thekilob

⁵ hXXps://doxbin[.]net/upload/thekilob

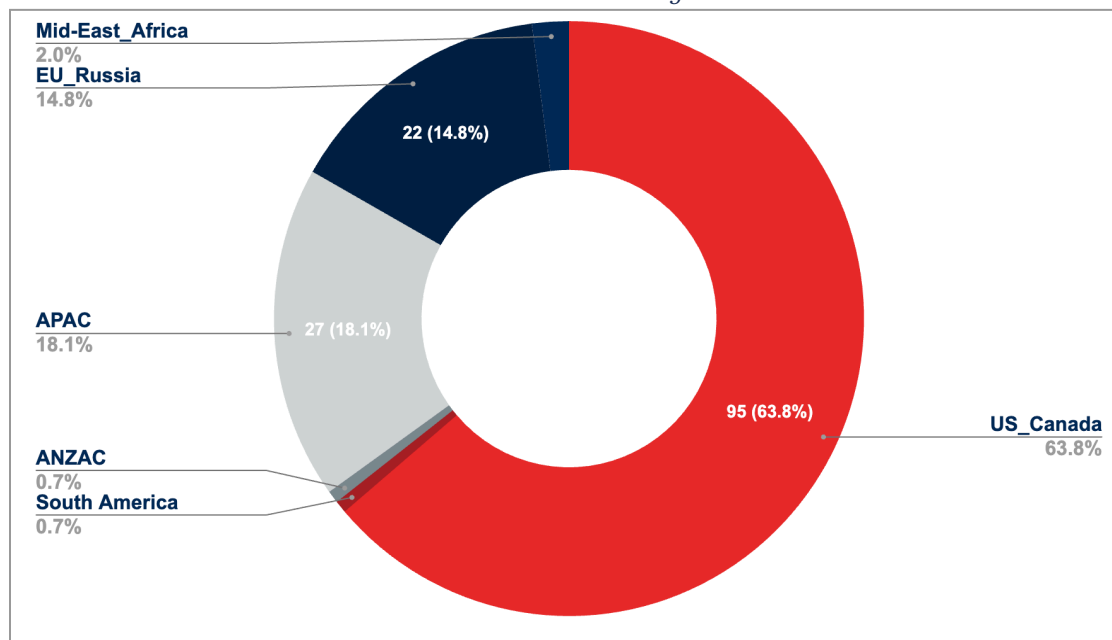
⁶ ZeroFox Intelligence

IntelBroker mainly targets the United States and Canada, the APAC region, and European countries.



Sectors Targeted by IntelBroker

Source: ZeroFox Intelligence



Regions Targeted by IntelBroker

Source: ZeroFox Intelligence

Appendix A: Actor Indicators

Information Associated with IntelBroker

Source	Type of Indicator	Indicator
BreachForums	Username	IntelBroker, ATF, Nationalist
Minecraft	Username	ClamAV
Jabber	Contact	ib@darknet[.]im
xss	Username	intelbroker
Telegram	Contact	IntelCN
XMPP	Contact	IntelBroker@darknet[.]im
Keybase	Username	IntelBroker
Keybase	Bitcoin address	bc1q6uzzurelqx348t6cr775yv9v4x43m88x7djqlf
Keybase	Zcash address	t1RPB1hdgSntRFYigC9jgAvqS8l6gzTo3us
X (formerlyTwitter)	Username	IntelBroker
PGP Key	Username	Zoran
Discord	Username	mr.bumpkin, leetacro, wezl
Skype	Username	TheKilob

| Appendix B: 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 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 C: 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%