ZEROFOX INTELLIGENCE

Brief

The Underground Economist: Volume 5, Issue 24

B-2025-12-04b

Classification: TLP:CLEAR

Criticality: LOW

Intelligence Requirements: Deep and Dark Web, Threat Actor, Data Breach

December 4, 2025

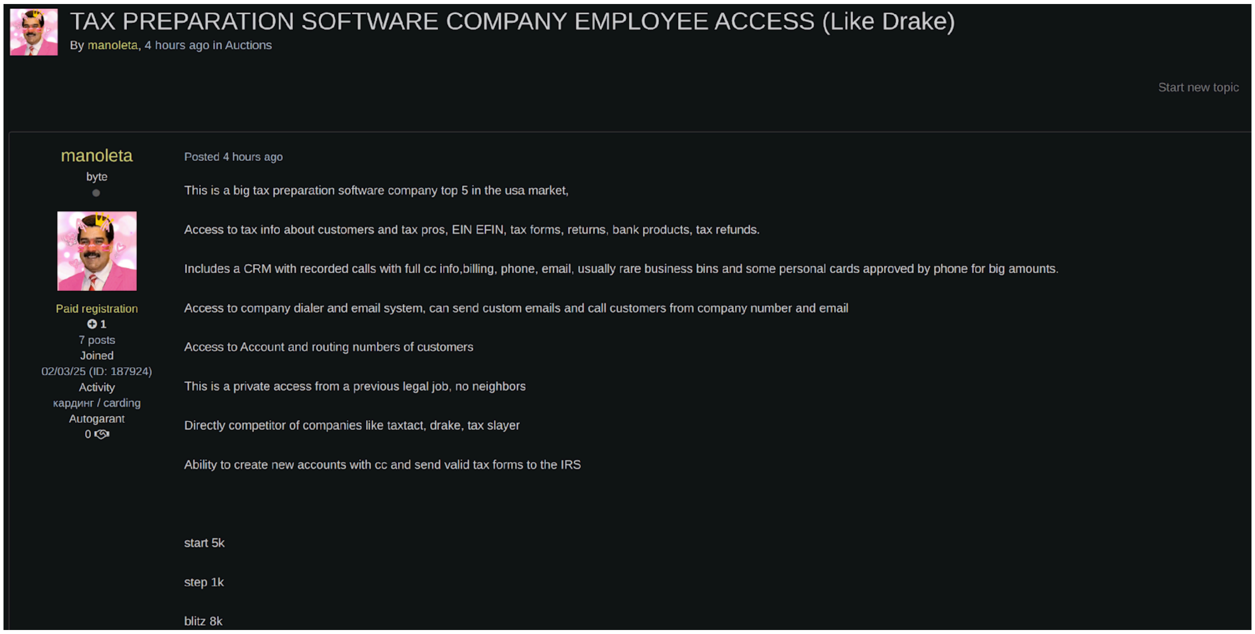
ZeroFox Intelligence is derived from a variety of sources, including—but not limited to—curated open-source accesses, vetted social media, proprietary data sources, and direct access to threat actors and groups through covert communication channels. Information relied upon to complete any report cannot 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 10:30 AM (EST) on December 4, 2025; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

| Brief | The Underground Economist: Volume 5, Issue 24

| Unnamed U.S. Tax Preparation Software Company Access for Sale

On December 3, 2025, the threat actor known as “manoleta” posted on the dark web forum Exploit, advertising employee access to an unnamed tax preparation software corporation. Manoleta listed the access for auction starting at USD 5,000 with a minimum bid increment of USD 1,000, or it can be purchased outright for USD 8,000. The seller provided images from the company’s software and dialer in the post, likely as proof of their access.

- According to manoleta, the tax prep software company is among the top five in the U.S. market, which will likely attract a host of financially motivated threat actors and those seeking to conduct social engineering campaigns with the data acquired.
- Manoleta first joined the Exploit forum in February 2025 and has garnered a positive reaction score of one, which likely lends credibility to the actor’s advertisement.



TAX PREPARATION SOFTWARE COMPANY EMPLOYEE ACCESS (Like Drake)
By manoleta, 4 hours ago in Auctions

manoleta
byte

Paid registration
1
7 posts
Joined
02/03/25 (ID: 187924)
Activity
кардинг / carding
Autogarant
0

Posted 4 hours ago

This is a big tax preparation software company top 5 in the usa market,

Access to tax info about customers and tax pros, EIN EFIN, tax forms, returns, bank products, tax refunds.

Includes a CRM with recorded calls with full cc info,billing, phone, email, usually rare business bins and some personal cards approved by phone for big amounts.

Access to company dialer and email system, can send custom emails and call customers from company number and email

Access to Account and routing numbers of customers

This is a private access from a previous legal job, no neighbors

Directly competitor of companies like taxtact, drake, tax slayer

Ability to create new accounts with cc and send valid tax forms to the IRS

start 5k

step 1k

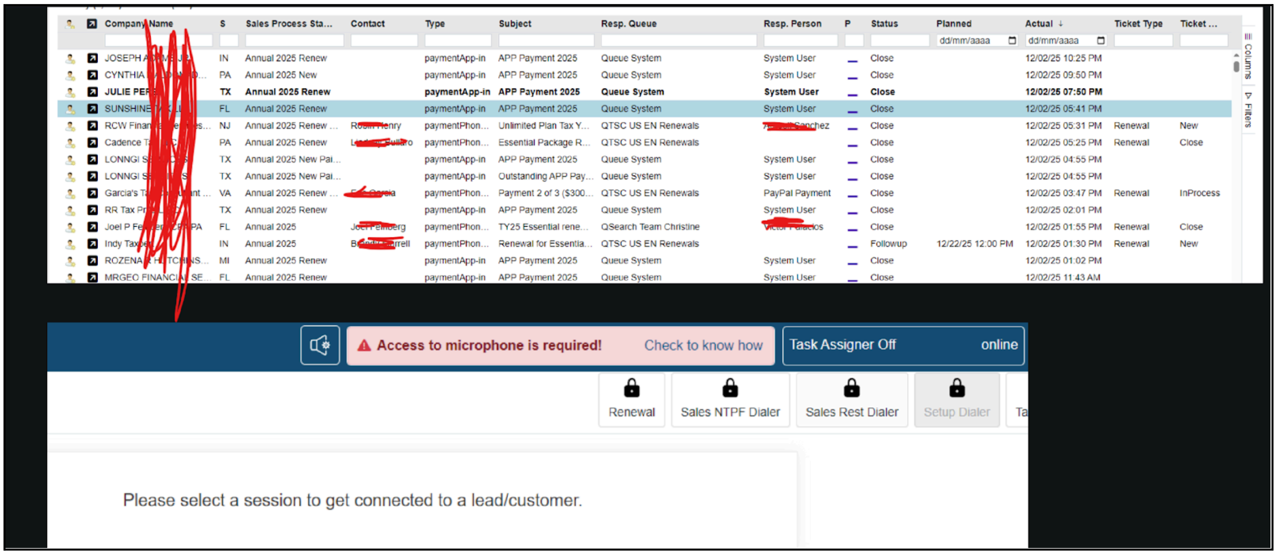
blitz 8k

manoleta's Exploit post
Source: ZeroFox Intelligence

Manoleta claims that the insider access includes access to tax information about customers and tax professionals, Employer Identification Number/Electronic Filing Identification Number (EIN/EFIN), tax forms, tax return documents, bank products, and tax refunds. The seller also claims to have access to the company's Customer Relationship Management (CRM) platform, which likely includes recorded phone calls containing sensitive personally identifiable information (PII). In addition, the buyer would also allegedly receive:

- Access to the company's dialer and email system, enabling them to send custom emails and call customers using the company's number and email;
- Access to customers' accounts and routing numbers;
- A "private" access originating from a previous legitimate job that is not shared with others;
- Access to resources of a company that directly competes with firms like TaxAct, Drake, and TaxSlayer; and

- The ability to create new accounts with credit cards and send valid tax forms to the Internal Revenue Service (IRS).



Company Name	S	Sales Process Sta...	Contact	Type	Subject	Resp. Queue	Resp. Person	P	Status	Planned	Actual ↓	Ticket Type	Ticket ...
										dd/mm/aaaa	dd/mm/aaaa		
[redacted]	IN	Annual 2025 Renew		paymentApp-in	APP Payment 2025	Queue System	System User	—	Close		12/02/25 10:25 PM		
[redacted]	PA	Annual 2025 New		paymentApp-in	APP Payment 2025	Queue System	System User	—	Close		12/02/25 09:50 PM		
[redacted]	**TX**	**Annual 2025 Renew**		**paymentApp-in**	**APP Payment 2025**	**Queue System**	**System User**	—	**Close**		**12/02/25 07:50 PM**		
[redacted]	FL	Annual 2025 Renew		paymentApp-in	APP Payment 2025	Queue System	System User	—	Close		12/02/25 05:41 PM		
[redacted]	NJ	Annual 2025 Renew ...	[redacted]	paymentPhon...	Unlimited Plan Tax Y...	QTSC US EN Renewals	[redacted]	—	Close		12/02/25 05:31 PM	Renewal	New
[redacted]	PA	Annual 2025 Renew	[redacted]	paymentPhon...	Essential Package R...	QTSC US EN Renewals		—	Close		12/02/25 05:25 PM	Renewal	Close
[redacted]	TX	Annual 2025 New Pai...		paymentApp-in	APP Payment 2025	Queue System	System User	—	Close		12/02/25 04:55 PM		
[redacted]	TX	Annual 2025 New Pai...		paymentApp-in	Outstanding APP Pay...	Queue System	System User	—	Close		12/02/25 04:55 PM		
[redacted]	VA	Annual 2025 Renew ...	[redacted]	paymentPhon...	Payment 2 of 3 ($300...	QTSC US EN Renewals	PayPal Payment	—	Close		12/02/25 03:47 PM	Renewal	InProcess
[redacted]	TX	Annual 2025 Renew		paymentApp-in	APP Payment 2025	Queue System	System User	—	Close		12/02/25 02:01 PM		
[redacted]	FL	Annual 2025	[redacted]	paymentPhon...	TY25 Essential rene...	QSearch Team Christine	[redacted]	—	Close		12/02/25 01:55 PM	Renewal	Close
[redacted]	IN	Annual 2025	[redacted]	paymentPhon...	Renewal for Essentia...	QTSC US EN Renewals		—	Followup	12/22/25 12:00 PM	12/02/25 01:30 PM	Renewal	New
[redacted]	MI	Annual 2025 Renew		paymentApp-in	APP Payment 2025	Queue System	System User	—	Close		12/02/25 01:02 PM		
[redacted]	FL	Annual 2025 Renew		paymentApp-in	APP Payment 2025	Queue System	System User	—	Close		12/02/25 11:43 AM		

Please select a session to get connected to a lead/customer.

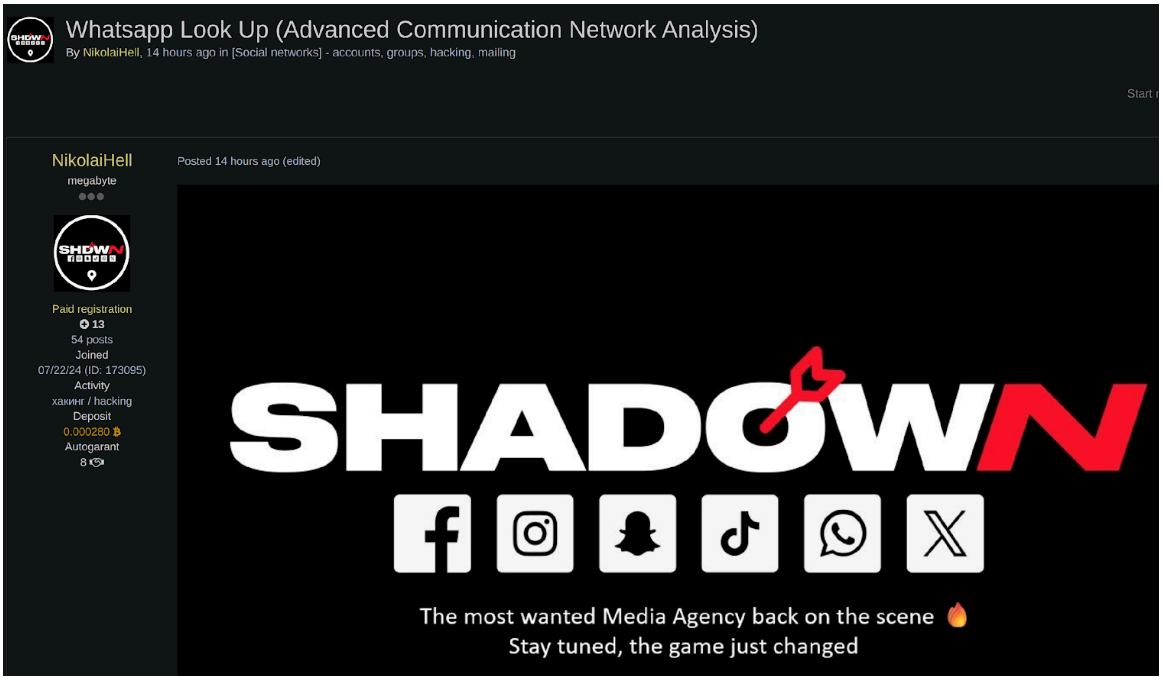
Additional image provided by manoleta

Source: ZeroFox Intelligence

The upcoming U.S. tax season is typically a time of increased fraud activity on the deep and dark web (DDW). Tax fraud remains a common practice among cybercriminals, and ZeroFox assesses that, if legitimate, the access advertised in manoleta's post is likely to allow fraudsters to exfiltrate and manipulate large volumes of sensitive tax data and other PII. Such data would almost certainly be used in social engineering campaigns—particularly spear phishing attacks and impersonations.

WhatsApp Look-up Service Advertised on Dark Web

On November 24, 2025, an actor known as "NikolaiHell" advertised a service called Advanced Communication Network Analysis (ACNA) on the Exploit dark web forum. The service advertised is essentially a WhatsApp look-up service that claims to provide a full CSV file of a target phone number's entire contact network. The price for the service ranges from USD 650–3,000 depending on the number of contacts.



Whatsapp Look Up (Advanced Communication Network Analysis)
By NikolaiHell, 14 hours ago in [Social networks] - accounts, groups, hacking, mailing

Start r

NikolaiHell
megabyte

Paid registration
13
54 posts
Joined
07/22/24 (ID: 173095)
Activity
хакинг / hacking
Deposit
0.000280 ฿
Autogarant
8

Posted 14 hours ago (edited)

The most wanted Media Agency back on the scene 🔥
Stay tuned, the game just changed

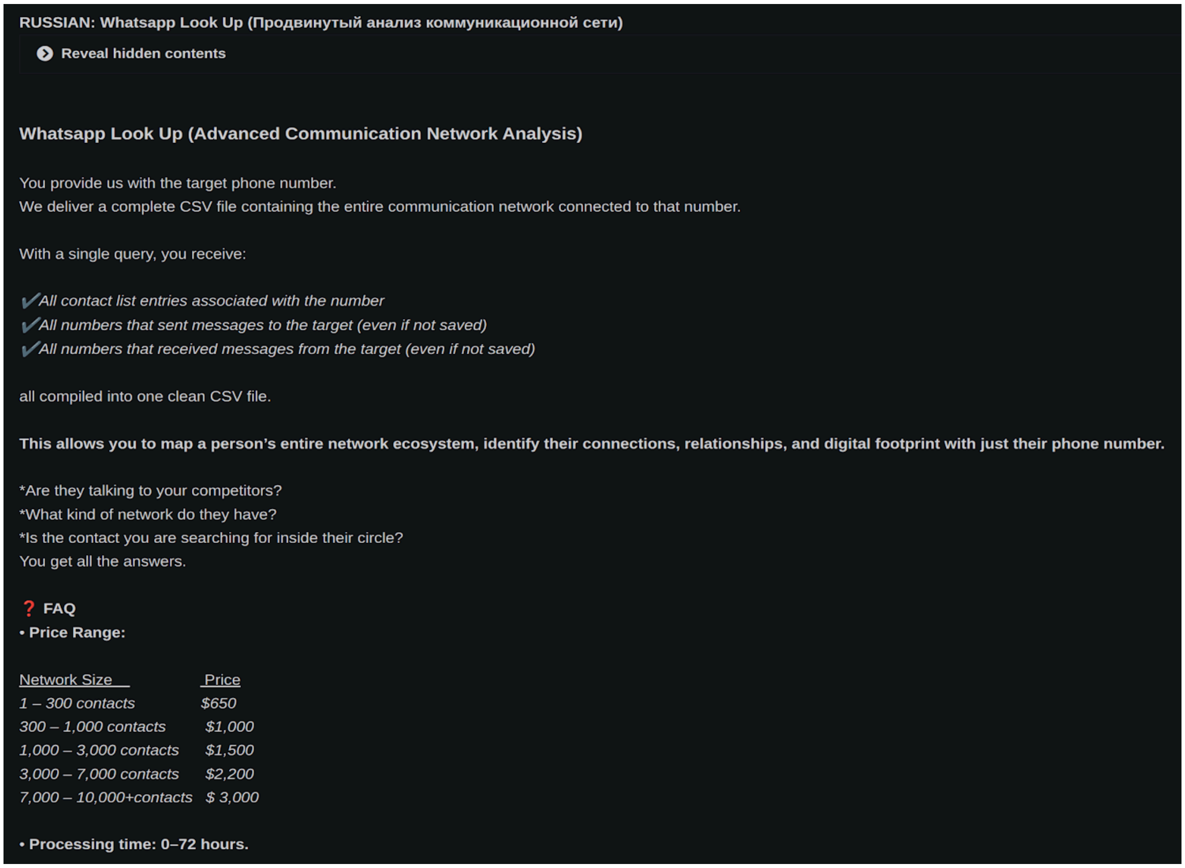
NikolaiHell's post on Exploit (Part 1)

Source: ZeroFox Intelligence

According to NikolaiHell, the information provided by the service is valuable for collecting intelligence on competitors that regularly conduct business over WhatsApp. Buyers must provide a single query for a seed phone number, and ACNA will reportedly provide:

- All contact list entries associated with the number
- All numbers that sent messages to the target (even if not saved)
- All numbers that received messages from the target (even if not saved)

Additionally, the service reportedly provides solutions for users banned on WhatsApp, Instagram, TikTok, or Facebook. It is likely that NikolaiHell is exfiltrating data and manipulating statuses on social media platforms and WhatsApp through insiders or compromised access to management accounts.



RUSSIAN: Whatsapp Look Up (Продвинутый анализ коммуникационной сети)

Reveal hidden contents

Whatsapp Look Up (Advanced Communication Network Analysis)

You provide us with the target phone number.
We deliver a complete CSV file containing the entire communication network connected to that number.

With a single query, you receive:

✔*All contact list entries associated with the number*
✔*All numbers that sent messages to the target (even if not saved)*
✔*All numbers that received messages from the target (even if not saved)*

all compiled into one clean CSV file.

This allows you to map a person's entire network ecosystem, identify their connections, relationships, and digital footprint with just their phone number.

*Are they talking to your competitors?
*What kind of network do they have?
*Is the contact you are searching for inside their circle?
You get all the answers.

❓ **FAQ**
• **Price Range:**

Network Size	Price
1 – 300 contacts	*$650*
300 – 1,000 contacts	*$1,000*
1,000 – 3,000 contacts	*$1,500*
3,000 – 7,000 contacts	*$2,200*
7,000 – 10,000+contacts	*$ 3,000*

• **Processing time: 0–72 hours.**

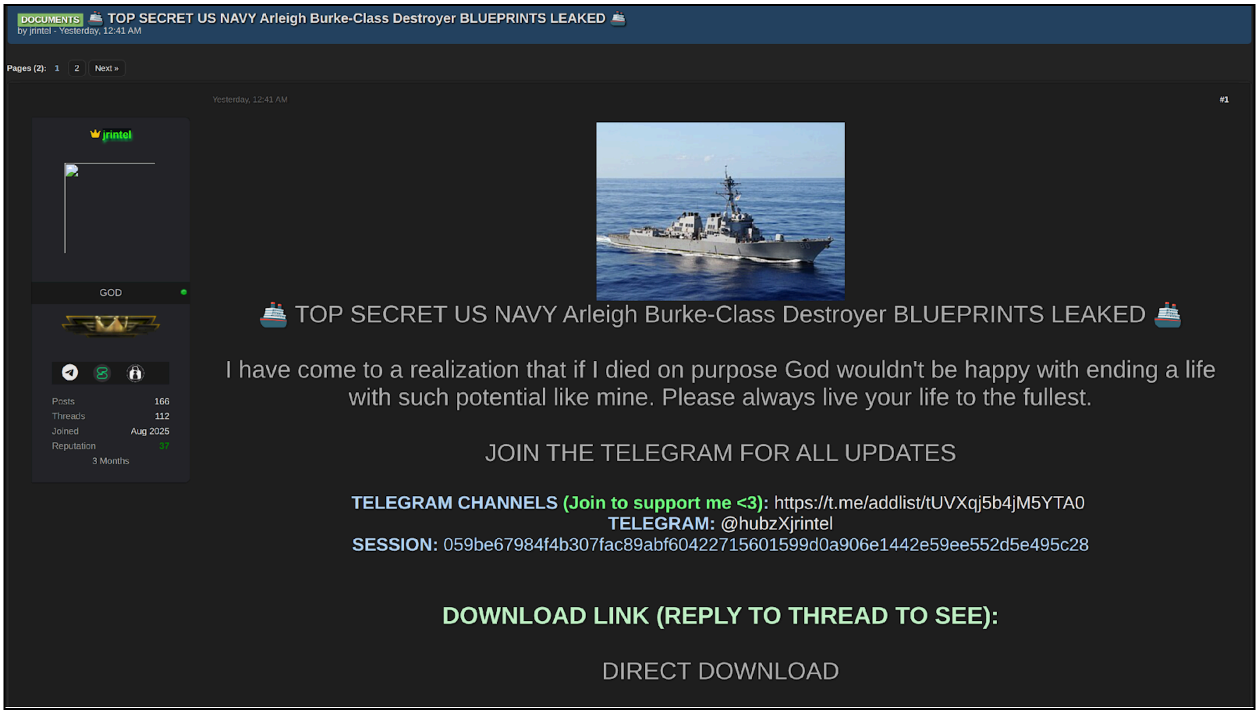
NikolaiHell's post on Exploit (Part 2)
Source: ZeroFox Intelligence

NikolaiHell is a registered user on the Exploit forum with a very solid reputation, indicating that this offering is likely legitimate and works as advertised. WhatsApp look-up and scraping services are common in law enforcement and intelligence, so it is almost certain that actors in the underground economy would seek to duplicate this capability.

Reputed Threat Actor Claims Top Secret Leak of U.S. Navy Documents

On November 24, 2025, well-known threat actor "jrintel" claimed in a DarkForums post to have accessed "top secret" U.S. Navy blueprints of the Arleigh Burke-Class destroyer. Jrintel shared a 2.3 MB file that appeared to show the schematics of MK 46 and MK 50 torpedoes. It is unclear whether the shared file is a sample of the leaked documents or the complete leak.

- The 2.3 MB file was shared free-of-charge, and the post did not specify further leaks, suggesting it is not a sample before the main leak. The post also included contact links via Telegram and Session. The post has received reactions from other users of DarkForums (mostly comments thanking jrintel).
- Jrintel joined DarkForums in August 2025 and has a positive reputation. The actor is known for advertising government and military information on dark web platforms and claiming it is “top secret.”
- In November 2025, jrintel advertised for sale allegedly classified files related to the Barak-8 missile system used by Israel and India, as well as documents about a U.S. unmanned aerial vehicle (UAV).



DOCUMENTS 🚢 TOP SECRET US NAVY Arleigh Burke-Class Destroyer BLUEPRINTS LEAKED 🚢
by jrintel - Yesterday, 12:41 AM

Pages (2): 1 2 Next »

Yesterday, 12:41 AM #1

jrintel
GOD

Posts	166
Threads	112
Joined	Aug 2025
Reputation	37

3 Months

🚢 TOP SECRET US NAVY Arleigh Burke-Class Destroyer BLUEPRINTS LEAKED 🚢

I have come to a realization that if I died on purpose God wouldn't be happy with ending a life with such potential like mine. Please always live your life to the fullest.

JOIN THE TELEGRAM FOR ALL UPDATES

TELEGRAM CHANNELS (Join to support me <3): https://t.me/addlist/tUVXqj5b4jM5YTA0
TELEGRAM: @hubzXjrintel
SESSION: 059be67984f4b307fac89abf60422715601599d0a906e1442e59ee552d5e495c28

DOWNLOAD LINK (REPLY TO THREAD TO SEE):

DIRECT DOWNLOAD

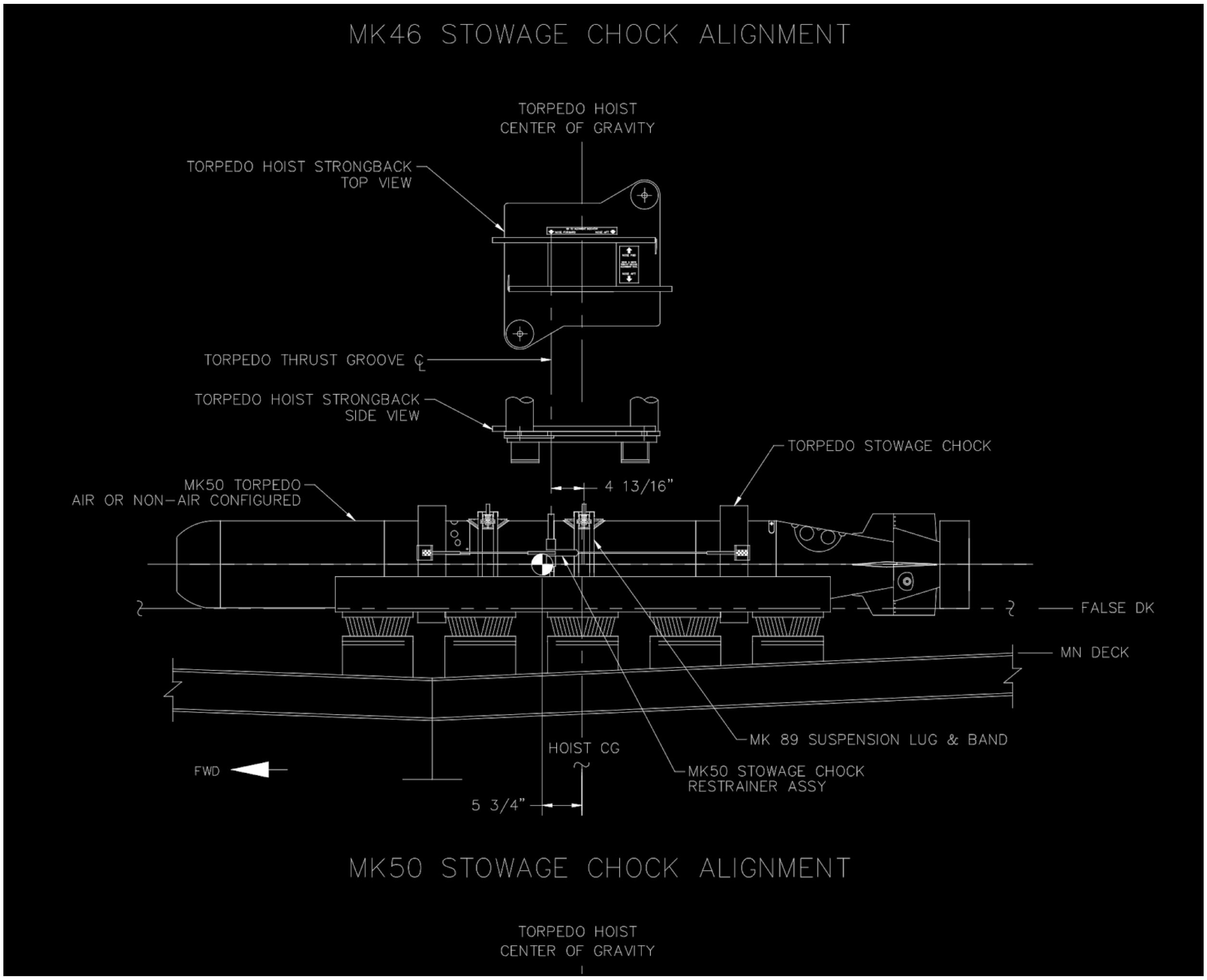
jrintel’s DarkForums post

Source: ZeroFox Intelligence

The U.S. Navy has not publicly acknowledged any data breach related to the torpedo schematics, but the documents appear to be legitimate. Some of the information in the schematics, including stowage chock alignment, would almost certainly be classified at least “Secret” due to the sensitive nature of weapon systems transport procedures. The schematics provided are likely not available from public sources.

MK 46 torpedoes are widely exported and used by militaries worldwide, suggesting there is a roughly even chance that jrintel sourced the schematics from non-U.S. military sources.

- It is also possible, though less likely, that jrintel’s information is the result of a cyber intrusion and data breach involving private military contractors working with the U.S. military.


MK46 STOWAGE CHOCK ALIGNMENT
TORPEDO HOIST CENTER OF GRAVITY
TORPEDO HOIST STRONGBACK TOP VIEW
TORPEDO THRUST GROOVE ℄
TORPEDO HOIST STRONGBACK SIDE VIEW
TORPEDO STOWAGE CHOCK
MK50 TORPEDO AIR OR NON–AIR CONFIGURED
4 13/16"
FALSE DK
MN DECK
MK 89 SUSPENSION LUG & BAND
HOIST CG
FWD
MK50 STOWAGE CHOCK RESTRAINER ASSY
5 3/4"
MK50 STOWAGE CHOCK ALIGNMENT
TORPEDO HOIST CENTER OF GRAVITY

The alleged schematics of MK 50 torpedo

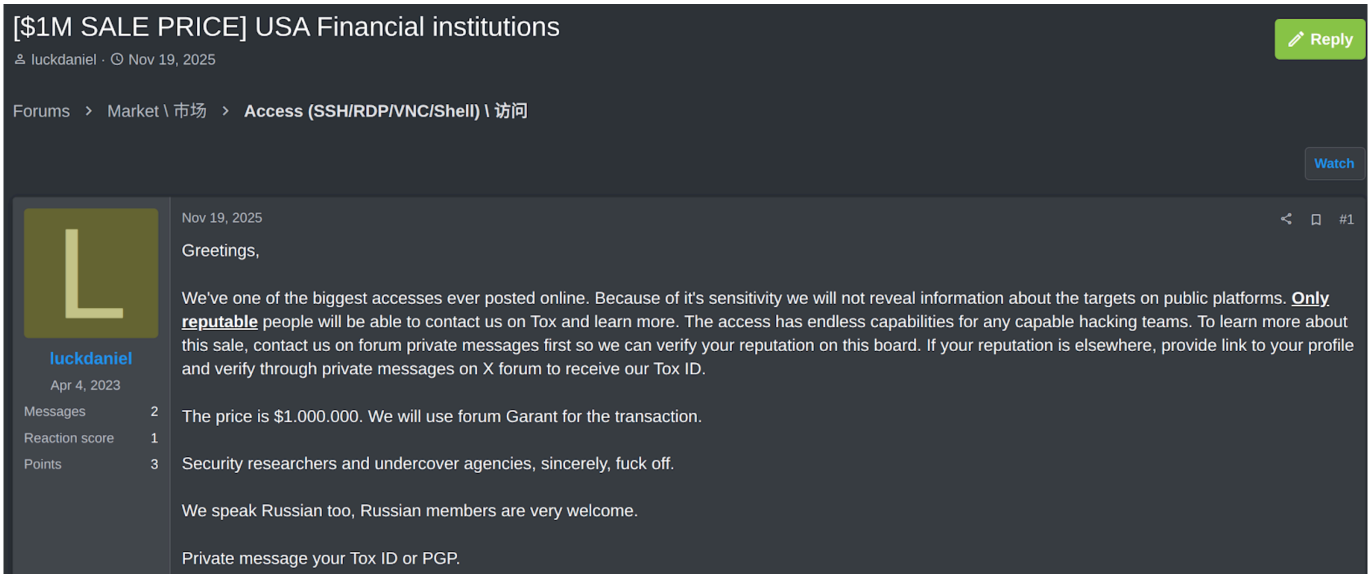
Source: ZeroFox Intelligence

The post and its contents are likely to be of interest to geopolitically motivated actors and foreign adversaries of the United States. Jrintel is likely to have shared the information free-of-charge to attract interest and gain a positive reputation as a legitimate broker of government and defense-related information.

Initial Network Access to U.S. Financial Institutions Advertised for Sale on Dark Web

On November 19, 2025, an actor using the alias “luckdaniel” posted on the dark web forum RAMP, advertising one of the most expensive initial network accesses ever observed on the DDW. According to the post, the target is an undisclosed U.S. financial institution, and the price of the access is USD 1 million.

- On November 21, 2025, luckdaniel provided an update on their post, stating that they could provide proof to the forum administrators. Again, they reiterated that they would not deal with users who had not demonstrated a strong reputation on the DDW.
- Luckdaniel joined RAMP in April 2023 and has conducted very little activity on the forum since then; therefore, ZeroFox cannot determine the credibility of the actor at the time of writing.



[$1M SALE PRICE] USA Financial institutions

luckdaniel · Nov 19, 2025

Nov 19, 2025

Greetings,

We've one of the biggest accesses ever posted online. Because of it's sensitivity we will not reveal information about the targets on public platforms. **Only reputable** people will be able to contact us on Tox and learn more. The access has endless capabilities for any capable hacking teams. To learn more about this sale, contact us on forum private messages first so we can verify your reputation on this board. If your reputation is elsewhere, provide link to your profile and verify through private messages on X forum to receive our Tox ID.

The price is $1.000.000. We will use forum Garant for the transaction.

Security researchers and undercover agencies, sincerely, fuck off.

We speak Russian too, Russian members are very welcome.

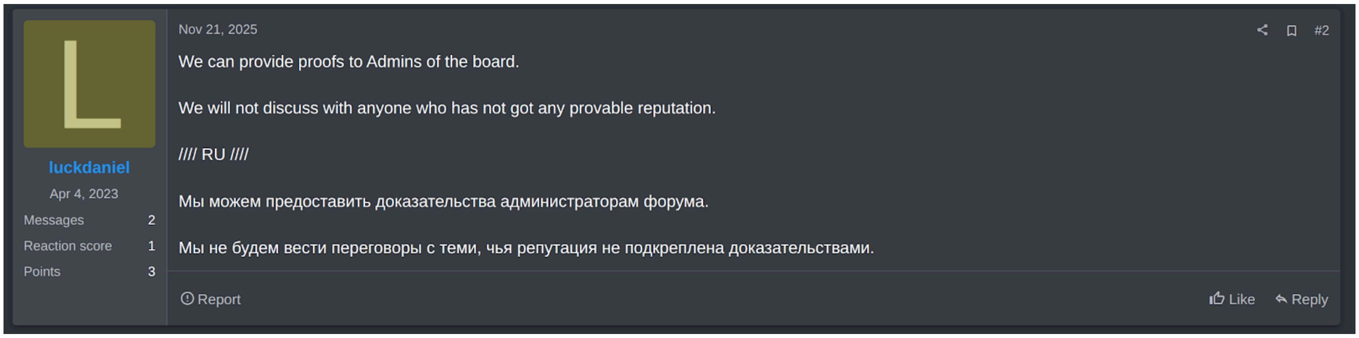
Private message your Tox ID or PGP.

luckdaniel's RAMP post

Source: ZeroFox Intelligence

Luckdaniel emphasized that security researchers and undercover agencies are strictly prohibited from acquiring access and that any further negotiations with a potential buyer are to be conducted through private messaging via Tox. In the post, luckdaniel claims that the access has "endless capabilities" for any credible threat actor which, given the sale price, implies the offering provides:

- High-privilege and persistent access—likely domain administrator (DA) or enterprise admin-level;
- Access to internal financial systems, such as internal banking applications or payment processing systems;
- Access to privileged data, such as PII and internal emails and communications; and
- Ransomware deployment capability.



We can provide proofs to Admins of the board.

We will not discuss with anyone who has not got any provable reputation.

//// RU ////

Мы можем предоставить доказательства администраторам форума.

Мы не будем вести переговоры с теми, чья репутация не подкреплена доказательствами.

luckdaniel's updated RAMP post

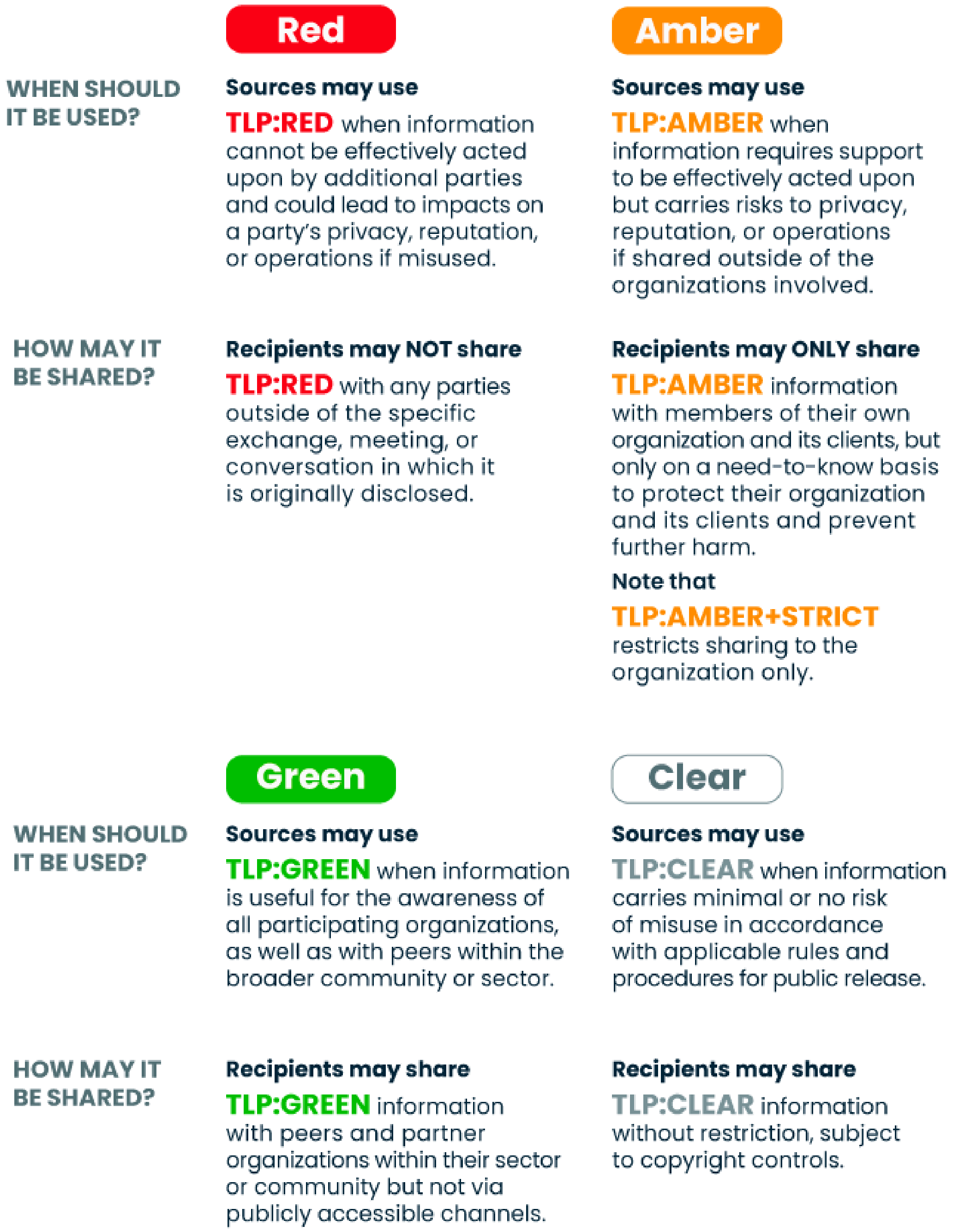
Source: ZeroFox Intelligence

Due to the substantial price of USD 1 million and the target being U.S. financial institutions, the advertisement is very likely to gain significant interest and traction on RAMP among financially motivated threat actors. If the access described is accurate, it could provide threat actors with an array of significantly malicious capabilities which almost certainly will cause significant disruption to victim institutions and their clients.

Recommendations

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

Appendix A: Traffic Light Protocol for Information Dissemination

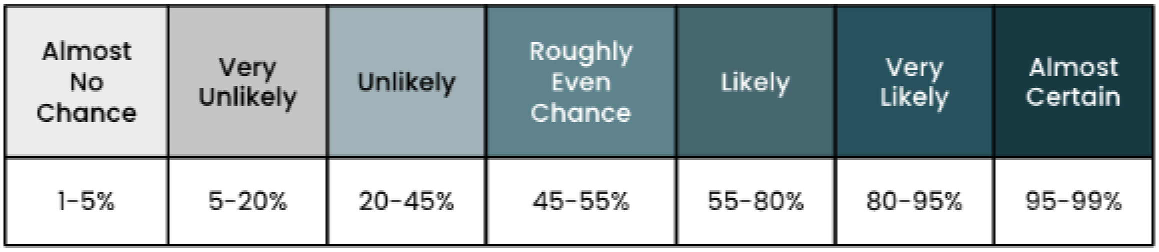


	Red	Amber
WHEN SHOULD IT BE USED?	**Sources may use** **TLP:RED** when information cannot be effectively acted upon by additional parties and could lead to impacts on a party's privacy, reputation, or operations if misused.	**Sources may use** **TLP:AMBER** when information requires support to be effectively 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 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%