



| Flash |

Financial Scams Circulate as U.S. Tax Season Nears End

F-2024-03-19a

Classification: TLP:CLEAR

Criticality: Medium

Intelligence Requirements: Deep & Dark Web, Tax Fraud, Data Theft

March 19, 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 12:00 PM (EDT) on March 19, 2024**; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

| Flash | Financial Scams Circulate as U.S. Tax Season Nears End

› Key Findings

- As the end of the U.S. tax season nears, ZeroFox Intelligence has observed an increase in tax fraud-related activity taking place in the deep and dark web (DDW).
- On March 9, 2024, a Russian-speaking threat actor posted in DDW forum xss, claiming they are able to supply two types of completed, illegitimate Internal Revenue Service (IRS) tax documents.
- Activity of this nature is very likely to increase in frequency over the coming weeks, with threat actors continuing to evolve their techniques, tactics, and procedures (TTPs) to most effectively leverage illicitly-obtained personally identifiable information (PII) that is relatively cheap and easily acquired in DDW forums.

| Details

As the end of the U.S. tax season nears, ZeroFox Intelligence has observed an increase in tax fraud-related activity taking place in the DDW, as threat actors seek to acquire and leverage illicitly-obtained information to conduct various scams.

On March 9, 2024, a highly-regarded Russian-speaking threat actor known as “MagaClub” posted in DDW forum xss, claiming they are able to supply two types of

illegitimate IRS tax documents—the U.S. Individual Income Tax Return (1040) and the Wage and Tax Statement (W2)—for a cost of USD 20 per form. The actor claimed to also be selling completed credit reports with scores over 700 (considered high) for USD 30 each. The tax documents and the credit reports are sold fully populated with illicitly obtained PII and use the forum’s escrow service.

- It is very likely that the forms sold by MagaClub are purchased primarily by malicious actors intending to file fraudulent tax returns in the name of the victim.
- The forms are very likely populated with PII from previous financial years. This information is likely obtained through data breaches implicating the IRS or one of the many third-party accountancy firms reportedly used by up to a quarter of U.S. citizens to assist in preparing and filing tax returns.¹ These forms are then submitted for the 2023 tax year in the hope that the PII contained within remains valid and extant.
- There is also a roughly even chance that MagaClub is able to procure completed forms via an ongoing intentional or unintentional data leak, such as an insider, given their claims of a “continuous supply.”
- ZeroFox Intelligence is unable to confirm the proportion of scams such as these that lead to the payout of fraudulent tax returns, though their popularity within DDW forums in the weeks approaching April 15 indicate that a significant number of cyber threat actors consider it lucrative.

¹ [hXXps://thecollegeinvestor\[.\]com/35771/file-taxes-survey-2021/](https://thecollegeinvestor[.]com/35771/file-taxes-survey-2021/)

CR/Tax Form (1040/W-2)
MagaClub · Yesterday at 8:16 AM

ESCROW AVAILABLE IN THIS THREAD!

New deal



MagaClub
Make America Great Again
Пользователь
Joined: Oct 17, 2019
Messages: 224
Reaction score: 81
Deposit: 0.005 B

Yesterday at 8:16 AM

Цена: 20
Контакты: DM

Всем привет. В постоянном наличии Credit Report и Tax Forms (1040/W-2)
Full credit report (CS 700+) - 30\$
Tax Form (1040/W-2) - 20\$
По всем вопросам в личку. Все через гаранта.

Advertisement by MagaClub in DDW forum xss*Source: ZeroFox Intelligence*

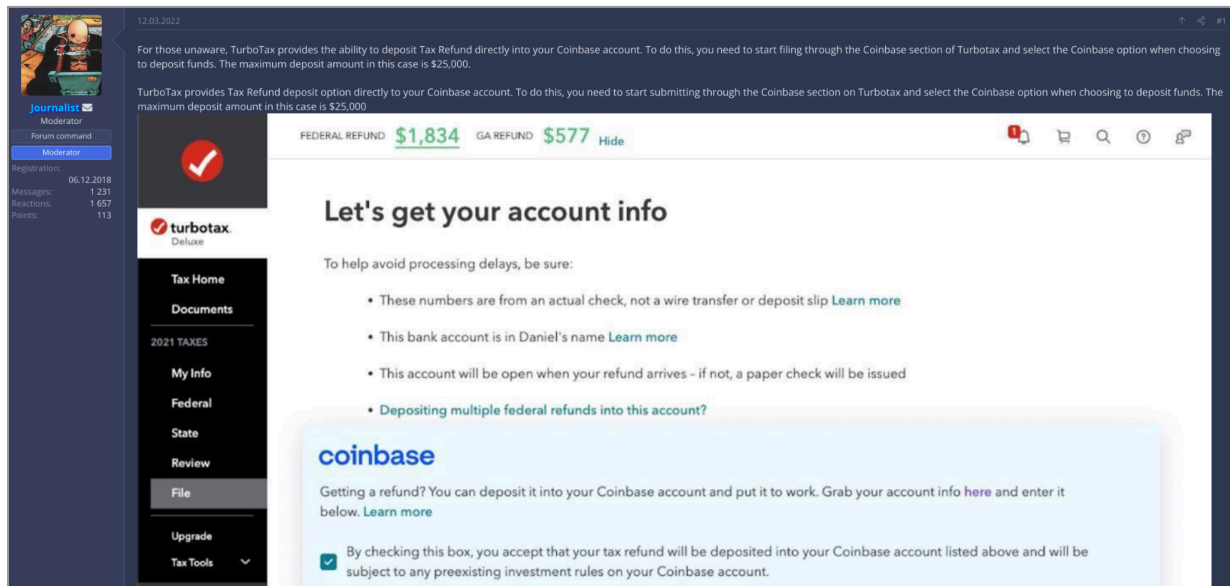
Threat actors are likely able to obtain tax return deposits by directly leveraging cryptocurrency exchange platforms, including via some third-party tax assistance software programs reportedly used by up to 50 percent of U.S. citizens.² These can enable threat actors to withdraw the currency with higher degrees of anonymity.

As well as tax return fraud, stolen PII is leveraged to conduct various other malicious tax-related schemes. Some of examples of these scams include:

- Threat actors use stolen PII to conduct phishing and spear-phishing campaigns, often masquerading as representatives of the IRS. These attacks are intended to trick the victim into providing personal details such as banking or Identity Protection PIN (IP PIN) information that can aid in further attacks. Malicious links can also be used to direct the victim to fake web pages that are able to deliver malware and harvest credentials.
- Threat actors attempt to collect false tax debt, using stolen PII to increase authenticity while imitating employees of either the IRS or an external debt collection agency. These attacks often leverage several social engineering techniques to encourage the victim's cooperation.

² [hXXps://www.credello\[.\]com/financial-resources/consumer-insights/tax-stress-return-survey/](https://www.credello.com/financial-resources/consumer-insights/tax-stress-return-survey/)

- Fake IRS letters claim that additional PII is needed in order to process an unclaimed tax refund. However, the information provided by the victim assists the threat actor in submitting fraudulent tax returns.



Post claiming that funds can be deposited to cryptocurrency platforms

Source: ZeroFox Intelligence

Activity of this nature is very likely to increase in frequency over the coming weeks, with threat actors continuing to evolve their TTPs to most effectively leverage illicitly-obtained PII that is relatively cheap and easily acquired in DDW forums. Social engineering is likely to play an increasingly more important role in granting threat actors the advantage needed to mitigate or circumvent contemporary IRS security features and claim fraudulent tax refunds.

Recommendations

- Individuals with a Social Security Administration (SSA) or an Individual Taxpayer Identification number (ITIN) should register annually for an IP PIN, using the following address:
 - [hXXps://www.irs.gov/identity-theft-fraud-scams/get-an-identity-protection-pin](https://www.irs.gov/identity-theft-fraud-scams/get-an-identity-protection-pin)
- Being implicated in a data breach could be the first step toward PII being leveraged to conduct tax fraud. In such a case, the individual should consider placing a “Fraud Alert” on their credit file.
- Suspected scamming or identity theft activity should be reported using [.gov] tools found here:
 - [hXXps://www.usa.gov/where-report-scams](https://www.usa.gov/where-report-scams)
 - [hXXps://www.identitytheft.gov/#/](https://www.identitytheft.gov/#/)
 - [hXXps://www.irs.gov/pub/irs-pdf/f14039.pdf](https://www.irs.gov/pub/irs-pdf/f14039.pdf)
- Individuals should scrutinize correspondence purporting to be from the IRS, particularly if received via unusual communication channels or if found to contain spelling or grammatical errors. If in doubt, further personal information should not be disclosed.
- Individuals using third-party tax return preparation services should ensure that documentation is appropriately signed upon completion.
- Organizations and individuals should ensure passwords are secure, unique credentials are used and phishing-resistant multi-factor authentication is implemented.

| 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%