CYBER THREAT ANALYSIS

Recorded Future®

By Insikt Group®

March 16, 2023

INTERNAL REVENUE SERVICE

IRS Cyberattack Highlights Risk of Tax Refund Fraud

Executive Summary

Tax season began on January 23, 2023, and with it came the return of tax refund fraud.

Recently, the threat group "Infinity Hackers BY" claimed to have conducted a successful cyberattack against the IRS. Whether or not the attack actually occurred, the threat group's claim highlights the threat posed by tax refund fraud, also known as stolen identity refund fraud (SIRF). Tax refund fraud occurs when criminals use stolen tax forms and personally identifiable information (PII) to submit fraudulent tax returns with the goal of stealing their victims' tax refunds.

Tax refund fraud incurs costs both for taxpayers and government agencies, particularly the IRS, and has demonstrated year-on-year growth in popularity across the dark web. In recent decades, electronic filing has simplified tax refund fraud; in order to conduct it, threat actors require only stolen tax forms and PII, which are often available for purchase on dark web sources, along with a fraudulently registered bank account.

Key Findings

- Tax refund fraud has become an increasingly popular topic on dark web forums. For the past 3 years, dark web forum posts relating to tax refund fraud have shown year-on-year growth, and in 2022, we observed 78,032 references to the keyword "tax" on dark web marketplaces.
- To conduct tax refund fraud, threat actors must obtain fraudulent or stolen tax forms, victim PII, and a fraudulently registered bank account before they submit a fraudulent tax return. Criminal tutorials, guides, references, and paid services simplify each of these tasks, ultimately facilitating tax refund fraud for inexperienced threat actors.
- The availability of stolen tax forms and PII necessary to conduct tax refund fraud drive its popularity and increase the risk it poses. Both stolen tax forms and associated PII are widely available via breached databases and dark web marketplaces.

Background

On January 12, 2023, the US Internal Revenue Service (IRS) announced that the 2023 tax season would begin on January 23, 2023. Tax season is now in full swing, and more than 168 million individual tax returns for the 2022 tax year are expected to be filed, accepted, and processed before the filing deadline of April 18, 2023.

The return of tax filing season throws tax refund fraud — also known as stolen identity refund fraud (SIRF) — into stark relief. By acquiring tax forms and sensitive personally identifiable information (PII) through data breaches, criminal services, and dark web resellers, criminals can file fraudulent tax returns under a victim's name in order to steal their tax refund. Electronic filing means that fraudulent returns can be swiftly submitted and processed, and stolen refunds can easily be deposited into fraudulently registered bank accounts, sent to prepaid payment cards, or even used to fund criminals' crypto accounts.

According to the US Department of Justice, tax refund fraud "threaten[s] to disrupt the orderly administration of the income tax system for hundreds of thousands of law-abiding taxpayers and [has] cost the United States Treasury billions of dollars". SIRF can result in delayed refunds for taxpayers and additional operating costs for the IRS. Once the fraud is discovered, victims must go through a daunting administrative process to prove their identities and rectify their situations.

The IRS recognizes the threat posed by SIRF, and has implemented advanced verification measures, encouraged taxpayers to safeguard their personal information and report suspicious activity, and even established a dedicated program to assist taxpayers affected by identity theft. The IRS also issues Identity Protection PINs (IP PINs) to confirmed victims of tax-related identity theft, which are used to verify the taxpayer's identity upon filing their tax return.

Threat Analysis

Alleged IRS Cyberattack Highlights Threat Posed by SIRF

On January 16, 2023, the administrators of a Russian-language Telegram carding channel created a post in which a threat group claimed to have carried out a successful cyberattack against the IRS. According to the group, the personal data of 198 million Americans was stolen during the attack. The post contained alleged video evidence of the compromise and was promptly shared in another Russian-language Telegram channel operated by a pro-Russian hacktivist threat group.

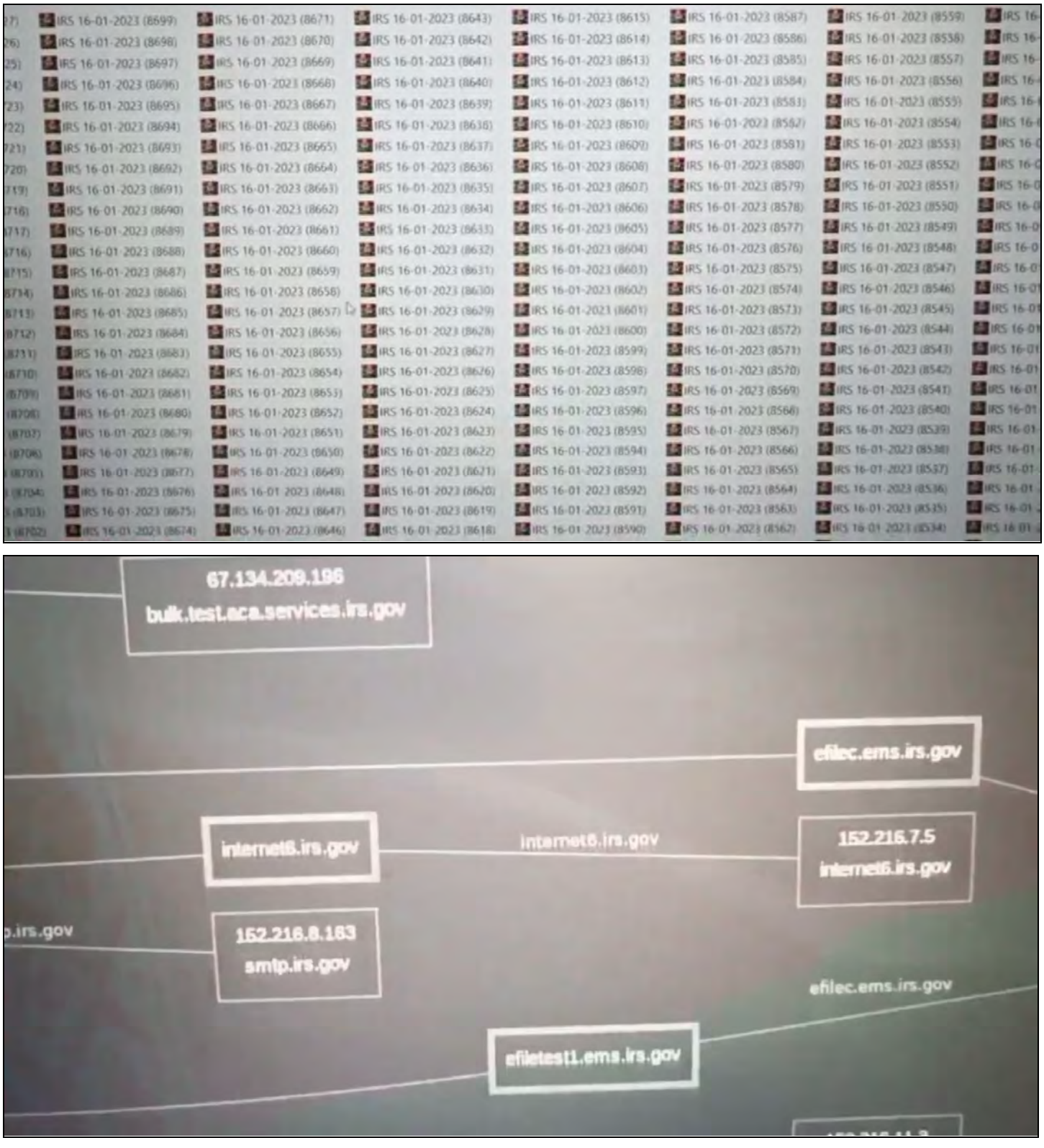


***Figure 1**: Screenshots from a short video posted to a Russian-language Telegram carding channel, which the channel's operators claimed was proof of a successful cyberattack against the IRS (Source: Telegram)*

The leader of the pro-Russian hacktivist threat group claimed that the IRS's infrastructure was compromised via a phishing attack. According to the threat actor, an IRS employee was tricked into entering their username and password on a fake version of a popular adult-entertainment website. Although the phishing attack allegedly occurred months ago, the threat actor stated that the attackers were only recently able to exploit the compromise.

It is entirely possible that the purported attack is pure fabrication. The pro-Russian hacktivist group has a history of seeking to provoke panic with spectacular claims, and its leader specifically claimed that this attack was conducted to demonstrate the capabilities of Russian and Belarusian threat actors in cyberspace. Given the current geopolitical confrontation between Russia and the US, pro-Russian threat groups may simply be seeking to stir up trouble with sensational news before tax season. As of this writing, we have yet to detect any sales of databases that are related to the supposed IRS breach on dark web marketplaces.

Nevertheless, the alleged cyberattack serves as an important reminder that taxpayers' sensitive PII and stolen tax records can be exploited to carry out tax refund fraud. In 2022, we saw 78,032 references to the keyword "tax" on dark web marketplaces, and for the past 3 years, we have observed year-on-year growth in the number of unique dark web forum posts directly related to SIRF.

2020	2021	2022
4,495	5,853	6,564

***Table 1**: For the past 3 years, dark web forum posts regarding tax refund fraud have steadily increased (Source: Recorded Future)*

How Does SIRF Work?

The alleged cyberattack raises the question of how exactly SIRF is committed — a question shared by many enterprising and ambitious threat actors.

Historical analysis indicates that during tax season, many threat actors involved in bank fraud seek to do so as part of a greater attempt to commit tax refund fraud. This is sensible — like holiday fraud, tax refund fraud is highly seasonal, relatively straightforward, and offers high returns given the time, resources, and effort required to conduct an attack. To execute an SIRF attack, cybercriminals must:

- Acquire stolen tax forms and victim PII
- Create a bank account to receive stolen tax refunds
- Submit a fraudulent tax return

For each of the stages described above, a multitude of criminal guides, recommendations, tutorials, and paid services can assist cybercriminals who lack prior experience in tax refund fraud.

Acquire Stolen Tax Forms and Victim PII

Stolen tax forms serve as the crucial foundation upon which tax refund fraud is built. Threat actors specifically target tax preparation firms in cyberattacks to steal tax forms, including:

- Form W-2 Wage and Tax Statement
- Form 1099-MISC Miscellaneous Information
- Form 1040 US Individual Income Tax Return

The previous year's Form 1040 is particularly valuable, as it contains the victim's adjusted gross income (AGI), which is necessary to electronically sign fraudulent tax returns — provided that the victim has not been issued an IRS Identity Protection PIN (IP PIN).

On December 16, 2022, the administrator of a Telegram tax refund fraud channel posted a price schedule for compromised tax forms in preparation for the 2023 tax filing season. Among these compromised tax forms were Form 1040, Form W-2, Form 1099-MISC, and more.

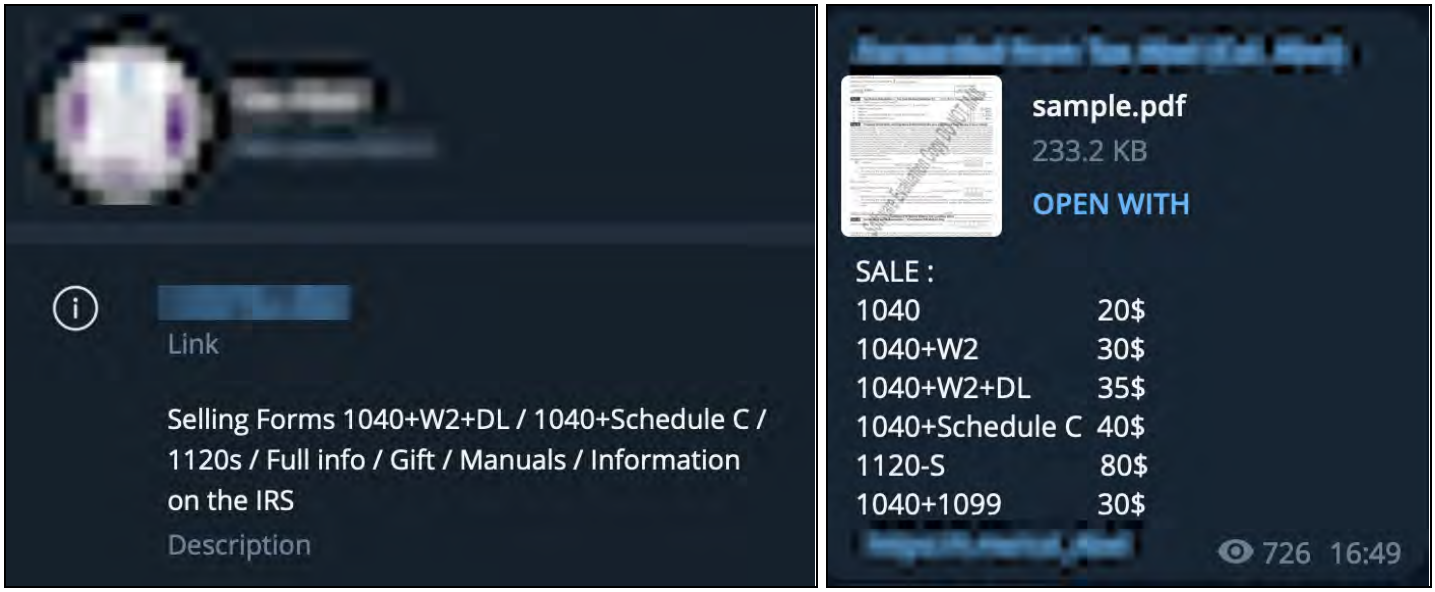


Figure 2: *Cybercriminals sell compromised tax forms that are crucial for tax refund fraud across various channels (Source: Telegram)*

With these tax forms in hand, threat actors have identified their targets. Next, "lookup" services allow criminal actors to pivot from their victims' stolen tax forms to the PII that will allow them to e-sign and file their fraudulent tax returns.

For example, the administrator of a Telegram carding channel advertised lookup services that criminal actors can use to acquire their victim's PII. Each entry is listed with a price to help cybercriminals find the bargains they're looking for.

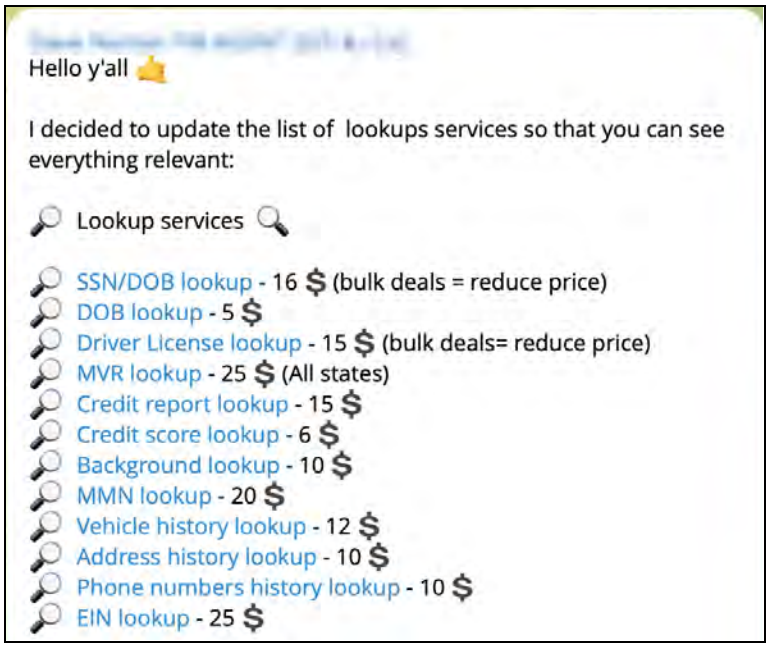


Figure 3: *This lookup service allows criminals to rapidly pivot from stolen tax forms to victim PII that they can use to facilitate tax refund fraud (Source: Telegram)*

Create a Bank Account to Receive Stolen Tax Refunds

To receive their victims' tax refunds, cybercriminals must control bank accounts that are registered in their victims' names. As with PII lookup, criminals can capitalize on services offered on dark web forums to do so. On August 23, 2022, a threat actor on a dark web forum posted an advertisement for their bank account registration service. Once cybercriminals provide the service with their target's PII, it registers a fraudulent bank account under the target's name.

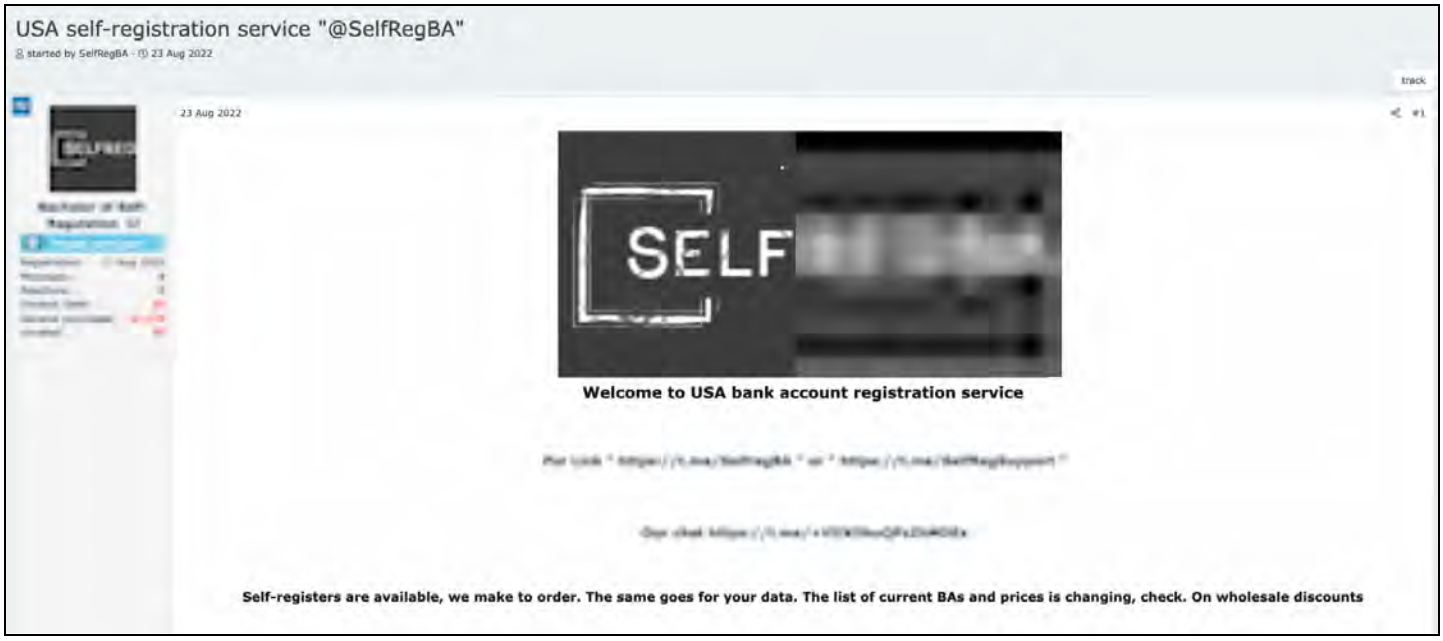
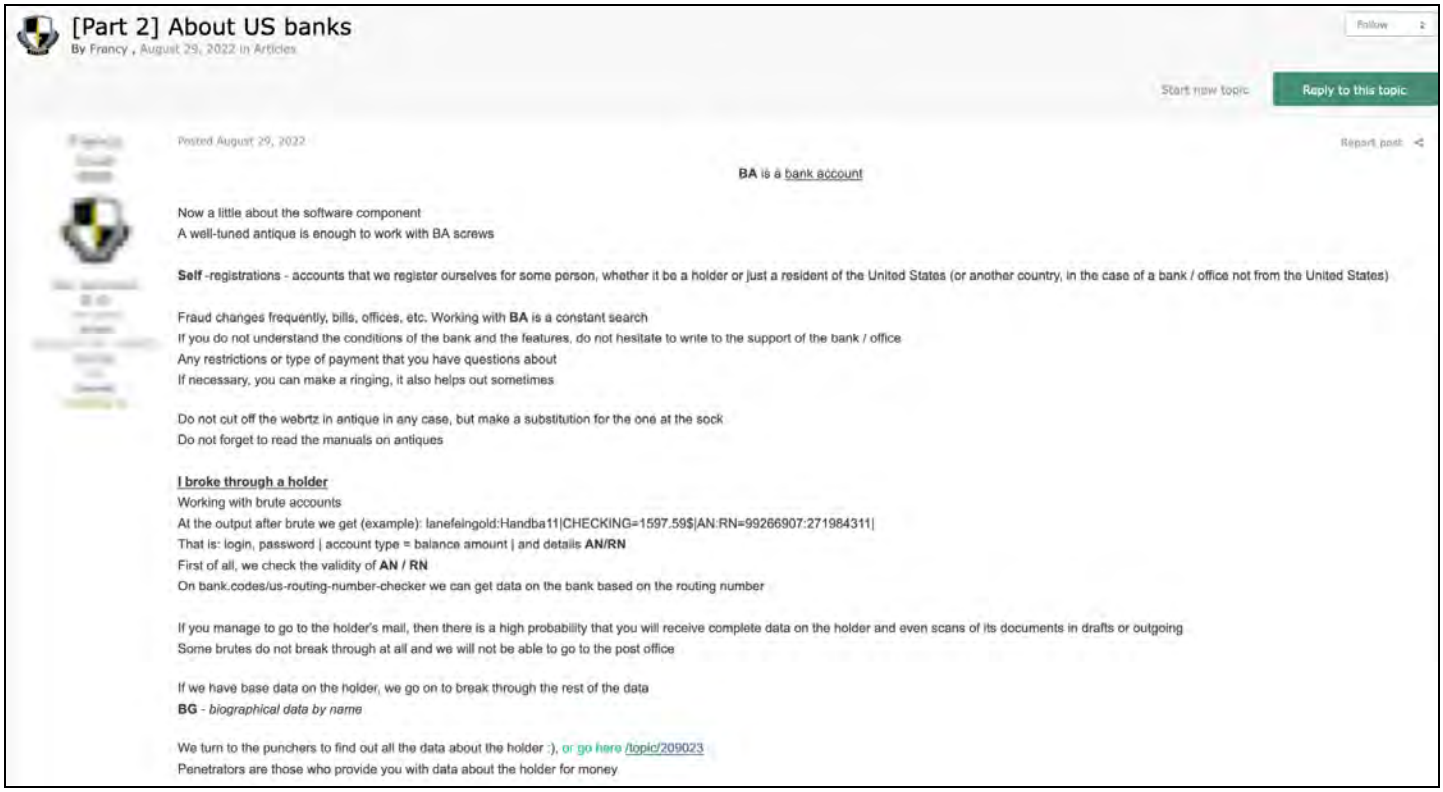


Figure 4: *This service assists threat actors in creating fraudulent bank accounts using victim PII (Source: Dark web forum)*

Alternatively, more self-reliant threat actors may choose to create bank accounts themselves using step-by-step tutorials. On August 29, 2022, a threat actor on a dark web forum posted a tutorial that demonstrated how to register fraudulent bank accounts under the names of cardholders whose payment card data has been compromised, among others.


[Part 2] About US banks
By Francy , August 29, 2022 in Articles

Follow

Start new topic | Reply to this topic

Posted August 29, 2022

Report post

BA is a bank account

Now a little about the software component
A well-tuned antique is enough to work with BA screws

Self -registrations - accounts that we register ourselves for some person, whether it be a holder or just a resident of the United States (or another country, in the case of a bank / office not from the United States)

Fraud changes frequently, bills, offices, etc. Working with **BA** is a constant search
If you do not understand the conditions of the bank and the features, do not hesitate to write to the support of the bank / office
Any restrictions or type of payment that you have questions about
If necessary, you can make a ringing, it also helps out sometimes

Do not cut off the webrtz in antique in any case, but make a substitution for the one at the sock
Do not forget to read the manuals on antiques

I broke through a holder
Working with brute accounts
At the output after brute we get (example): lanefeingold:Handba11|CHECKING=1597.59$|AN:RN=99266907:271984311|
That is: login, password | account type = balance amount | and details **AN/RN**
First of all, we check the validity of **AN / RN**
On bank.codes/us-routing-number-checker we can get data on the bank based on the routing number

If you manage to go to the holder's mail, then there is a high probability that you will receive complete data on the holder and even scans of its documents in drafts or outgoing
Some brutes do not break through at all and we will not be able to go to the post office

If we have base data on the holder, we go on to break through the rest of the data
BG - *biographical data by name*

We turn to the punchers to find out all the data about the holder :), or go here /topic/209023
Penetrators are those who provide you with data about the holder for money

Figure 5: *This tutorial provides threat actors with instructions to create fraudulent bank accounts (Source: Dark web forum)*

Submit a Fraudulent Tax Return

Once cybercriminals have acquired a target's PII and registered a fraudulent bank account in their victim's name, all that remains is to file a fraudulent tax return and receive the tax refund. US taxpayers have largely transitioned from paper returns to e-filing and direct deposits, mainly using tax preparation software. Criminals make use of the same tools to facilitate tax refund fraud.

On March 5, 2022, the administrator of a Telegram carding channel shared video instructions demonstrating how to submit tax returns using popular tax preparation software. In its preface, the post indicated that this software is an advantageous resource for tax refund fraud because it allows for the immediate deposit of tax refunds into crypto exchange accounts — that is, without using an intermediary bank account. It is likely that using a crypto exchange account to retrieve stolen refunds would still require actors to conduct preliminary new account fraud, as described in the previous section.

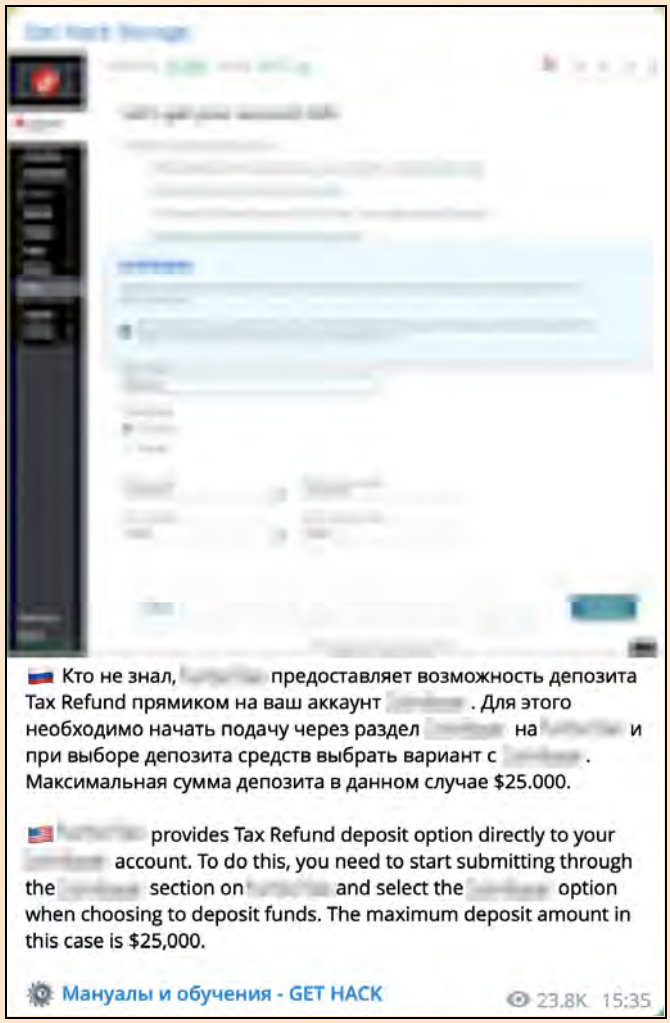


Figure 6: *A video tutorial shows criminals how to submit fraudulent tax returns using tax preparation software (Source: Telegram)*

Other threat actors have also zeroed in on the use of tax preparation software to facilitate tax refund fraud. On February 8, 2023, a threat actor on a dark web forum advertised another tutorial that describes how to file a fraudulent tax return and receive a tax refund using the same tax preparation software.

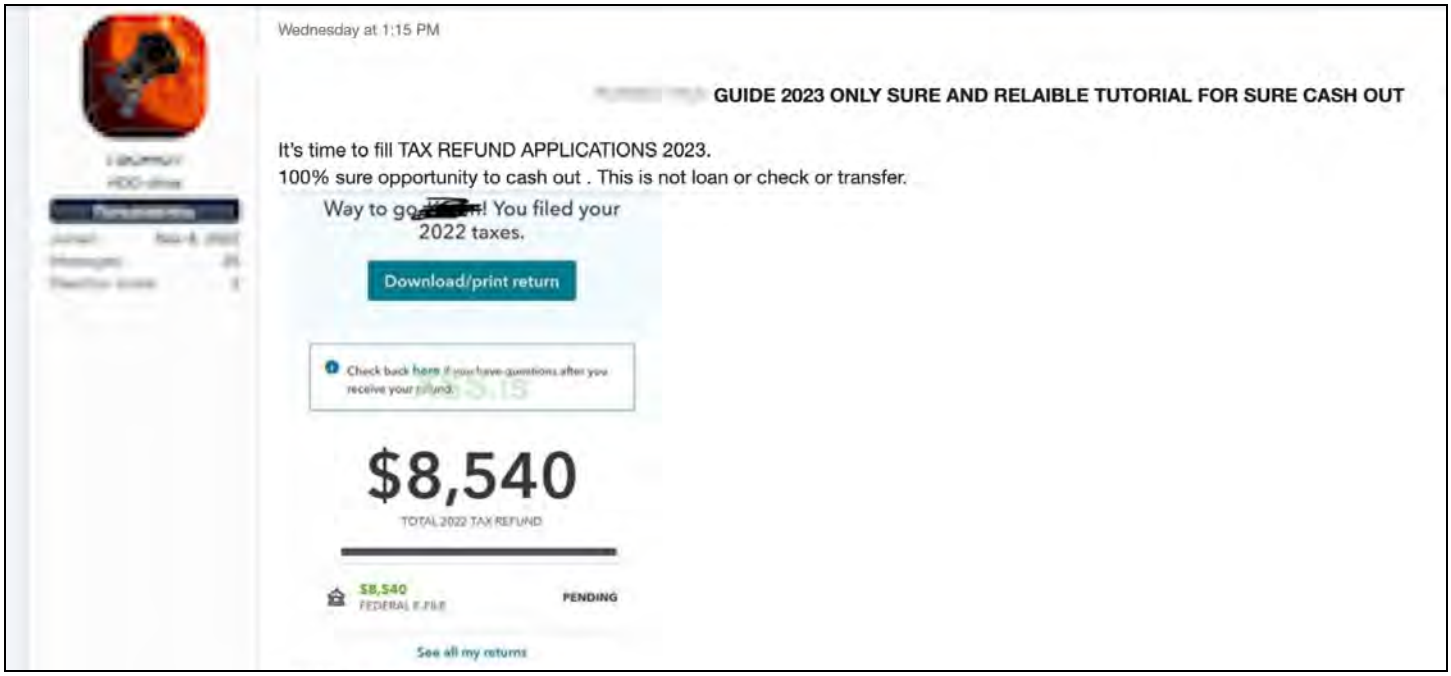


Figure 7: *A threat actor advertised a tutorial on how to submit fraudulent tax returns using tax preparation software (Source: Dark web forum)*

The Availability of PII and Tax Forms Increases the Risk Posed by SIRF

The relative accessibility of stolen tax forms and PII appears to be driving the popularity of tax refund fraud across the cybercriminal community. In addition to the sources listed above, our research indicates that cybercriminals have 2 chief means of obtaining stolen tax records and PII: data breaches and dark web marketplaces.

Data Breaches

Large-scale data breaches affecting all manner of organizations — from multinational corporations to government agencies and healthcare providers — have grown increasingly common over the past decade. Tax preparation firms are not exempt, and data breaches targeting tax preparers can provide threat actors with a vast supply of tax forms and victim PII that can be used to carry out tax refund fraud.

On July 27, 2022, a threat actor on a dark web forum advertised a database containing US residents' Social Security numbers (SSNs), dates of birth (DOBs), driver's license numbers, and W-2 tax forms. According to the threat actor, this data was previously used to obtain Coronavirus Tax Relief and was stolen from 2 tax preparation firms. The actor stated that the data belonged to over 435,000 victims from Ohio, Kansas, Texas, New York, and Florida.

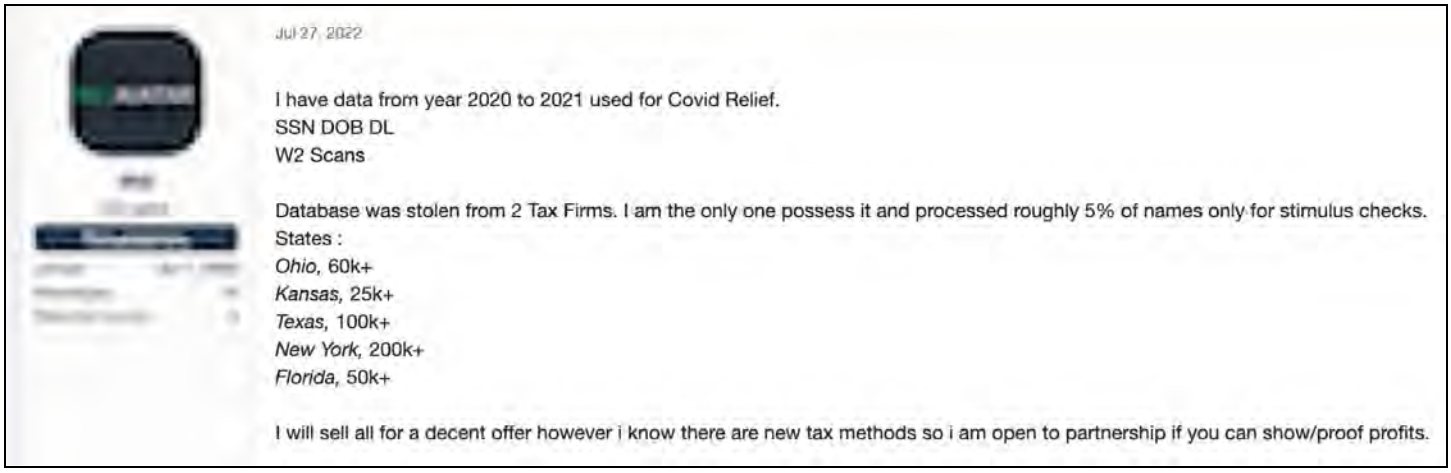


Figure 8: *A threat actor advertised a PII database that contained both PII and stolen W-2 forms (Source: Dark web forum)*

On January 3, 2023, a threat actor on a dark web forum auctioned a database of 12,000 US residents' PII records. Compromised information included SSNs, DOBs, full names, and employment information, all of which is necessary to e-file fraudulent tax returns. The auction for this database opened at $600, with immediate purchase available to actors willing to pay $900 outright. On average, each entry in the database was valued at 8 cents.

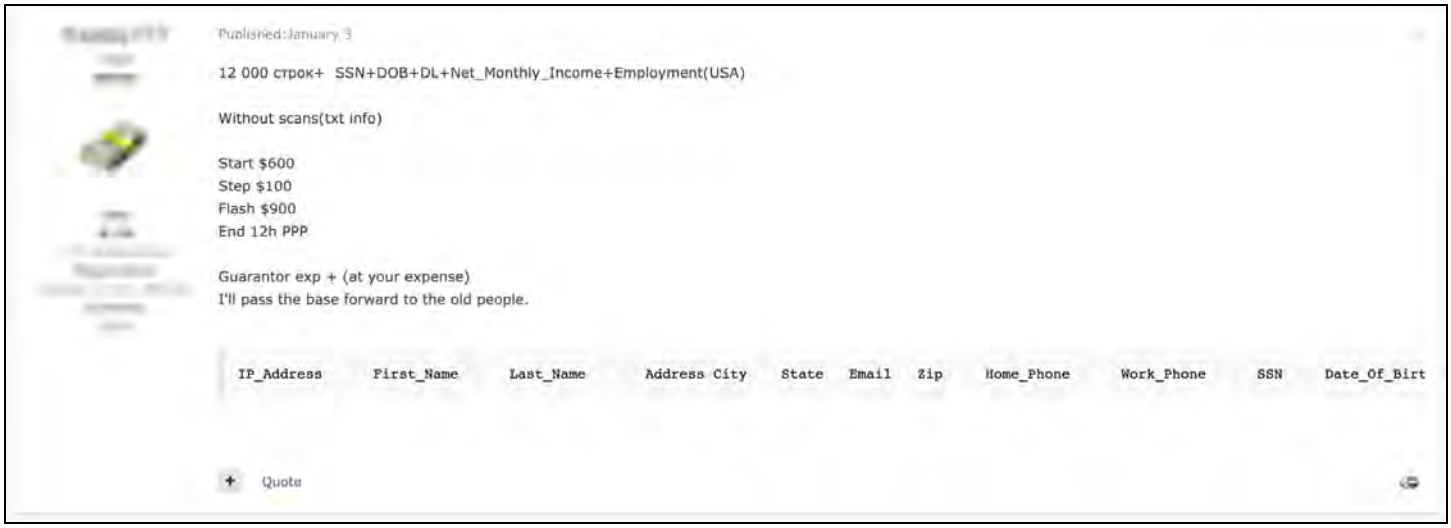


Figure 9: *A threat actor auctioned a database containing 12,000 entries of PII relating to US residents (Source: Dark web forum)*

On August 17, 2022, a threat actor on a dark web forum offered to sell a database that contained PII relating to 147 million US residents. The database included full names, email and physical addresses, phone numbers, and financial information that included credit scores and account balances. The threat actor also claimed that they had prepared a ready-to-go bundle of 6.9 million particularly valuable PII records relating to men born between 1980 and 2000. This database was listed for sale at $1.5 million — or just over 1 cent per entry.

Figure 10: *A threat actor advertised a database containing the PII data of 147 million US residents (Source: Dark web forum)*

The Dark Web Information Market

Across dark web marketplaces, entrepreneurial criminals scrupulously collect and curate sensitive information for sale. Unlike breached databases, which are often bought and sold in bulk, sellers on dark web marketplaces parcel out compromised data and tax records to be sold on an individual basis. Much of this information is obtained via cyberattacks and account compromises committed against individual (rather than organizational) victims. Besides tax forms and PII, the information sold on dark web marketplaces includes compromised login credentials, account data, payment card data, and much more.

Importantly, cybercriminals can purchase this non-PII data in order to indirectly acquire the tax forms and PII necessary to conduct tax refund fraud:

- Compromised user login credentials are highly desirable, allowing threat actors to enact account takeover (ATO) attacks that enable them to steal PII and tax forms.
- Compromised payment card data is frequently accompanied by victim PII that can facilitate tax refund fraud.
- Compromised documentation (including stolen passport data, driver's license numbers, billing statements, or tax records) can be leveraged to facilitate identity theft and register fraudulent bank accounts as part of a greater attempt to conduct tax refund fraud.

Figure 11: *This dark web marketplace is an especially popular purveyor of PII and other sensitive data that can be used to conduct tax refund fraud (Source: Dark web marketplace)*

Mitigations

- File taxes early to reduce criminals' window of opportunity to file fraudulent returns in your name.
- Request an Identity Protection PIN (IP PIN) with the IRS. IP PINs are unique 6-digit numbers assigned to eligible taxpayers that can greatly reduce the risk of tax refund fraud.
- Use the IRS Free File program. The IRS's free e-file service offers taxpayers a secure means of electronically filing taxes that can reduce the risk of identity theft or tax refund fraud.
- For taxpayers who choose not to take advantage of IRS Free File, choose a reputable tax preparation service to file your tax return. Reputable tax preparation services are more likely to keep sensitive personal information secure.
- Secure your online accounts with strong passwords and multi-factor authentication (MFA). In many cases, this is enough to deter opportunistic threat actors.
- Exercise caution while sharing personal information online, and treat emails or phone calls that request personal information with suspicion.
- Routinely monitor credit reports to detect suspicious activity. If suspicious activity is found, immediately notify credit reporting agencies, the IRS, the Federal Trade Commission (FTC), and local law enforcement.

Outlook

In the current tax season, an IRS cyberattack allegedly carried out by the threat group Infinity Hackers BY highlights the threat posed by tax refund fraud. Once cybercriminals have access to stolen tax records and PII, the steps necessary to file fraudulent tax returns and steal victims' tax refunds are relatively straightforward, and they are made simpler by abundant criminal guides and services on the dark web. Because of the complexity of tax law, taxpayers are unlikely to detect tax refund fraud until they personally file their tax return. This may lead to processing delays — and ultimately, a delayed refund and increased operating costs for government agencies.

Stolen tax forms and PII are widely available on the dark web, creating an extensive attack surface for threat actors seeking to conduct tax refund fraud. Moreover, over the past 3 years tax refund fraud has become an increasingly popular topic in the cybercriminal community. For these reasons, we assess that SIRF will continue to represent a significant threat to taxpayers and government agencies in coming years.

About Insikt Group®

Recorded Future's Insikt Group, the company's threat research division, comprises analysts and security researchers with deep government, law enforcement, military, and intelligence agency experience. Their mission is to produce intelligence that reduces risk for clients, enables tangible outcomes, and prevents business disruption.

About Recorded Future®

Recorded Future is the world's largest intelligence company. Recorded Future's cloud-based Intelligence Platform provides the most complete coverage across adversaries, infrastructure, and targets. By combining persistent and pervasive automated data collection and analytics with human analysis, Recorded Future provides real-time visibility into the vast digital landscape and empowers clients to take proactive action to disrupt adversaries and keep their people, systems, and infrastructure safe. Headquartered in Boston with offices and employees around the world, Recorded Future works with more than 1,500 businesses and government organizations across more than 60 countries.