

CYBER
THREAT
ANALYSIS

•|||• Recorded Future®

By Insikt Group®

February 15, 2021



THE BUSINESS OF FRAUD: Tax Refund Fraud



Recorded Future analyzed current data from the Recorded Future® Platform, dark web sources, and open-source intelligence (OSINT) between January 2021 and November 2021 in a review of the current tax refund fraud landscape. This report expands upon findings addressed in the first Insikt Group Fraud Series report, "[The Business of Fraud: An Overview of How Cybercrime Gets Monetized](#)".

Executive Summary

Threat actors use a diverse set of sophisticated tactics, techniques, and procedures (TTPs) to defraud tax service authorities worldwide. Overwhelmingly, however, the focus of tax fraud is the United States Internal Revenue Service (IRS). This type of fraud is not limited to identity theft but also encompasses corporate network compromise, ransomware, money laundering, and social engineering attacks. Tax return fraud is an established and perennial business on the dark web that primarily coincides with tax season in the United States from January 1 to April 15 each year.

Key Judgments

- The number of ransomware attacks and network intrusions affecting accounting firms and tax refund services providers steadily grew in 2021.
- Threat actors primarily advertise and request tax refund fraud-related services on Russian-language top-tier forums such as Exploit, XSS, and Verified; however, they sell compromised account login credentials for tax-related services mostly on the dark web shops like Genesis Store, Russian Market, and Amigos Market.
- Tax return fraud will remain a significant threat for the foreseeable future and is likely to remain largely focused on defrauding US citizens and those required to file US tax returns.

Background

Tax return fraud, also known as [stolen identity refund fraud](#) (SIRF), is a specific case of identity theft where a criminal files a federal or state tax return using a victim's information with the goal of stealing their tax refund. The success of these schemes relies on criminals' filing tax returns before the person whose information has been stolen files their taxes. In the underground economy, tax refund fraud frequently requires collaboration between multiple threat actors with different specialties, such as collecting credit reports and tax forms in bulk, gaining access to online tax preparation software to submit the tax return, and recruiting money mules to receive and send the stolen tax refunds. Other attackers may target tax preparation firms directly, as gaining access to these networks will provide both the victim personally identifiable information (PII) and the tax software needed for SIRF.

While most tax fraud is seasonal, peaking in the months before filing and extension deadlines, some threat actors file amended tax returns of compromised accounts even years after the victims had already filed, including fictitious losses and requesting additional refunds without the victim ever knowing.

Tax refund fraud is a perennial problem involving the use of identity information and often includes using stolen or misdirected W-2 forms to electronically file an unauthorized tax return to claim a refund in the name of a taxpayer. Victims usually first learn of the crime after having their returns rejected because a criminal filed their return first. Individuals who are not required to file a return can also be a victim of refund fraud, including individuals who wouldn't be due a refund from the IRS.

As many criminals who commit tax fraud are operating out of countries with no extradition policies, it can be difficult, although [not impossible](#), to prosecute them successfully.

Threat Analysis

SIRF crimes are often perpetrated by large criminal enterprises. An operation might include individual criminals who steal Social Security numbers (SSN) and other PII, others who file false returns with the IRS, those who facilitate obtaining the refunds, and the leaders who promote the schemes. These criminal enterprises exploit the speed and relative anonymity of highly automated systems for storing personal information, preparing and filing tax returns electronically, and generating income tax refunds quickly — often in the form of electronic payments.

Identities used in SIRF crimes may be stolen from anywhere. For example, SIRF criminals have used SSNs stolen from hospitals, nursing homes, and public death records, thereby exploiting some of the most vulnerable members of society. However, everyone with an SSN is potentially vulnerable to identity theft.

Typically, SIRF perpetrators file false returns electronically early in the tax filing season so that the IRS receives the false return before a legitimate taxpayer has time to file their taxes. The SIRF perpetrators arrange to have the refunds electronically transferred to debit cards or delivered to physical addresses where they can obtain the stolen refund from the mail.

The entire process can be broken down as follows:

- Obtain PII
- File fraudulent returns
- Launder the stolen money (this activity can be observed on criminal underground forums)

Criminal Underground Forums

Within the underground ecosystem, four communities (Exploit, XSS, Verified, and Raid) generate the fraud ecosystem, with threat actors facilitating the sale of stolen PII and providing members with supplementary services that help to minimize the risk associated with this type of criminal activity.

For example, as shown in this Verified Forum Direct Messages leak, one threat actor, “Scarlet”, offers automation solutions to fellow members. In a conversation with the threat actor “Rob” that occurred on January 18, 2021, Scarlet suggested that they can automate the tax refund filing process so it will work with “200 hired employees”.

I need to draw on my data 2019 Business tax Shortmoney
Tax links Ashan
Help with Form SS-4 helsenki7
Buy scans (business topics) dotcom1
I will buy Dedicated computers with TAX software samuraiage
TAX forms (Taxes) who the Pro pulls from the Bots and fulfills. bobrikowwww
TAX in007
nerv; alcatraz - n3rv@jabber.dk *****
Need Turkish kit (ID / TAX + bill * + selfi *) Azino
куплю 1040 + w2 tax form 2019 foodandtickets
Buy 1040 tax form for 2019 Rob.
Buy 1040+W2 tax forms GameStop
2019 tax refund form needed urgently abby0111
tax return - automated Scarlet
break EIN / TAX ID - I'll pay \$ 100 for a break CashoutMaster
Куплю 1099s и 1120 tax forms LLC/INC encrypted

Figures 1 and 2: Posts that offer tax-related criminal services and solutions (Source: Verified Forum)

Tax Refund Service
By GREAT, Tuesday at 02:18 PM in Auctions

Follow 1

Start new topic Reply to this topic

Report post

GREAT
terabyte
★★★★★
04/17/19 ID: 922041
Activity
dpyrce / other

Seller
18
260 posts
Joined

Posted Tuesday at 02:18 PM

Всем привет. Продам доступ к сервису по приему TAX форм в следующих странах: US, UK, DE, IE, NO, DK, NL, AU. Компания работает > 20 лет. Ежегодно подается примерно 20 000 форм, из них US = 15 000.

Схема их работы. Принимают от человека весь пакет документов -> Сами подают за него их -> получают выплату -> направляют человеку.

Есть 3 вектора эксплуатации доступа:

1. Эксплуатировать прошлогодние комплекты(Хранят за 4 последних года, в базе ~ 80 000 комплектов)
2. Перехватывать комплекты и подавать их самостоятельно
3. Вписывать свои реквизиты для получения от компании

База и все аттачи пользователей выкачаны. В скатом виде (.tar.gz), все это дело занимает 200GB. (Попкупателю передадим в зашифрованном архиве сами - это лучше, чем если вы будете лично и без опыта выкачивать и все полагите).

Доступ к сервису живой и готов к эксплуатации. Если бы я работал по Tax формам - сам бы использовал, но я далек от этого, кто знает - тот знает.

Старт: \$100 000
Шаг: \$10 000
Блиц: \$150 000

Гарант приветствует. Всех с началом сезона Tax Refund !

+ Quote

Figure 3: GREAT auctioning off network access to a tax refund firm (Source: Exploit Forum)

On October 5, 2021, the threat actor "GREAT" was observed on Exploit selling network access to a service that processes tax forms in the US, UK, Germany, Ireland, Norway, Denmark, the Netherlands, and Australia. The threat actor listed three attack vectors for potential buyers:

- Use PII from databases (the service stores data from the past four years, approximately 80,000 data packages (the PII required to carry out such fraud). The threat actor stated that they downloaded the full dump (approximately 200 GB in a compressed and encrypted format). They also mentioned that the server is "alive" and ready to work.
- Resell the compromised databases.
- File counterfeit tax forms by entering and submitting fictitious personal information.

On July 13, 2021, the threat actor "zanko", a member of Exploit, sold a database of a tax refund service provider with more than 250,000 user records who operate in more than five countries, including the US, the UK, the Netherlands, Ireland, and Germany for a total of \$4,000 to an unknown buyer. According to the threat actor, the database contained PII such as SSNs, addresses, full names, tax information, and additional information.

On January 6, 2021, "bl33d", a member of Exploit, was auctioning US taxpayer PII for as many as 1,500 individuals, including W-2 forms, driver's licenses, and SSN scans. bl33d provided screenshots indicating that the data was possibly obtained from a certified public accounting (CPA) firm in California. As shown in Figure 5, the driver's licenses sold by bl33d appear to have been issued between 2017 to 2019, suggesting that their viability for unauthorized use will be extended considering their expiration date.

In addition to the sale of PII and tax forms needed to conduct SIFR, underground communities have multiple members who purchase access to PCs and networks belonging to CPA firms running tax software, as well as provide money laundering services to obtain fraudulent tax returns.

One such threat actor is "iqservicc", who regularly buys Remote Desktop Protocol (RDP) access to PCs running recent, popular tax software. This allows an attacker to fraudulently file taxes on legitimately purchased and registered tax software through IP addresses that would not appear suspicious (as opposed to VPNs, proxies, or geographically distant IP addresses). Such a combination greatly increases the chance of processing a successful tax refund through the IRS.


On October 12, 2021, the threat actor "inthematrix1", a member of Exploit, auctioned off access to the network of an unspecified Indian accounting company, claiming to have gained access to the server with corporate documents. The starting price was \$2,200 or it could be purchased directly for \$4,000.

环 tax refund site DB Follow 1

By zanko, Yesterday at 01:27 PM in [Access] - FTP, shells, root, sql-inj, DB, Servers

Start new topic Reply to this topic

zanko
Access & 0 Days
●●●



Paid registration
6
89 posts
Joined
10/09/20 (ID: 109365)
Activity
хакинг / hacking

Posted yesterday at 01:27 PM

selling database of tax refund service provider. operates in 5+ countries, US, UK, Germany, Ireland, Netherland. contains 250k client details such as tax info, ssn, name, address etc.


Quick sale: 4k

Name/proof will be revealed who is genuine and previous buying history on forum, I also have my own list of people who come ask name and never comeback so if you one of those don't bother to pm else straight report.

+ Quote

Figure 4: Zanko sold a database of a tax refund service provider (Source: Exploit Forum)

bl33d
Mindcoms
●●●●



Paid registration
11
144 posts
Joined
11/15/19 (ID: 97214)
Activity
спам / spam
Deposit
0.033000 ₿

Posted January 4 Report post

Each folder represents each client , in each folder you will find W2 scans + DL scans , sometimes there is ssn card scans but occasionally you may find W2 and dl Scans of multiple persons in one folder. in some you will find W2 history of a client from 2017 -2019 DL scans have good quality and 70++ % have good expiry dates .


<http://prntscr.com/wgbfb2> DL scans front
<http://prntscr.com/wgbgxx> DL scans back
<https://prnt.sc/wgbjxk> W2 Scans
<https://prnt.sc/wgbmmv> MULTIPLE SSN SCANS
<https://prnt.sc/wgbonr> MULTIPLE DL SCANS
<https://prnt.sc/wgbr3u> DL + SSN SCAN FRONT
<https://prnt.sc/wgbrx9> DL + SSN SCAN BACK
<http://prntscr.com/wgbthz> W2

Start : \$11,000
 Step : \$250
 Blitz : \$15,000

+ Quote

Figure 5: bl33d's advertisement (Source: Exploit Forum)

iqservicc
gigabyte
●●●●



User
1
129 posts
Joined
05/07/14 (ID: 55174)
Activity
другое

Posted September 3

Всем доброго времени суток.

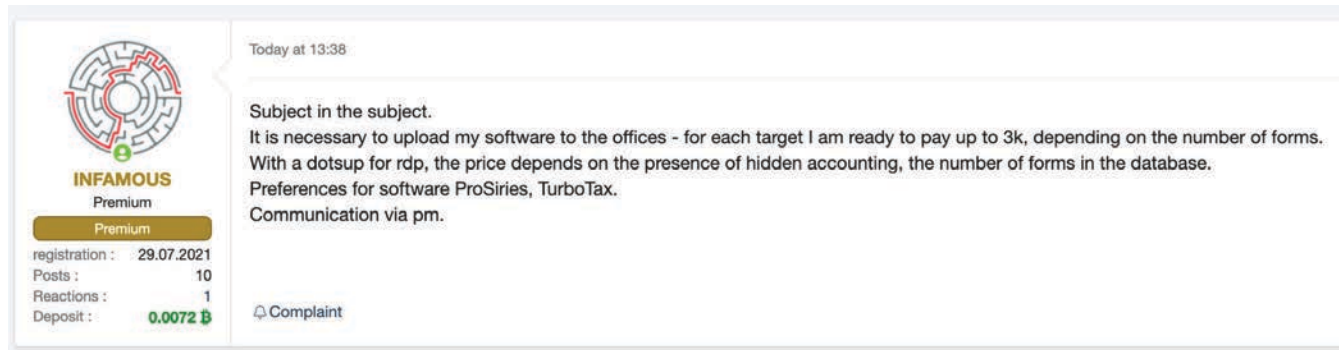
- Скупаем ваши US рдп (дедики) с программами ProSeries, Turbotax, Drake, Lacarte, ATX, Taxwise, TAXSLAYER PRO, CrossLink, ProTaxPro. [2021]
- Наши цены вас порадуют, если рдп не были сданы в 100+ рук. Цена зависит от доступа, с админ правами, без - с целой сеткой либо без.
 - Оплачиваем в BTC без задержек.
- Все легко проверяется, поэтому сразу прошу отсечься любителям халавы дабы не тратить время как вам так и нам.
- За подробностями в ПМ.

For ENG

- We buy RDP's with softwares on them ProSeries, Turbotax, Drake, Lacarte, ATX, Taxwise, TAXSLAYER PRO, CrossLink, ProTaxPro. [2021]
 - High prices if it's not reselled access.
 - Paying BTC, no delays.
- For further information please write to the PM.

+ Quote

Figure 6: An advertisement shared by iqservicc (Source: Exploit Forum)



Today at 13:38

Subject in the subject.
It is necessary to upload my software to the offices - for each target I am ready to pay up to 3k, depending on the number of forms.
With a dotsup for rdp, the price depends on the presence of hidden accounting, the number of forms in the database.
Preferences for software ProSeries, TurboTax.
Communication via pm.

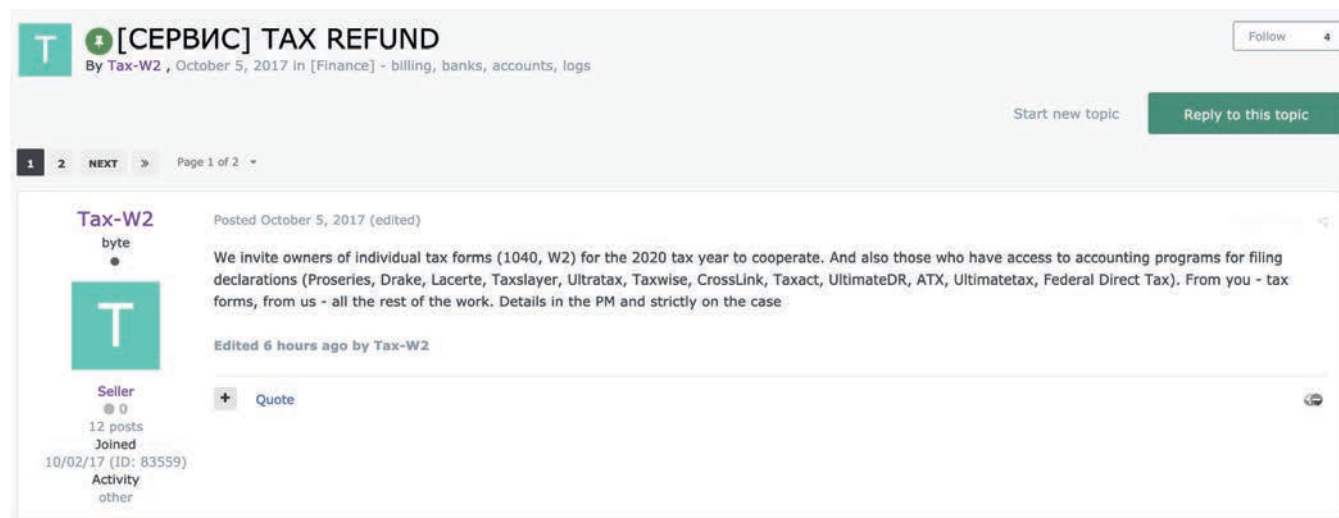
Complaint

Figure 7: An advertisement shared by threat actor INFAMOUS (Source: XSS forum)

On October 13, 2021, threat actor “INFAMOUS” requested on XSS forum to deploy their malware in the networks of the CPA firms for a \$3,000 fee. They mentioned a preference for filing with various tax software.

- On March 10, 2021, threat actor bl33d on Exploit sold RDP access to a server connected to another server that hosted Lacerte tax software belonging to an unspecified US accounting firm. The opening price for RDP account credentials was \$100, or access could be purchased directly for \$500. The winner of the auction was likely the threat actor “mistarmicky”.
- On February 28, 2021, the threat actor “pshmm” on Exploit was auctioning off access to a domain administrator account with linked documents of an unnamed Canadian tax-related company with thirty hosts. The starting price for the account credentials was \$500, with the option of an immediate purchase for \$1,000. The results of this auction are unknown.

The final link to this fraud chain is the tactic referred to as a “cashout method.” Cashout services are offered by threat actors such as “Асад” (Asad), who specialize in laundering funds stolen from tax refunds through an automated clearing house (ACH) or using a wire transfer to accounts under their control. This type of service would be used by actors such as “iqservicc”, who submits tax refunds through compromised computers running tax software with a victim’s PII obtained from other threat actors such as bl33d. Асад likely uses a series of money mules and verified crypto-exchange accounts, transferring funds from one to another before finally delivering the funds to an account controlled by their client, who is ultimately the threat actor who initiated the fraudulent refund.



[СЕРВИС] TAX REFUND
By Tax-W2, October 5, 2017 in [Finance] - billing, banks, accounts, logs

Follow 4

Start new topic Reply to this topic

1 2 NEXT Page 1 of 2

Tax-W2
byte
•

Posted October 5, 2017 (edited)

We invite owners of individual tax forms (1040, W2) for the 2020 tax year to cooperate. And also those who have access to accounting programs for filing declarations (Proseries, Drake, Lacerte, Taxslayer, Ultratx, Taxwise, CrossLink, Taxact, UltimateDR, ATX, Ultimatetax, Federal Direct Tax). From you - tax forms, from us - all the rest of the work. Details in the PM and strictly on the case

Edited 6 hours ago by Tax-W2

Quote

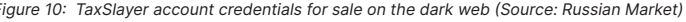
Seller
• 0
12 posts
Joined
10/02/17 (ID: 83559)
Activity
other

Figure 8: An advertisement by Tax-W2 (Source: Exploit)



Genesis Store, Russian Market, and other shops provide a unique opportunity for threat actors to combine online identity takeover with SIRF by allowing them to gain direct access to victim PII and online tax preparation software in a single marketplace. An ideal victim would have an account from a credit bureau like TransUnion, Experian, or Equifax, along with a tax software account. An attacker would be able to purchase account credentials, session cookies, and browser fingerprints from Genesis Store, gather PII, and then submit a tax return on the same tax software used by the victim, circumventing the tax agency's anti-fraud measures. Genesis Store is a criminal marketplace that sells "bots" or combinations of accounts, session cookies, browser fingerprints, and other system information, which threat actors can purchase and upload into a custom Chromium plugin called "Genesis Security".

The bots sold on Genesis Store can provide a wealth of financial information from accounts at credit bureaus, the IRS, online tax preparation software, and cloud-based payroll software, all of which can provide an attacker with all the resources necessary for income tax return fraud. Examples of accounts advertised on Genesis Store include ADP and Paylocity accounts, through which an attacker can download a victim's W-2. There are consistently TransUnion, Equifax, Experian, and CreditKarma accounts in stock that can provide a wealth of personal and financial information. IRS and Social Security Administration (SSA) accounts are also commonly found on the Genesis Store, which can be used by threat actors to request victim tax documents from previous years.



Genesis Store is also a source for online tax preparation software accounts. An ideal Genesis bot for tax fraud would use tax software paired with the credit bureau payroll software so all the tools and PII are accessible together for a single individual or family.

Bots that operate without access to online tax software or credit bureau accounts can also be sources for income tax fraud through online identity takeover. The higher-value US bots sold on Genesis Store frequently come with related social media and financial accounts. Armed with the large amounts of PII stored in merchant and social media accounts and mobile phone providers, an attacker could bypass knowledge-based authentication (KBA) protections used by credit bureaus. In theory, an attacker could purchase the exact tax software they need with the victim's own information and then file under a victim's name.

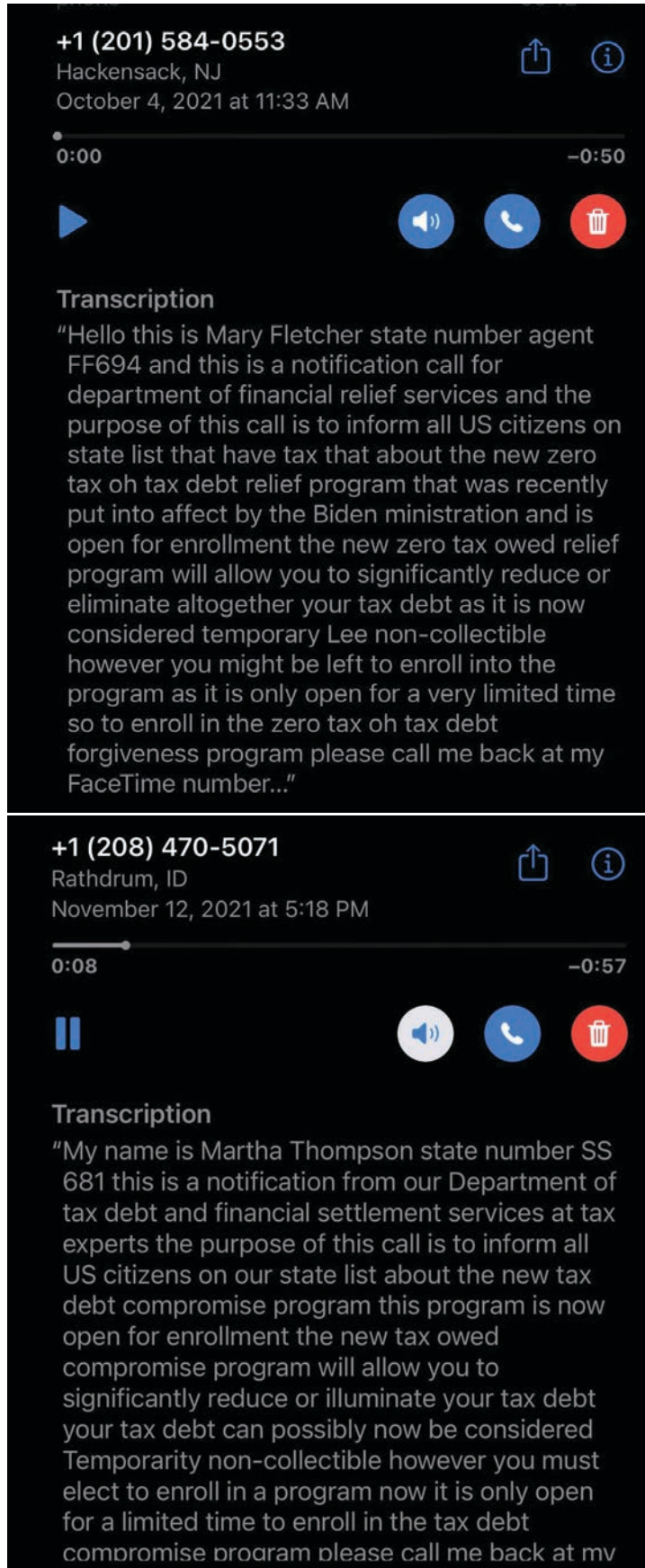
Phone Scams

The IRS has [reported](#) that “thousands of people have lost millions of dollars and their PII to tax scams. Scammers use regular mail, telephone, or email to set up individuals, businesses, payrolls, and tax professionals.” The IRS has made clear that they do not initiate contact with a taxpayer through email, text messages, or social media channels and that they will not request personal or financial information; they advise the public to recognize the [telltale signs](#) of a scam.

As shown in figures 12 and 13, criminal actors will portray themselves as legitimate operators from the IRS and try to obtain sensitive personal information. These operators will try to intimidate the victim and pressure them to provide the PII or commit fraud on their behalf. Sometimes, the threat actors attempt to coerce the victim into sending them money to avoid “penalties” and “criminal liabilities”.

The screenshot shows a marketplace listing for a "W-2 form for tax refund" by the vendor "empiredeals". The listing includes a thumbnail image of a W-2 form, a price of USD 65.00, and a quantity of 1. The listing also features a "Vendor Level 5" and "Trust level 5" badge. The product details include "Product Class: Digital Goods", "Quantity Left: 987", "Ends In: Never", "Origin Country: Worldwide", "Ships to: Worldwide, Europe", and "Payment: Escrow". The listing is categorized under "D - 1 day - USD 0.01 / 0.00000 BTC". Below the listing, there is a section for "Description", "Feedback", and "Refund policy". The description text reads: "I AM NOW OFFERING CUSTOM SCANS SERVICE: VERIFY YOUR APPLICATIONS / ACCOUNTS EASY AND FAST: AND IF YOU ADD 45\$ I WILL DO SELFIE FOR YOU- 24 hours delivery time...". The refund policy states: "1) DL FROM USA , ALL STATES - FOR SAMPLES MESSAGE ME".

Figure 11: W-2 tax refund fraud method advertised by “empiredeals” (Source: MGM Grand Market)



Figures 12 and 13: Voicemail messages transcribed (Source: Recorded Future)

Ransomware Victims

Since early 2020, Recorded Future has identified more than 40 public ransomware incidents involving the accounting services industry. The most recent event occurred on October 7, 2021, when the AvosLocker ransomware gang threatened to expose stolen data from the "Hill and Associates CPAs", a tax preparation firm in Lincoln, Nebraska. Ransomware operators exposed several 1040 forms on their extortionist blog, AvosLocker Press Release, to prove access.

Mitigations

While identity theft may be difficult to prevent entirely, there are steps one can take to make it more difficult:

- Check your credit report regularly.
- Do not carry your SSN card or any document containing your SSN.
- Properly dispose of documents that contain sensitive information; shred them instead of throwing them in the trash.
- Only give out your PII when absolutely necessary — especially on websites and social media websites — and keep track of who you give it to (this could help determine the source of a breach of PII if you become a victim).
- Protect your personal computers by using firewalls and the latest anti-virus software.
- File your taxes as early as possible during tax season since criminals using stolen identities tend to file their fraudulent returns early to obtain refunds before the legitimate filer submits a return.
- If not required to file a tax return, consider filing anyway to prevent someone else from filing a false return in your name and to be alerted in case someone has already filed a false return in your name.

Outlook

Within the underground economy, there are relatively few threat actors who specialize in creating fake tax returns or providing tax forms from sources such as compromised companies. The personally identifiable information of US taxpayers, by contrast, is available in abundance on criminal marketplaces, which can give threat actors direct access to the victim information along with online tax software to file fraudulent returns in an online identity takeover. This ideal combination of data will likely make Genesis Store an attractive resource for threat actors looking to file fraudulent tax returns and lowers the barriers to entry for newcomers in this niche category of fraud.

About Recorded Future

Recorded Future is the world's largest provider of intelligence for enterprise security. By combining persistent and pervasive automated data collection and analytics with human analysis, Recorded Future delivers intelligence that is timely, accurate, and actionable. In a world of ever-increasing chaos and uncertainty, Recorded Future empowers organizations with the visibility they need to identify and detect threats faster; take proactive action to disrupt adversaries; and protect their people, systems, and assets, so business can be conducted with confidence. Recorded Future is trusted by more than 1,000 businesses and government organizations around the world.

Learn more at recordedfuture.com and follow us on Twitter at @RecordedFuture.