Carbon Black.

Tax Fraud & "Identity Theft On Demand" Continue to Take Shape on the Dark Web

APRIL 2019

Introduction

While online sales of identity and banking information have both been easily accessible to malicious actors for a decade or more, there has been a recent maturation in the dark web economy focused on tax identity theft.

Carbon Black's recent research into various marketplaces on the dark web found W-2 forms, 1040 forms and how-to guides for illicitly cashing out tax returns available. W-2s and 1040s are available on the dark web at relatively low cost, ranging from $1.04 to $52. Names, Social Security Numbers (SSNs) and birthdates can be obtained for a price ranging from $0.19 to $62.

For a more comprehensive investment (around $1,000) a relatively inexperienced hacker can purchase authenticated access to a U.S.-based bank account, file a false tax return, claim the IRS refund and cash out via a cryptocurrency exchange for a 100+% return on investment.

Perhaps most notable is that an identity theft cycle can now be completed by an attacker without ever stepping foot outside or showing their face to another human via "identity fraud on demand," a process by which a hacker can provide stolen/purchased identity information and receive an original image of a person holding a forged passport with matching picture/information and scans of the forged identity documents.

The research also found that various tax identity theft products and services on the dark web are becoming cheaper; sellers are working hard to differentiate themselves and their products; and new products are being developed to meet identity thieves' demands, forming a living, breathing economy built to empower even entry-level hackers.

This evolution in tax fraud and tax identity theft is congruent to various dark web economies, including ransomware, as Carbon Black outlined in a 2017 report, further suggesting that attackers are constantly evolving their behaviors to "follow the money." This report highlights some of the offerings available on the robust dark web economy of scale.

ATTACKERS ARE CONSTANTLY EVOLVING THEIR BEHAVIORS TO "FOLLOW THE MONEY."

Carbon Black.

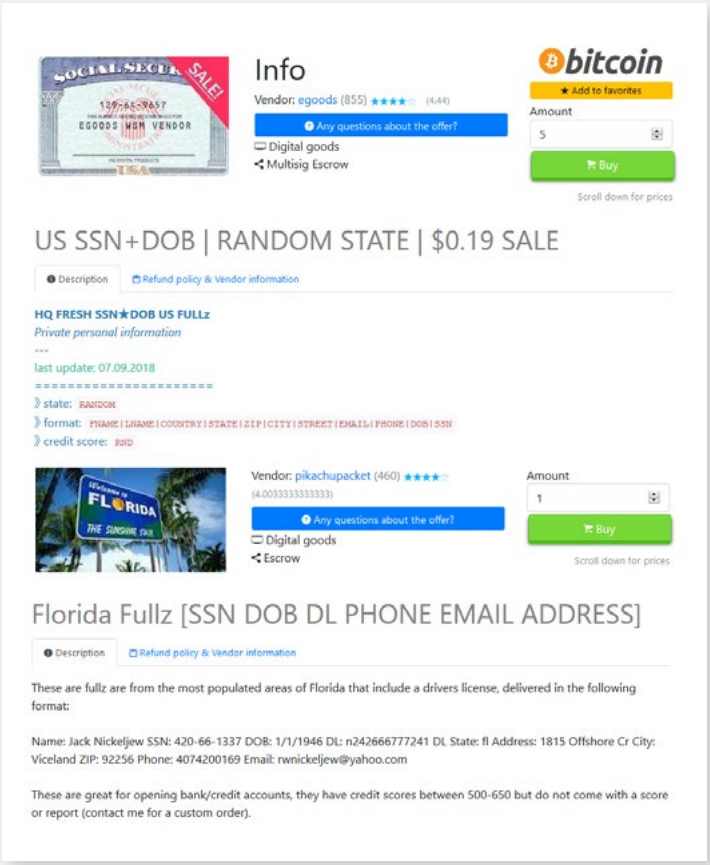
A Deeper Look at Tax Identity Theft

Several dark web marketplaces are currently advertising tax information, all of which are encouraging tax identity theft. Listings include previous years' W-2 forms, form 1040 information and SSNs, among other information, indicating that cyber criminals are not just looking to make a quick buck, but also trying to steal a person's financial future.

More prevalent are listings selling "how-to" guides for cashing out with tax returns. These listings are cheap, some as low as $5, but do not provide any actual tax data. The sellers that offer these listings usually list other similar documentation for credit card fraud and PayPal scams.

Our research found:

12 listings for **U.S. NAME/ SSN/DOB/AND MORE** available by 10 vendors across four dark web markets. Prices ranged from $0.19 to $62.



Carbon Black.

Three vendors were selling **PREVIOUS YEAR TAX FORMS, TO INCLUDE W2S, FORM 1040S AND OTHER FORMS**. Prices ranged from $1.04 to $52. These typically come from hacked accounting firms and enable false tax return filings.

Carbon Black.

TAX DATA (1040-W2) 2015-2016 (TAX RETURN FILES)

Vendor	ar[redacted] (4.83★) (453/6/17) (49/2/2)
Price	Ƀ0.01445 ($52)
Ships to	Worldwide
Ships from	Worldwide
Escrow	Yes

Shipping options

Ƀ0.00 ($0)	1 FILE ($50)	○
Ƀ0.111 ($400)	10 FILES ($450) (-$50 OFF)	○
Ƀ0.236 ($850)	20 FILES ($900) (-$100 OFF)	○
Ƀ0.625 ($2250)	50 FILES ($2,300) (-$200 OFF)	○
Ƀ1.236 ($4450)	100 FILES ($4,500) (-$500 OFF)	○
Ƀ2.5 ($9000)	200 FILES ($9,000) (-$1,000 OFF)	○
Ƀ0.0111 ($40)	1 FILES REQUEST	○

Product description

W2+1040, and bunch other forms for clients,
you get a folder with full tax return files from past year 2016+2015
from MN,WI,CA mostly.

it has all the information needed to fill return,
previous year AGI, etc etc.

here's a full file to see an example of what you will get from this listing
---
https://drive.google.com/open?id=0[redacted]
---
most clients have alot more forms and data than this demo.
price will be $50 each for now, and will go up

for Support & Inquiries
[redacted]@jabb3r.org
ICQ: 7[redacted]

Terms and conditions of a[redacted]

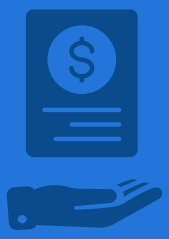
[redacted] on TGF, EVO, AB, Hansa, TR, WallSt and now dream

- I replace dead cards (within 24hours) [card are 100% valid checked before delivery]
- If u disputed before getting back to me don't expect me to replace.
- for RDPs if its died within 12hours ill replace.
- for Fulls, if there's any invalid profiles, ill replace.

You will always be Satisfied and Happy,
You will get what you paid for, because im a Fair guy,
I look after my clients.

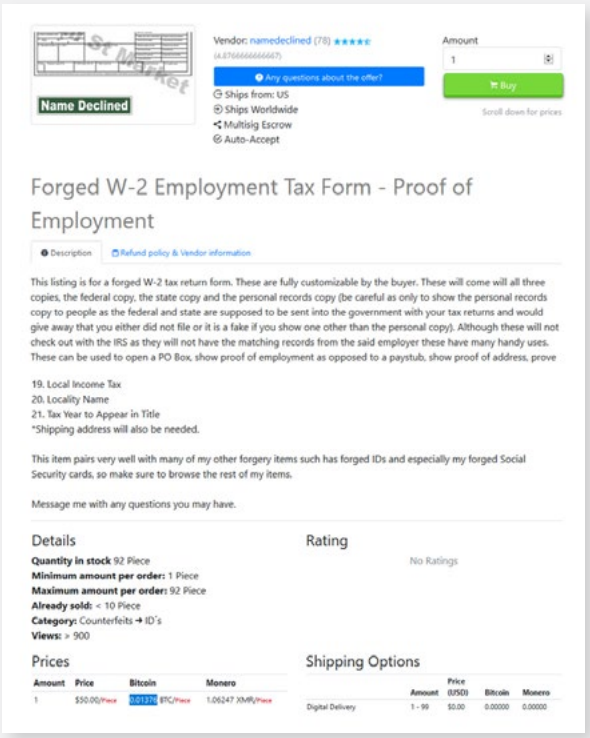
---
for support & Inquiries:
[redacted]@jabb3r.org
ICQ: 7[redacted]

167d ★★★★★ Dang.... you don't know how much of an impact these files will make on my ventures. Friends, at the quality of which these are, the potential profitability you can gain are just insane. I will be $90+ by days end from a $50 buy. PRO this guy is, buy everything.



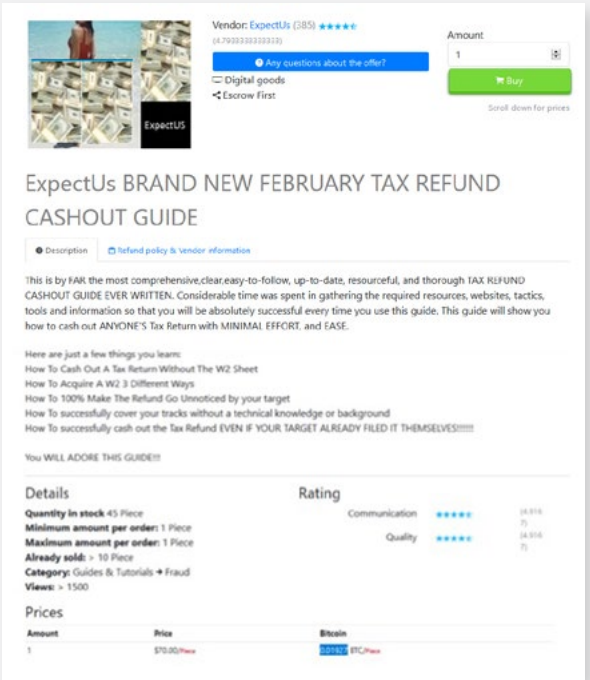
Three offerings for **FORGED W2 FORMS** are as low as $50 but require the buyer to supply all the required information.

Carbon Black.



HOW-TO GUIDES FOR CASHING OUT OTHER PEOPLE'S TAX RETURNS are available for around $5 but one offer, claiming to be the most comprehensive guide for tax refund cash out, was listed for $70.

Carbon Black.



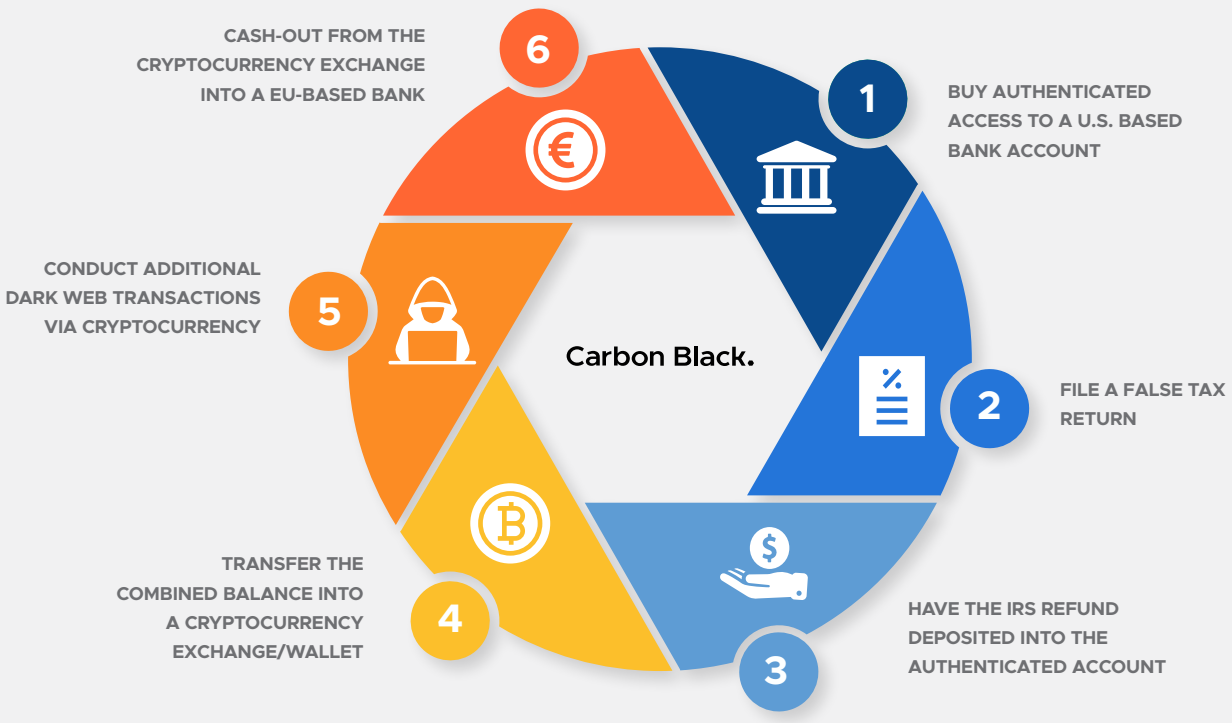
"Full Cycle Tax Fraud"

Tax fraud affects thousands of citizens per year. The theft of a tax return can empower a criminal to steal someone's financial future, not just this year's tax refund. Tax information theft could easily extend to credit cards and home equity loan fraud, which could haunt a victim for decades.

There is a silver lining. With the help of big data and analytics, the IRS identified nearly $10 billion in tax fraud in 2018—about four times higher than 2017—a positive indication that the government's concerted effort to crack down on fraud is creating a higher level of visibility into the problem.

On its website, the IRS outlines its "Dirty Dozen" tax scams, highlighting some techniques well known by security professionals, with phishing topping the list. Also appearing on the list is identity theft, though the role the dark web plays in this theft is glaringly absent.

According to Carbon Black's research, the current dark web economy is such that, for a $1,000 investment, a relatively inexperienced "hacker" can:



Completing this cycle means an attacker can more than double their initial $1,000 investment. The United States tax refund system, when exposed to the ruthless efficiency of dark web marketplaces, has been turned into a Vegas-style slot machine. Insert some bitcoin, pull the handle and figure out how to receive your $2,000 - $3,000 from the U.S. Treasury courtesy of a faceless victim thousands of miles away.

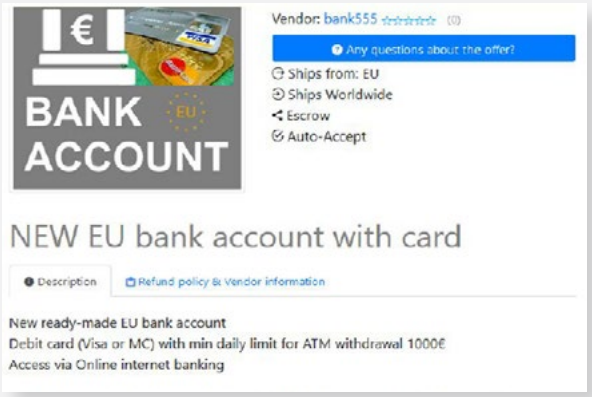
Bank Customer Credentials

There are also a variety of bank customer credential types available on the dark web. Carbon Black's research found 98 listings for bank login information with prices ranging from $1 to $2,080 per account. The most expensive listings were for those that had extremely high balances available to cash out or custom-made bank accounts for anonymizing transactions.

Dark web marketplace banking credentials appear to come in two key flavors:

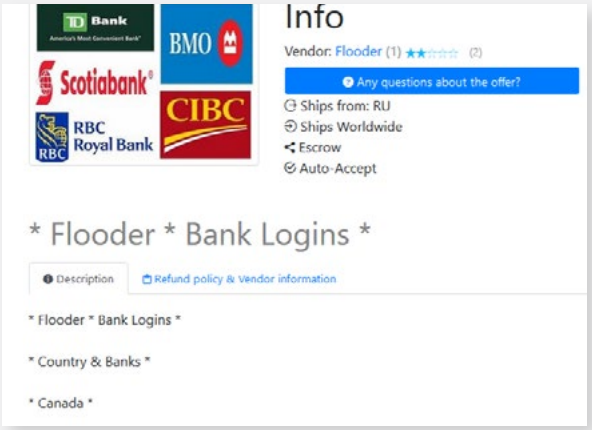
1. FOREIGN BANK ACCOUNTS that will be set up for you (typically in Eastern European countries that are members of the EU).

Carbon Black.



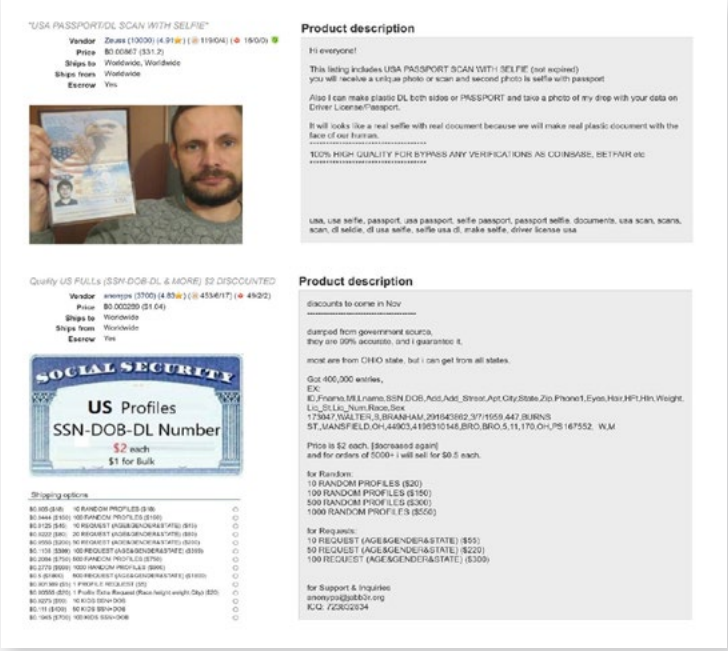
2. "WESTERN" (U.S., CANADA, AUSTRALIA) ACCOUNTS that have been compromised and have cash balances available for transfer.

Carbon Black.



Note: Often, the listings will claim that they are not responsible for security questions or SMS verifications showing that two-factor authentication makes exploiting credentialed access to accounts more difficult.

“Identity Fraud On Demand”



A whole new variety of offerings are becoming more common on the dark web, something we are referring to as “identity fraud on demand.” A hacker can now provide stolen/purchased identity information (Name, DOB, SSN, etc.) and receive an original image of some person holding a forged passport with matching picture/information and scans of the forged identity documents.

This is significant. As 100%-online financial services become available (banking, cryptocurrency exchanges, etc.) these institutions have moved to a form of identity verification where the customer provides an image/photograph of themselves with their driver’s license or passport in the same image (side-by-side face/ID verification, similar to what you experience when going through airport security) and scans of the identity documents. A hacker can now create a completely anonymous financial account by purchasing full validation elements without even exposing their facial likeness/image.

Combining various identity fraud-related resources allows individuals to open U.S.-based online bank accounts with completely falsified data. Many of the online-only banks require scanned copies of documentation and photo verification of the document holder. Having a stolen Social Security Account Number card printed and combining this real information with photo verification model services creates a challenging threat for the banking industry – where an unknown individual can take over a real identity with forged documents and a visual likeness – none of which belong to the swindler.

Financial Industry-Specific Malware

During our search, we also found financial industry-specific malware offerings. Zeus Bot/ZeusNet were the most frequently referenced.

The GozNym 2.0 banking and point-of-sale Trojan was listed for $750 euro and was the most expensive listing. This malware needs to be placed on machines that process financial data: customers, bankers, point-of-sale devices, and call center machines.

Carbon Black.

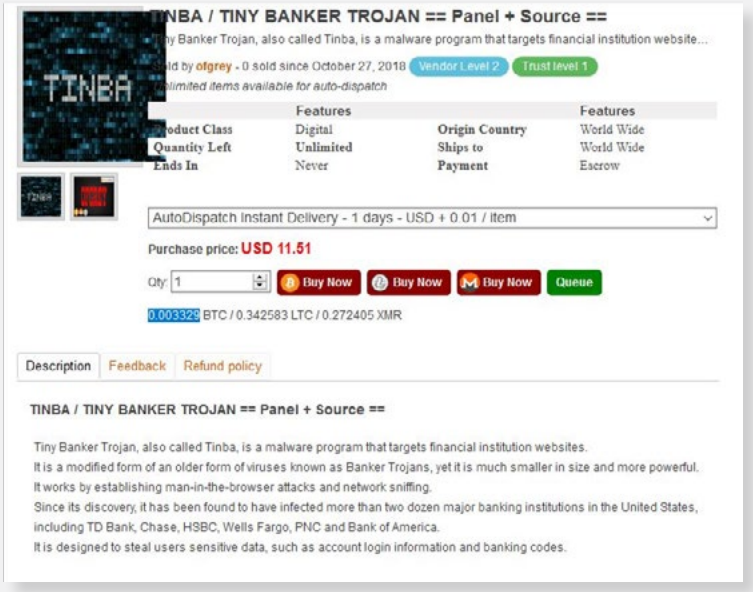
FINANCIAL MALWARE FINDINGS

52 listings for **HOW-TO GUIDES FOR ZEUS BOT**; ranging from $4 - $10

TINY BANKER/TINBA RUNS approximately $11 for the actual binary

Four **GENERICALLY NAMED BANK BRUTEFORCE SOFTWARE** offerings ranging from from $40 - $450

GOZNYM SOURCE CODE is available for 750 euro



Conclusion

From a consumer's perspective, curbing tax fraud and identity theft stemming from the dark web can be a tough, if not impossible, task. In many respects, the onus of responsibility in keeping data safe is on the companies and organizations housing the information.

That said, consumers can take a few critical steps to strengthen their cyber hygiene and decrease their chances of becoming a victim.

1. Make sure to use a bank that offers **MULTI-FACTOR AUTHENTICATION** for logins. It's also a good practice to use Mozilla as your browser for any sensitive online activity.

2. **USE A PASSWORD MANAGER** (locked by a master key that only you know) and do not save passwords in your browser.

3. **FILE YOUR TAXES AS SOON AS POSSIBLE.** In the event someone does get a hold of your information and attempts to file a return in your name, the fraudulent return will be rejected if your return has already been submitted. (Another motivation to get those taxes in early!)

4. **IGNORE THE INCLINATION TO GIVE YOUR INFORMATION AWAY.** If a website doesn't have a legitimate need for personal information, don't provide it. This can help limit future exposure.

5. Never transfer money (via wire, electronic check, credit card, etc.) based off an email request you're not expecting without directly **AUTHENTICATING THE REQUESTOR VIA TELEPHONE OR IN PERSON FIRST.** Putting a lock on (and/or setting notifications for) your credit will also put an additional measure in place to monitor nefarious activity.

About Carbon Black

Carbon Black (NASDAQ: CBLK) is a leader in endpoint security dedicated to keeping the world safe from cyberattacks. The company's big data and analytics platform, the CB Predictive Security Cloud (PSC), consolidates endpoint security and IT operations into an extensible cloud platform that prevents advanced threats, provides actionable insight and enables businesses of all sizes to simplify operations. By analyzing billions of security events per day across the globe, Carbon Black has key insights into attackers' behavior patterns, enabling customers to detect, respond to and stop emerging attacks.

More than 5,000 global customers, including 34 of the Fortune 100, trust Carbon Black to protect their organizations from cyberattacks. The company's partner ecosystem features more than 500 MSSPs, VARs, distributors and technology integrations, as well as many of the world's leading IR firms, who use Carbon Black's technology in more than 500 breach investigations per year.

Carbon Black.

1100 Winter Street
Waltham, MA 02451
P: 617.393.7400
F: 617.393.7499

carbonblack.com