Examining a U.S. Tax Scammer's Web Infrastructure through the DNS Lens

Table of Contents

Executive Report

The 2024 U.S. tax season is well underway, and as usual, scams of all kinds targeting taxpayers and causing the Internal Revenue Service (IRS) problems have cropped up. One such ongoing malicious campaign has explicitly been trailing its sights on small business owners and the self-employed.

Malwarebytes identified three domains as indicators of compromise (IoCs) to date. In a bid to help potential victims avoid the perils the threat can cause, the WhoisXML API research team sought to find all other possible attack vectors aided by our comprehensive DNS intelligence.

Our IoC expansion led to the discovery of these components of the tax scammer's attack infrastructure:

- Nine email-connected domains
- One IP address that turned out to be malicious
- Nine domains that contained a string found among the IoCs

DNS Revelations about the 2024 U.S. Tax Scam IoCs

We began our investigation by looking more closely at the three domains Malwarebytes named as IoCs.

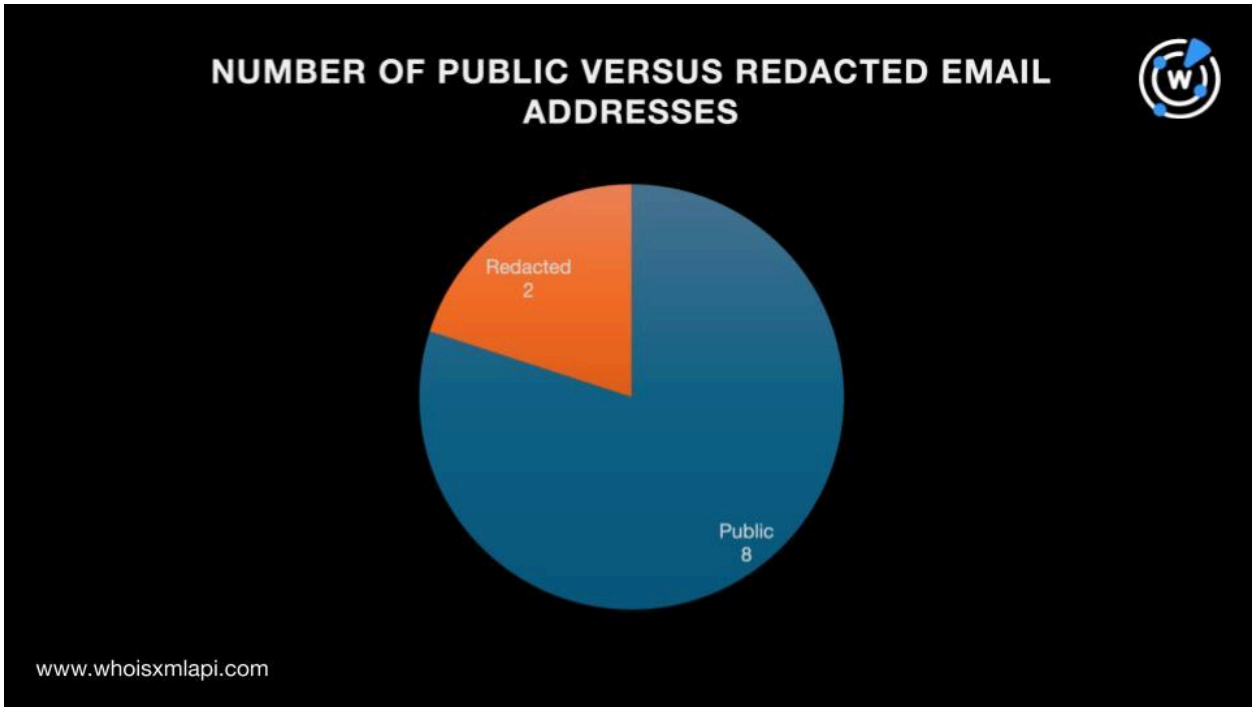
A bulk WHOIS lookup for them revealed that only one domain IoC—irs-ein-gov[.]us—had a current WHOIS record. It was created on 4 March 2024 and registered under Tucows Domains, Inc. in the U.S.

It is also interesting to note that irs-ein-gov[.]us's WHOIS record contained the domain IoC's registrant name, organization, and email address. A search for other domains with the same

registrant details as irs-ein-gov[.]us, however, did not turn up any result, leading us to infer that the name, organization, and email address were specially crafted for this particular scam.

DNS Deep Dive Findings Using the 2024 U.S. Tax Scam IoCs as Jump-Off Points

To know more about the U.S. tax scammer's attack infrastructure, we queried the three domains classified as IoCs on WHOIS History API. The search led to the discovery of 10 email addresses from their historical WHOIS records, eight of which were public.



Next, we used the eight public email addresses as Reverse WHOIS API search terms that provided us with nine email-connected domains after duplicates and the IoCs were filtered out.

While none of them are currently tagged as malicious, two had the text string **esta**, the abbreviation for "Electronic System for Travel Authorization," a document citizens from Visa Waiver Program (VWP) countries who plan to travel to the U.S. for temporary business or pleasure need to have. They could thus serve as vehicles for scams targeting ESTA applicants.

We then subjected the three domains categorized as IoCs to DNS lookups that uncovered one IP address resolution—35[.]206[.]97[.]71.

According to IP Geolocation Lookup, 35[.]206[.]97[.]71 was located in the U.S. under Google LLC's administration. It was also associated with phishing and considered suspicious based on Threat Intelligence Lookup.

A Reverse IP/DNS Lookup query for 35[.]206[.]97[.]71 showed that it is seemingly a shared IP address so we did not use it to analyze IP-connected domains.

As our final step, we looked for other domains that started with the unique strings found among the three domains identified as IoCs using Domains & Subdomains Discovery. Only one string—irs-ein-gov—appeared in other web properties, specifically nine domains.

Are There Signs of Other 2024 U.S. Tax Scams in the DNS?

To check if there were other domains scammers could be using to go after U.S. taxpayers in the DNS, we used two text string combinations closely resembling those used in the featured scam that could easily figure in other tax scams as Domains & Subdomains Discovery search terms, namely:

- Contains **tax + payment + irs**
- Contains **tax + payment + us**

Our search led to the discovery of 135 domains after filtering out duplicates, the IoCs, and the email-connected domains. Apart from the strings **tax**, **payment**, **irs**, and **us**, some of the string-connected domains also contained other strings like **claim**, **info** or **information**, and **refund**, indicating that possible future scams related to tax refunds and claims may emerge.

Threat Intelligence API checks for the 135 string-connected domains revealed that 13 of them were associated with various threats. All of them, in fact, were connected with phishing.

Several cybersecurity companies and even the IRS also warned the public of a new kind of tax scam that just surfaced, which has to do with fake tax preparers. That said, we also scoured the DNS for domains that contained the text string combination **tax + preparer**. Domains & Subdomains Discovery provided us with 1,243 string-connected domains.

Our analysis of the 1,243 domains containing **tax + preparer** also had strings like those shown in the table below, hinting at possible trends.

CATEGORY	TEXT STRINGS	POSSIBLE DOMAIN VISITORS

Education and training	**academy**, **become**, **course**, **education**, **guide**, **howto**, **learning**, **program**, **review**, **school**, **training**, **university**, **workshop**, etc.	People who wish to become or train tax preparers
Tax preparer characteristics	**accredited**, **best**, **certified**, **dope**, **experienced**, **firstclass**, **great**, **irsapproved**, **licensed**, **methodical**, **notyouraverage**, **professional**, **qualified**, **registered**, **super**, **topnotch**, **visionary**, etc.	People in search of tax preparers with specific characteristics
Price	**affordable**, **forless**, **free**, **lowcost**, etc.	People looking for cheap services
Specialization	**audit**, **bitcoin**, **blockchain**, **bond**, **cpa**, **crypto**, **dmv**, **estate**, **federal**, **insurance**, **marketing**, **meta**, **nft**, **notary**, **property**, **retirement**, **smallbusiness**, **uber**, etc.	People on the lookout for tax preparers with special skills or knowledge
Location or nationality	**city**, **domicile**, **latino**, **local**, **national**, **nearme**, specific place names (e.g., **sanfrancisco**, **houston**, **miami**, etc.), **state**, etc.	People who want to avail of services in specific locations or from certain races
Availability	**24**, **asap**, **express**, **live**, **nextday**, **now**, **overnight**, **rapid**, **today**, etc.	People in a hurry to file their taxes
Accessibility	**ai**, **app**, **cloud**, **efile**, **etax**, **internet**, **itax**, **mobile**, **online**, **portal**, **remote**, **site**, **smartphone**, **software**, **tool**, **virtual**, **web**, etc.	People in search of tools to help with tax preparation or preparers without leaving their homes
Directory	**career**, **check**, **connect**, **directory**, **find**, **forum**, **get**, **gig**, **group**, **hire**, **job**, **join**,	People looking for tax preparer lists or wish to be part of such

	link, **list**, **matchmaker**, **network**, **registry**, **service**, **team**, etc.	

—

Our in-depth investigation of the ongoing tax scam targeting individuals and small businesses in the U.S. unveiled several web properties that could be connected to the same infrastructure. We specifically uncovered nine email-connected domains, one malicious IP address, and nine string-connected domains.

We also found that other threat actors or groups may be going after U.S. taxpayers based on the presence of 135 U.S. tax- or IRS-related domains in the DNS, nearly 10% of which are already dubbed as malicious to date.

If you wish to perform a similar investigation or learn more about the products used in this research, please don't hesitate to contact us.

Disclaimer: *We take a cautionary stance toward threat detection and aim to provide relevant information to help protect against potential dangers. Consequently, it is possible that some entities identified as "threats" or "malicious" may eventually be deemed harmless upon further investigation or changes in context. We strongly recommend conducting supplementary investigations to corroborate the information provided herein.*

Appendix: Sample Artifacts

Sample Email-Connected Domains

- application-esta-united-states[.]us
- apply-irs-ein[.]us
- checkautomobilehistory[.]com
- codecanyons[.]xyz
- designtricks[.]xyz

Sample String-Connected Domains

Strings Found among the Domain IoCs

- irs-ein-gov-forms[.]com
- irs-ein-gov-number[.]com
- irs-ein-gov-tax-id[.]com
- irs-ein-gov-taxid[.]com
- irs-ein-gov[.]agency

Strings Used for U.S. Tax Payment Scams

- aspenholidayunitytaxicabpaymentsystem[.]us
- aus-taxpayments[.]info
- austaxpayment[.]info
- businesstaxpayment[.]com
- co-jackson-ms-taxpayments[.]us
- coronavirus-tax-relief-and-economic-impact-payments[.]com
- coronavirus-tax-relief-and-economic-impact-payments[.]online
- cryptoirstaxpayment[.]com
- cryptoirstaxpayment[.]us
- etaxpayment[.]us
- firstdownpaymenthomebuyertaxcredit[.]com
- firstdownpaymenthomebuyertaxcredit[.]org
- firstdownpaymenttaxcredit[.]com
- firstdownpaymenttaxcredit[.]org
- furusato-tax-payment[.]com
- furusato-taxpayment[.]com
- furusato-taxpayment[.]info
- furusatotaxpayment[.]com
- housepaymentcalculatorwithtaxes[.]com
- hurusato-tax-payment[.]com
- hurusato-taxpayment[.]com
- incometaxpayment[.]us
- incometaxpayments[.]us
- irs-claim-taxpayment[.]com
- irs-claimtaxpayment-homeonline[.]com
- irs-finance-tax-payment[.]com
- irs-financial-claimpaymenttax[.]com
- irs-financial-taxus-payments[.]com
- irs-government-tax-payment[.]com
- irs-government-tax-payments[.]com
- irs-page-tax-payment[.]com
- irs-page-tax-payments[.]com
- irs-payment-refund-tax[.]com
- irs-payment-tax-financial[.]com
- irs-payment-tax-relief[.]com
- irs-payment-tax[.]com
- irs-payment-taxfinancial[.]com
- irs-payment-taxrefund[.]com
- irs-paymentonline[.]tax
- irs-payments-tax[.]com
- irs-profil-tax-payment[.]com
- irs-profile-get-taxpayment[.]com
- irs-profiletax-getpayment-information[.]com
- irs-return-payment-tax[.]com
- irs-service-tax-payment[.]com
- irs-tax-claim-payment[.]com
- irs-tax-claim-payments[.]com
- irs-tax-claimpayment[.]com
- irs-tax-financial-payment[.]com
- irs-tax-government-payment[.]com

Strings Related to Tax Preparers

- 1040eztaxpreparer[.]com
- 1040taxpreparer[.]com
- 1040taxpreparer[.]net
- 1040taxpreparerbond[.]com
- 1040taxpreparerbonds[.]com
- 247taxpreparer[.]com
- 4ataxpreparer[.]com
- 911fortaxpreparers[.]fm
- a1tax-preparers[.]com
- a1tax-preparers[.]net
- a1taxpreparer[.]com
- abqtax-preparers[.]com

- abqtax-preparers[.]net
- accreditedtaxpreparer[.]com
- accreditedtaxpreparerhealdsburg[.]com
- acetaxespreparers[.]com
- acetaxpreparers[.]com
- actaxpreparer[.]com
- adepttaxpreparer[.]com
- adrianavlad-taxpreparer[.]com
- advicefortaxpreparers[.]com
- affordabletaxpreparers[.]com
- agoodtaxpreparer[.]com
- aitaxpreparer[.]com
- aitaxpreparer[.]net
- aitaxpreparer[.]org
- aitaxpreparers[.]com
- albanytaxpreparer[.]com
- albasnytaxpreparer[.]com
- albuquerquetaxpreparer[.]com
- alcantarataxpreparer[.]com
- allucastaxpreparerservices[.]com
- allucastaxpreparerservicesllc[.]info
- americantaxpreparers[.]com
- americasbesttaxpreparers[.]com
- americastaxpreparer[.]biz
- americastaxpreparer[.]com
- americastaxpreparer[.]info
- americastaxpreparer[.]net
- americastaxpreparer[.]org
- americastaxpreparers[.]com
- americataxpreparers[.]com
- annapolistaxpreparer[.]com
- aranotaryandtaxpreparer[.]com
- aranotaryandtaxpreparerfl[.]com
- aranotarytaxpreparer[.]com
- aranotarytaxpreparer[.]org
- arcadiataxpreparer[.]com
- arcadiataxpreparer[.]ws
- arizonataxpreparer[.]com
- arizonataxpreparereando[.]com
- arlingtontaxpreparer[.]com
- arlingtontxtaxpreparers[.]com
- artaxpreparer[.]com
- asaptaxpreparer[.]com
- askataxpreparer[.]com
- askmytaxpreparer[.]com
- ataxpreparer[.]com
- ataxpreparer[.]ws
- atlantataxpreparer[.]com
- atlastaxpreparers[.]com
- atotaxpreparer[.]com
- austelltaxpreparers[.]com
- austintaxpreparer[.]com
- austintaxpreparer[.]net
- authorized-tax-return-preparer[.]com
- authorized-tax-return-preparer[.]org
- authorizedtaxpreparer[.]org
- awptaxpreparer[.]com
- azbtaxpreparer[.]com
- aztaxpreparer[.]com
- aztaxpreparers[.]com
- bakersfieldtaxpreparer[.]com
- baltimoretaxpreparer[.]com
- baptaxpreparer[.]com
- bayareataxreturnpreparers[.]com
- beataxpreparer[.]com
- becomeataxpreparer[.]com
- becomeataxpreparer[.]net
- becomeataxpreparer[.]org
- becomeataxpreparerfree[.]com
- becomeataxpreparerfree[.]net
- becomeataxpreparerfree[.]org
- becometaxpreparer[.]com
- becometaxpreparer[.]net
- becometaxpreparer[.]org
- benjamintaxpreparer[.]com
- bestcpataxpreparer[.]com
- bestcpataxpreparer[.]nom[.]za
- bestincometaxpreparer[.]com
- bestlocaltaxpreparer[.]com

- bestlocaltaxpreparer[.]org
- bestlocaltaxpreparers[.]com
- bestlocaltaxpreparers[.]org
- bestlocaltaxpreparers[.]ph
- bestratedlocaltaxpreparers[.]com
- bestratedtaxpreparers[.]com
- besttaxpreparer[.]com
- besttaxpreparer[.]net
- besttaxpreparercpa[.]com