Tempering Tax Season Troubles with DNS Intel

Table of Contents

Executive Report

Each year, threat actors zoom in on U.S. taxpayers in a bid to intercept their payments and line their pockets instead. And while the tax day—15 April 2025—has passed, those who need more time can settle their dues up to 15 October 2025 without getting penalized if they requested an extension.

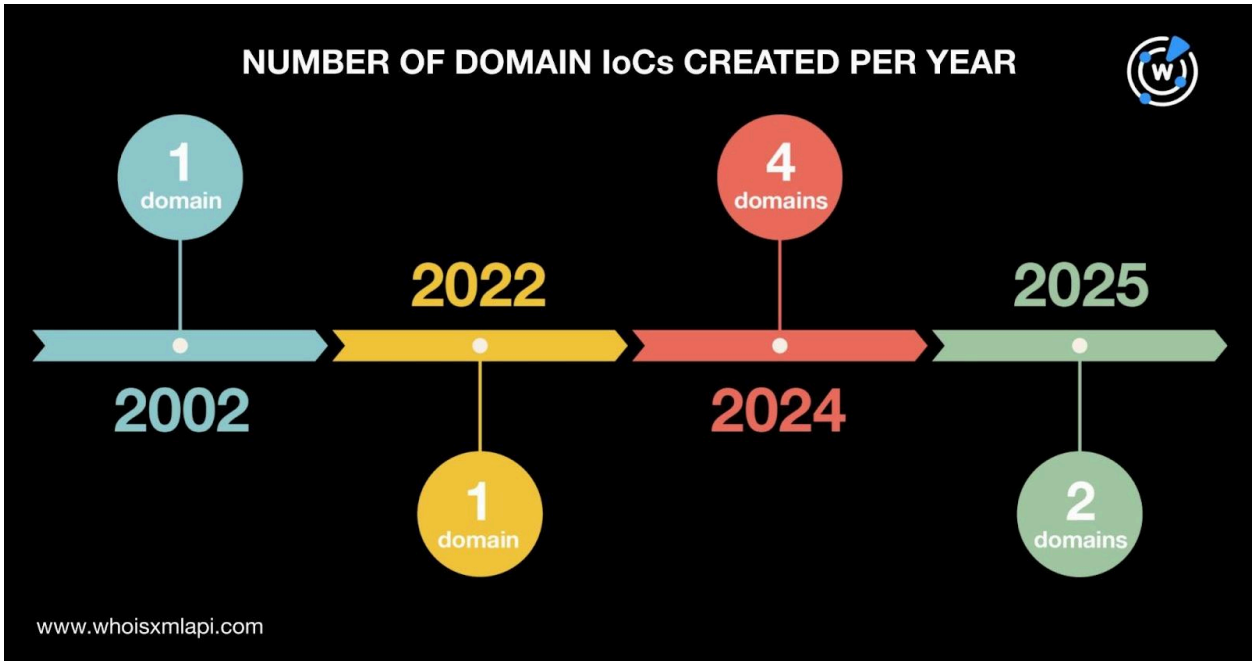
That said, ongoing tax-themed phishing campaigns may affect those who have not yet filed their tax returns. Microsoft cybersecurity researchers identified 11 domains and one IP address as indicators of compromise (IoCs) related to one such campaign. WhoisXML API expanded the current IoC list and uncovered potentially connected artifacts, namely:

- Two alleged victim IP records, obtained from the Internet Abuse Signal Collective (IASC) tied to one Autonomous System number (ASN)
- 153 email-connected domains, one of which turned out to be malicious
- 13 additional IP addresses, 11 of which have already figured in malicious campaigns
- Two IP-connected domains
- 197 string-connected domains

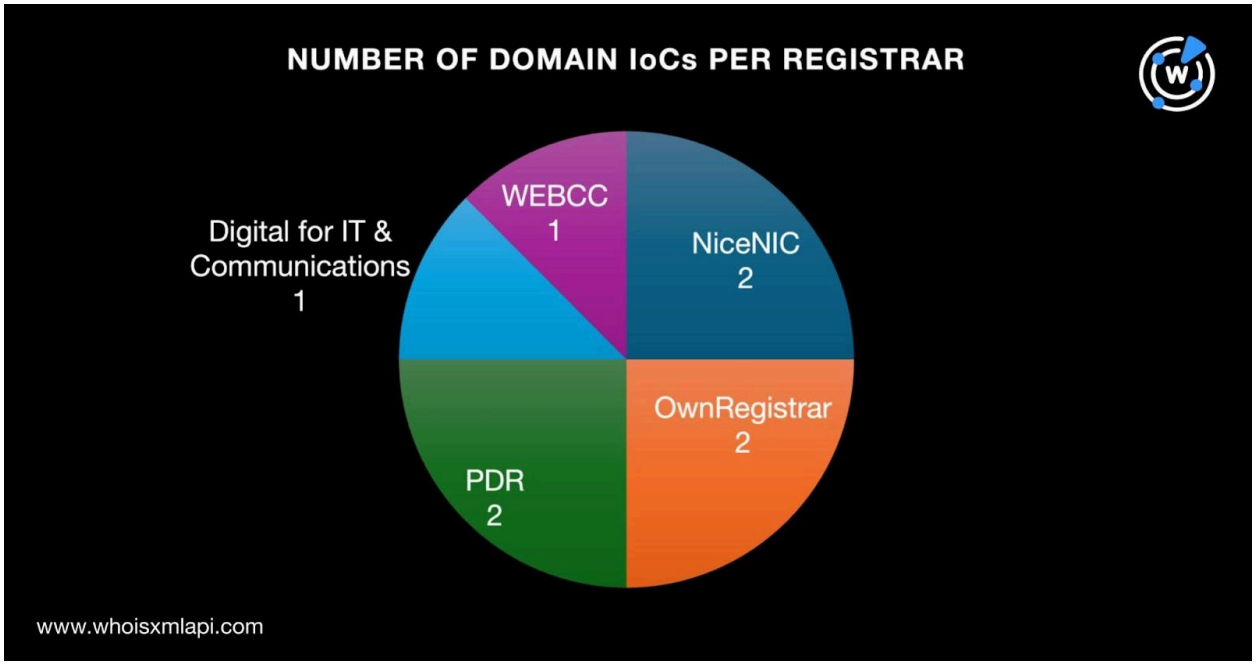
A Closer Look at the Tax-Themed Threat IoCs

We started our in-depth analysis of the 2025 tax-themed threat by looking further into the current list of IoCs. First, we queried the 11 domains on Bulk WHOIS API and discovered that eight of them had current WHOIS records. We also found that:

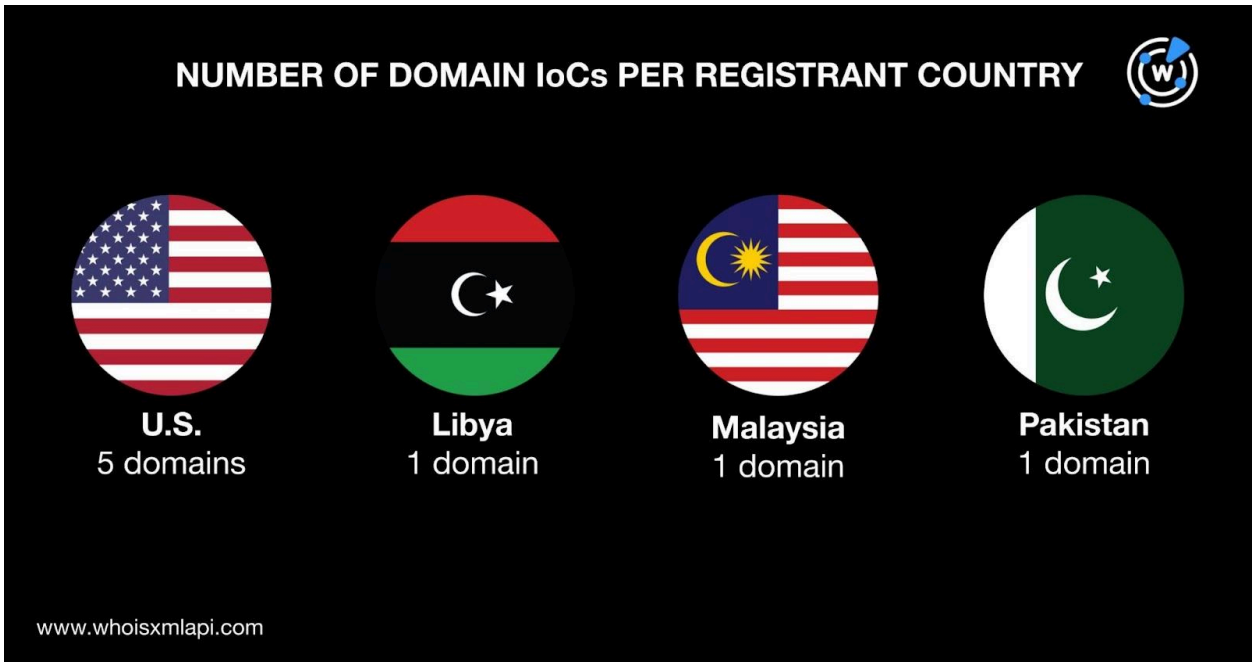
- The eight domains identified as IoCs were created between 2002 and 2025. Specifically, one domain each was created in 2002 and 2022, four were created in 2024, and two were created in 2025.



- They were administered by five different registrars led by NiceNIC, OwnRegistrar, and PDR, which accounted for two domains each. One domain each was administered by Digital for IT & Communications and WEBCC.



- They were registered in four different countries led by the U.S., which accounted for five domains. One domain each was registered in Libya, Malaysia, and Pakistan.



A DNS Chronicle API for the 11 domains tagged as IoCs revealed that eight recorded 273 domain-to-IP resolutions over time. The IoC historyofpia[.]com posted the oldest resolution date—7 February 2017. Take a look at historical DNS details for three other domains below.

DOMAIN IoC	NUMBER OF RESOLUTIONS	FIRST RESOLUTION DATE
acusense[.]ae	15	26 February 2024
muuxxu[.]com	4	10 December 2024
proliforetka[.]com	14	31 January 2025

Next, we queried the sole IP address identified as an IoC on IP Geolocation API and found that it was geolocated in Colombia and administered by Telmex Colombia.

A DNS Chronicle API query for the IP address tagged as an IoC, however did not turn up any result.

In addition, using sample netflow data our researchers obtained from the IASC, we further analyzed 181[.]49[.]105[.]59, which served as a command-and-control (C&C) IP address related to the threat we analyzed. The sample data revealed two alleged victim IP records, both of

which could be associated with the same ISP Energy Group Networks operating under ASN 18779 according to an additional IP Geolocation API query.

Tax-Themed Threat IoC List Expansion Analysis Findings

After knowing more about the IoCs, we searched for their DNS breadcrumbs.

We kicked off our deep dive by querying the 11 domains identified as IoCs on WHOIS History API. The results showed that seven of them had 17 email addresses in their historical WHOIS records. Eight of the 17 email addresses were public.

A Reverse WHOIS API query for the eight public email addresses revealed that while they did not appear in current WHOIS records, they all appeared in historical records. However, two of these email addresses were excluded from further analysis as they were associated with a high number of connected domains, potentially indicating domaining activities unrelated to the threat we analyzed. In sum, the six public email addresses left on our list led to the discovery of 153 email-connected domains after duplicates and those already tagged as IoCs were filtered out.

We then queried the 153 email-connected domains on Threat Intelligence API and found that one of them—0913u[.]com—has already been classified as a generic threat source.

Next, a DNS Lookup API query for the 11 domains identified as IoCs revealed that six of them had active IP resolutions. In particular, the six domains resolved to 13 unique additional IP addresses, none of which matched the known IP address tagged as an IoC.

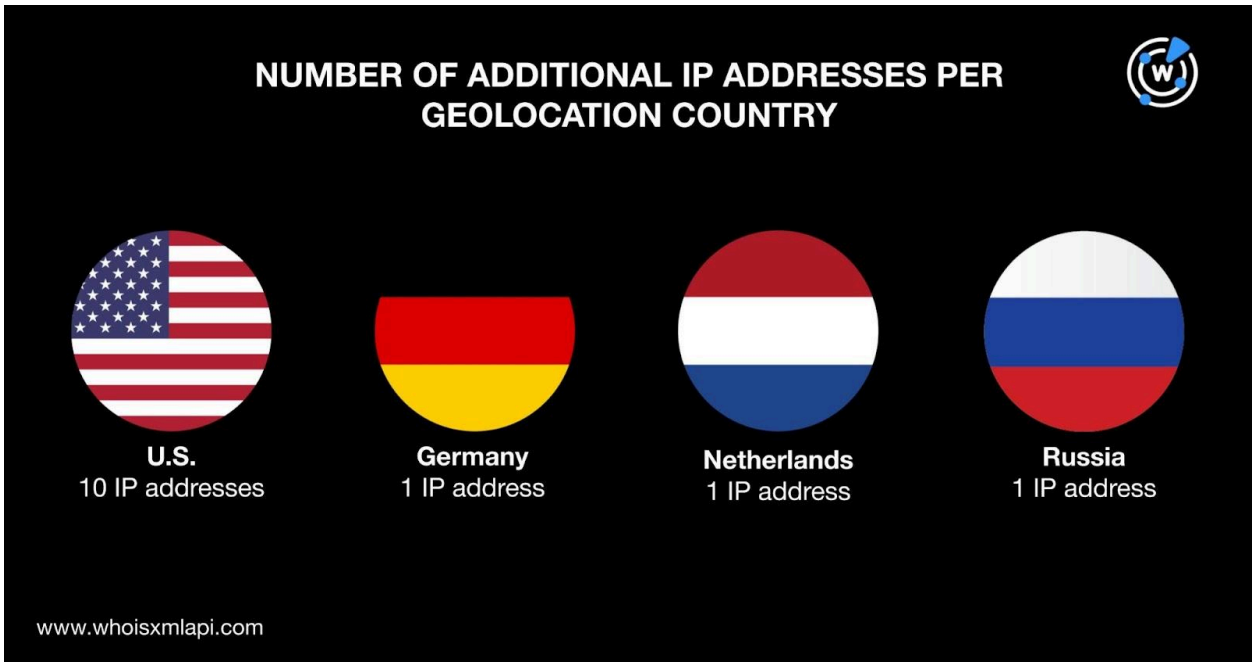
We queried the 13 additional IP addresses on Threat Intelligence API and found that 11 have already been weaponized for various cyber attacks. Take a look at five examples below.

MALICIOUS ADDITIONAL IP ADDRESS	ASSOCIATED THREATS
104[.]21[.]16[.]1	Attack Command and control (C&C) Generic threat Malware distribution Phishing Spamming Suspicious activity
104[.]21[.]48[.]1	Attack C&C

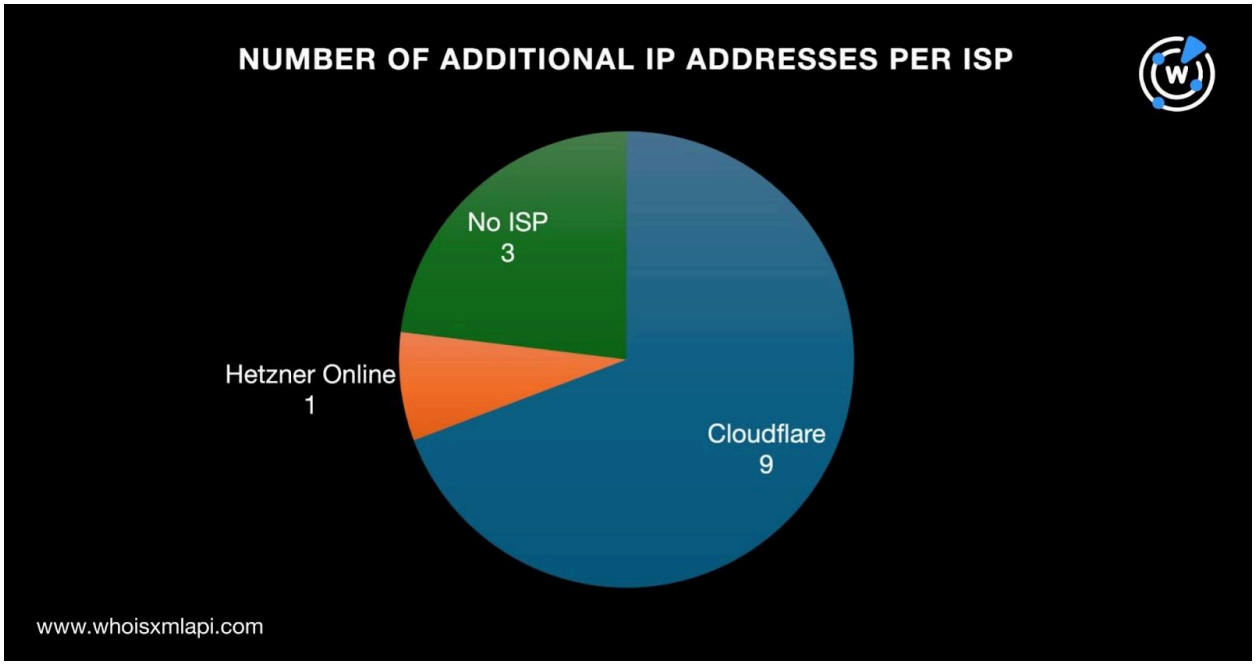
	Generic threat Malware distribution Phishing Spamming Suspicious activity
104[.]21[.]96[.]1	Attack C&C Generic threat Malware distribution Phishing Spamming Suspicious activity
87[.]251[.]67[.]203	C&C
94[.]232[.]40[.]48	C&C

A Bulk IP Geolocation Lookup query for the 13 additional IP addresses revealed that:

- They were geolocated in four different countries led by the U.S., which accounted for 10 IP addresses. One IP address each was geolocated in Germany, the Netherlands, and Russia.



- While three IP addresses did not have ISPs on record, nine were administered by Cloudflare. One IP address was administered by Hetzner Online.



We now had 14 IP addresses for further analysis—one tagged as an IoC and 13 additional from our DNS Lookup API query earlier. A Reverse IP API query for the 14 IP addresses revealed that 13 had current domain resolutions. A closer look showed that two IP addresses could be dedicated. Together, they hosted two IP-connected domains after duplicates, those already identified as IoCs, and the email-connected domains were filtered out. Interestingly, these two new domains—www[.]cronoze[.]com and www[.]muuxxu[.]com—were actually subdomains of two of the IoCs under study.

To cap off our investigation, we used the 11 text strings found in the 11 domains tagged as IoCs as search terms on Domains & Subdomains Discovery. These five strings appeared at the start of other domains:

- acusense.
- ebrand.
- historyofpia.
- nlxtg.
- porelinofigoventa.

In particular, the five text strings above led to the discovery of 197 string-connected domains after duplicates, those already identified as IoCs, and the email- and IP-connected domains were filtered out.

—

Our expansion analysis of the 12 IoCs related to the tax-themed phishing campaigns allowed us to uncover two alleged victim IP records and 365 connected artifacts comprising 153 email-connected domains, 13 additional IP addresses, two IP-connected domains, and 197 string-connected domains. In addition, 12 of the connected artifacts have already figured in various cyber attacks.

Download a sample of the threat research materials now or contact sales to discuss your intelligence needs for threat detection and response or other cybersecurity use cases.

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

- 01[.]ly
- 029nanya[.]com
- 0913e[.]com
- ad-teleskies[.]net
- afaqexpo[.]com
- afaqexpo[.]net
- ccxxxh[.]com
- checkin[.]ly
- chooran[.]net
- dalisg[.]com
- demos[.]ly
- digital[.]ly
- e-guolu[.]com
- eventon[.]ly
- eventsin[.]ly
- fastfood[.]ly
- firstco-ly[.]com
- fishing[.]ly
- hczxjz[.]com
- hlhssly[.]com
- hsslsl[.]com
- ibrand[.]ly
- ilibya[.]ly
- ilibya[.]tv
- libya-host[.]net
- libya-host1[.]net
- libyaelections[.]ly
- maab[.]com[.]ly
- maairways[.]com
- maairways[.]net
- nserver[.]ly
- nsyzx[.]com
- obtain[.]ly
- oil[.]ly
- pakavn[.]com
- pchjsy[.]com
- pencycleuk[.]com
- qdyqsb[.]com
- rentals[.]ly
- rundazhuangshi[.]com
- shanxidjqz[.]com
- skyline[.]ly
- slslc[.]cn
- taxdgs[.]com
- tdexlibya[.]com
- teleskies[.]com
- vitrina[.]ly
- vr[.]ly
- vtour[.]ly
- whystrong[.]com
- wingstours[.]com
- wnadc[.]com
- xadlbyq[.]com
- xbddcw[.]com
- xfzybz[.]com
- ysfkq[.]com
- yuzhing[.]com

Sample Additional IP Addresses

- 104[.]21[.]112[.]1
- 104[.]21[.]16[.]1
- 104[.]21[.]32[.]1
- 87[.]251[.]67[.]203
- 94[.]232[.]40[.]48

Sample IP-Connected Domain

- www[.]cronoze[.]com

Sample String-Connected Domains

- acusense[.]ai
- acusense[.]ca
- acusense[.]cn
- ebrand[.]ae
- ebrand[.]ag
- ebrand[.]agency
- historyofpia[.]net
- nlxtg[.]cn
- nlxtg[.]tk
- porelinofigoventa[.]ph
- porelinofigoventa[.]ws