Thumbing through the DNS Traces of TamperedChef

Table of Contents

1. Executive Report
2. Appendix: Sample Artifacts

Executive Report

The Acronis Threat Research Unit (TRU) recently discovered a massive malvertising campaign leveraging apps users commonly install on their computers. Dubbed “TamperedChef,” users were tricked into downloading malicious scripts via clever social engineering ruses. The scripts automatically executed their payloads that resulted in nefarious actions, including establishing and selling remote access for profit, stealing and monetizing sensitive credentials and healthcare data, preparing compromised systems for future ransomware deployment, and engaging in opportunistic espionage by exploiting access to high-value targets.

The researchers identified 58 IoCs comprising URLs and subdomains. We extracted 58 unique domains from the IoCs and weeded out those that were legitimate with the help of the WhoisXML API MCP Server. This step left us with 46 domains for further analysis. Our in-depth investigation led to these discoveries:

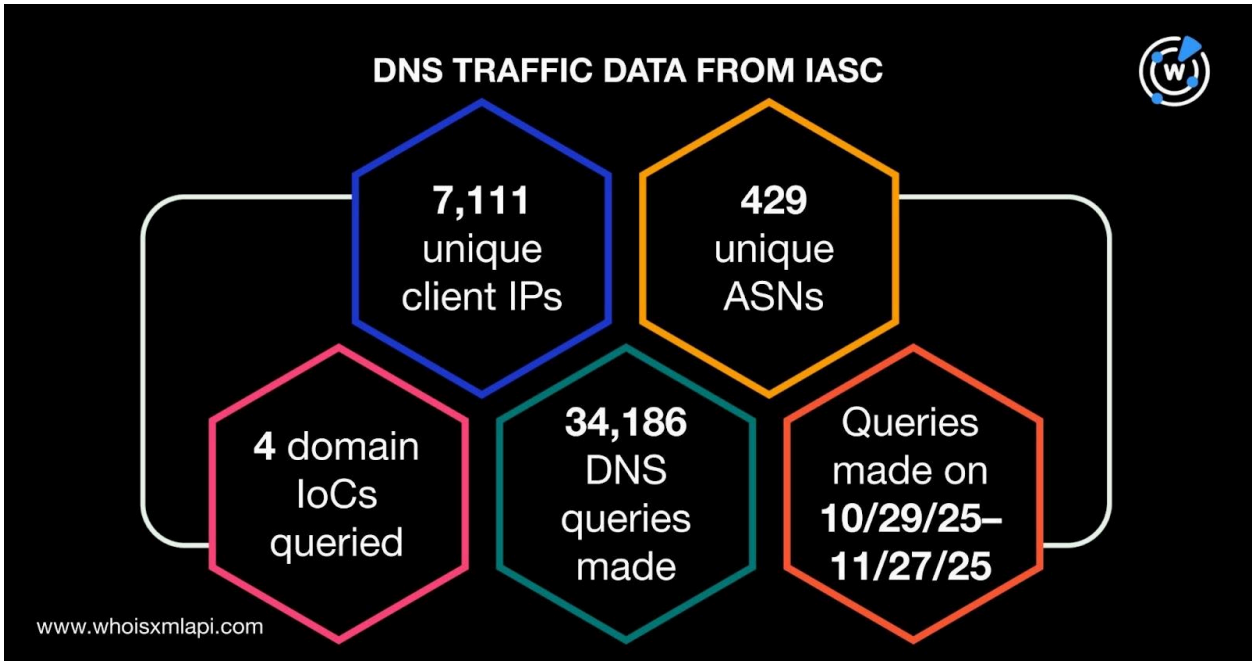
- 28 domains tagged as IoCs deemed likely to turn malicious 155–335 days before being dubbed as such
- 7,111 unique client IP addresses queried four domains identified as IoCs based on sample IASC network traffic data
- 97 email-connected domains
- 24 IP addresses, 10 were malicious
- 952 IP-connected domains
- Five string-connected domains

A Closer Look at the IoCs

We began our foray deep into the DNS by querying the 46 domains identified as IoCs on First Watch Malicious Domains Data Feed. We discovered that 28 of them were deemed likely to turn malicious upon registration, that is, between 155 and 335 days before they were dubbed as IoCs on 19 November 2025. Take a look at more details below.

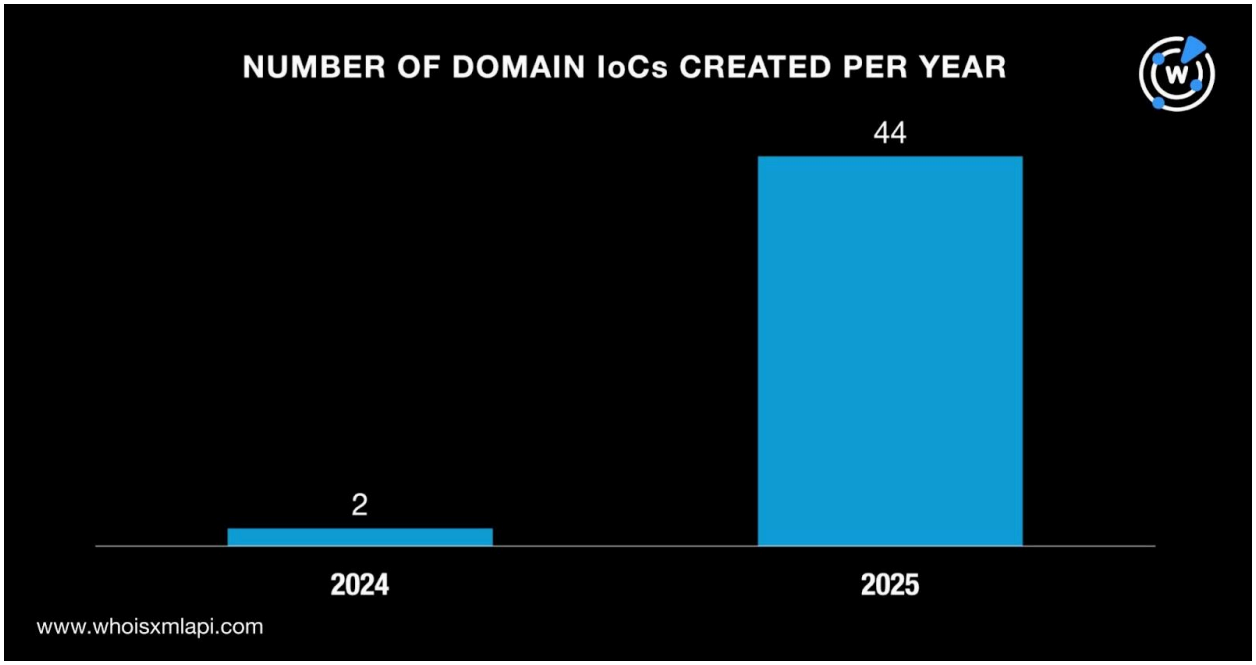
DOMAIN IoC	FIRST WATCH DATE	NUMBER OF DAYS PRIOR TO REPORT DATE
opfktvbbb0d5pphzlc[.]com	19 December 2024	335
effortlesspdf[.]com	15 January 2025	308
k2ioeasm874fnacr9x[.]com	24 January 2025	299
meg7xqos0m7h9urhr0[.]com	24 January 2025	299
85etpt40zf7ht4yd1u[.]com	27 January 2025	296

In addition, sample network traffic data from the IASC revealed that 7,111 unique client IP addresses under 429 distinct ASNs communicated with four of the domains tagged as IoCs. Altogether, they made 34,186 DNS queries between 29 October and 27 November 2025.



Next, we queried the 46 domains identified as IoCs on WHOIS API. We found out that:

- They were all fairly newly created, between 20 November 2024 and 6 September 2025 to be exact.



- All of them were administered by Namecheap.
- All of them were registered in Iceland.

A DNS Chronicle API query, meanwhile, for the 46 domains tagged as IoCs showed that 24 had historical domain-to-IP resolutions. The domains resolved to 438 IP addresses over time. These resolutions were recorded as far back as 5 February 2017 specifically by getallmanuals[.]com.

Interestingly, getallmanuals[.]com was created on 15 January 2025 according to its current WHOIS record but resolved to 184[.]168[.]221[.]38 as early as 15 January 2025. That could mean that getallmanuals[.]com's domain registration expired and it was picked up again recently potentially by the actors behind TamperedChef. Here are more details about five other domains tagged as IoCs.

DOMAIN IoC	NUMBER OF RESOLUTIONS	FIRST RESOLUTION DATE	LAST RESOLUTION DATE
usermanualsonline[.]com	24	11 December 2024	30 September 2025
effortlesspdf[.]com	20	16 January 2025	20 November 2025
getmanualviewer[.]com	16	17 January 2025	28 October 2025
k2ioeasm874fnacr9x[.]com	1	27 January 2025	27 January 2025
85etpt40zf7ht4yd1u[.]com	2	28 January 2025	29 January 2025

The Hunt for New Artifacts

We started our search for new artifacts by querying the 46 domains identified as IoCs on WHOIS History API. All of them had email addresses in their historical WHOIS records. Specifically, they had 54 unique email addresses in their records. Further scrutiny revealed that four were public email addresses.

Next, we queried the four public email addresses on Reverse WHOIS API. While none of them appeared in any domain's current WHOIS records, all did so in historical records. This step led to the discovery of 97 email-connected domains after duplicates and those already tagged as IoCs were filtered out.

Afterward, we queried the 46 domains identified as IoCs on DNS Lookup API, which revealed that 14 of them had active IP resolutions. All in all, the 14 domains resolved to 24 unique IP addresses.

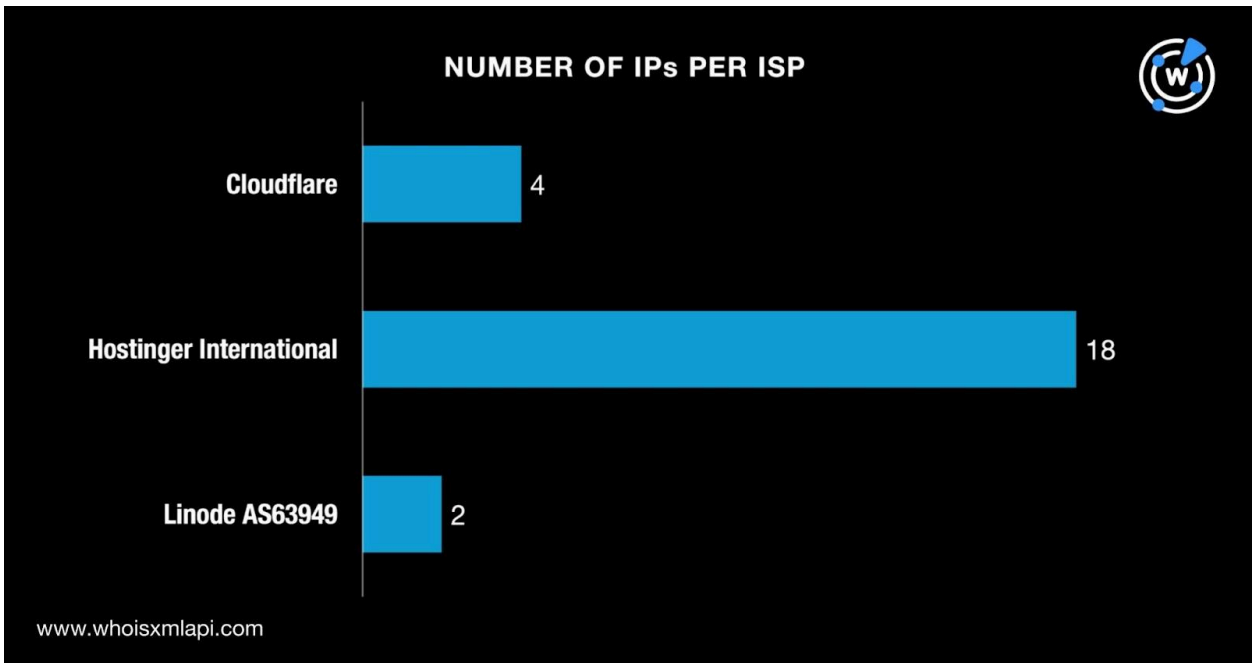
A Threat Intelligence API query for the 24 IP addresses showed that 10 of them have already been weaponized for nefarious campaigns. Take a look at five examples below.

MALICIOUS IP ADDRESS	ASSOCIATED THREAT	DATE FIRST SEEN	DATE LAST SEEN
84[.]32[.]84[.]190	Phishing Malware distribution Generic threat Suspicious activity	14 June 2023 1 December 2023 8 September 2023 8 March 2024	21 November 2025 17 November 2025 13 October 2025 1 October 2025
84[.]32[.]84[.]194	Malware distribution Suspicious activity	15 October 2023 15 September 2023	21 November 2025 11 November 2025

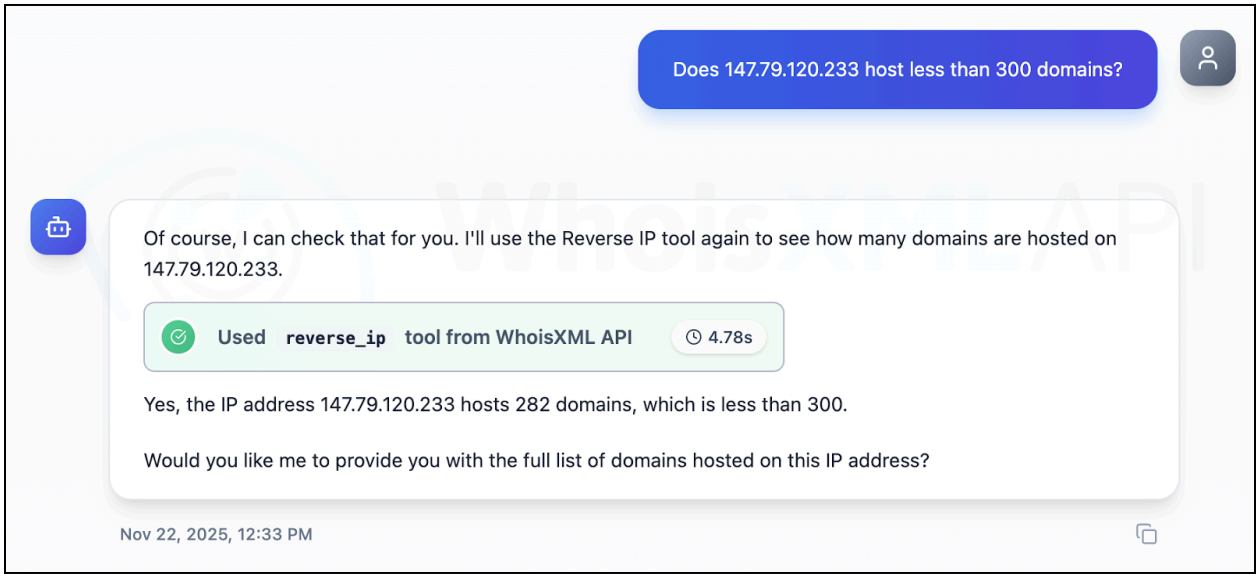
	Phishing Generic threat	19 July 2023 18 January 2024	15 October 2025 12 October 2025
104[.]21[.]91[.]64	Phishing Malware distribution Generic threat	19 May 2023 31 March 2023 17 June 2023	21 November 2025 20 November 2025 17 October 2025
104[.]21[.]95[.]128	Phishing Generic threat Malware distribution	9 July 2023 10 July 2023 30 March 2023	21 November 2025 16 November 2025 5 October 2025
172[.]67[.]144[.]246	Phishing Generic threat Malware distribution	9 July 2023 10 July 2023 30 March 2023	21 November 2025 16 November 2025 5 October 2025

Next, we queried the 24 IP addresses on Bulk IP Geolocation Lookup and discovered that:

- They were all geolocated in the U.S.
- They were administered by three ISPs, namely, Hostinger International (18 IP addresses), Cloudflare (four IPs), and Linode AS63949 (two IPs).



Reverse IP API queries for the 24 IP addresses, meanwhile, via Jake AI showed that six of them could be dedicated hosts. We used the prompt “Does (IP) host less than 300 domains?” for each IP address.



Sample Jake AI query result

Altogether, the six dedicated IP addresses hosted 952 IP-connected domains after filtering out duplicates, those already identified as IoCs, and the email-connected domains.

Afterward, we subjected the 46 domains tagged as IoCs to closer scrutiny and extracted 46 unique text strings. We queried the 46 strings on Domains & Subdomains Discovery and found out that these three appeared at the start of other domains:

- k2ioeasm874fnacr9x.
- pyej17uw09d1bqlndg.
- usermanualsonline.

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

—

Our in-depth analysis of TamperedChef revealed that 28 of the 46 domains identified as IoCs were deemed likely to turn malicious between 155 and 335 days before they were dubbed as IoCs. We also uncovered 1,078 new artifacts comprising 97 email-connected domains, 24 IP addresses, 952 IP-connected domains, and five string-connected domains. Notably, 10 of the new artifacts have already figured in various attacks.

If you wish to 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

- 0-99[.]com
- 10inc[.]com
- 10zm[.]com
- advertisedoffer[.]com
- allgal[.]com
- alltypeloans[.]com
- b-i-t-c-o-i-n[.]com
- bettamart[.]com
- bitcoinoid[.]com
- chinesebarter[.]com
- chineseherbguide[.]com
- chineseoriental[.]com
- democratise[.]com
- dezignformat[.]com
- econocrat[.]com
- econocrats[.]com
- eternalplan[.]com
- finecities[.]com
- finecity[.]com
- flavoringherbs[.]com
- gamesconventionasia[.]com
- graphiv-lab[.]com
- graphiv[.]com
- heliciculture[.]com
- heliculture[.]com
- helpingsupport[.]com
- jobshiok[.]com
- jpass88[.]com
- kaypoh[.]com
- l-i-f-i[.]com
- leedoubleukay[.]com
- leewk[.]com
- malaysianmalaysia[.]com
- malaysianonline[.]com
- mediashiok[.]com
- newzealandcity[.]com
- niftybucks[.]com
- noloanshark[.]com
- offerltd[.]com
- polymorphousmarketing[.]com
- popclassic[.]com
- privateexclusive[.]com
- quickhour[.]com
- realtyadvertisement[.]com
- realtyadvertisements[.]com
- sg10[.]com
- sg25[.]com
- sgcitizen[.]com
- towkay[.]com
- traumatise[.]com
- underwearsecrets[.]com
- vendfood[.]com
- vertised[.]com
- vertiser[.]com
- westmalaysia[.]com
- ys25[.]com
- yuanreminbi[.]com
- zg00[.]com
- zg21[.]com
- zo00[.]com

Sample IP Addresses

- 104[.]21[.]91[.]64
- 104[.]21[.]95[.]128
- 147[.]79[.]120[.]116
- 147[.]79[.]120[.]233
- 147[.]79[.]120[.]30
- 148[.]135[.]128[.]127

- 148[.]135[.]128[.]36
- 172[.]234[.]24[.]211
- 172[.]239[.]57[.]117
- 172[.]67[.]144[.]246
- 46[.]202[.]183[.]132
- 46[.]202[.]183[.]75
- 77[.]37[.]76[.]163
- 77[.]37[.]76[.]212
- 77[.]37[.]76[.]43
- 84[.]32[.]84[.]190
- 84[.]32[.]84[.]194
- 92[.]112[.]198[.]67
- 92[.]112[.]198[.]70

Sample IP-Connected Domains

- 0vxe[.]com
- 1090ce78-a573-43df-908b-4bc549764a3a[.]random[.]dolar777slot[.]info[.]cdn[.]hstgr[.]net
- 1487eccc-1fc4-4957-adb6-2a5a7fe954e3[.]random[.]freelancersquadbd[.]com[.]cdn[.]hstgr[.]net
- a534028c-bdc6-42df-b444-49a65fdbb691[.]random[.]key2gift[.]com[.]cdn[.]hstgr[.]net
- a8246e4f-25f9-42a3-b578-bd24db1c22ea[.]random[.]eduverseclub[.]com[.]cdn[.]hstgr[.]net
- abonnement-iptv-france[.]fr
- b2c1727c-cefc-4e93-901b-c9cf85864bfc[.]random[.]srnseeds[.]in[.]cdn[.]hstgr[.]net
- baidyanath[.]net[.]in
- bakeoftheday[.]ca[.]cdn[.]hstgr[.]net
- c2e5cc31-1452-4801-8def-dcdf35db73bd[.]random[.]paycash4myproperty[.]com[.]cdn[.]hstgr[.]net
- c7402a95-6fc9-4756-b4e6-fa6c7eeb29c6[.]random[.]bodhihealthbeauty[.]co[.]uk[.]cdn[.]hstgr[.]net
- camarilloweather[.]com
- d229da4d-8570-49ca-93ee-e046915ac93c[.]random[.]game707[.]org[.]cdn[.]hstgr[.]net
- d2b73001-55f2-4c30-bd49-18a5189cad2e[.]random[.]henfad[.]com[.]cdn[.]hstgr[.]net
- d678b654-e13b-402b-9a77-9489b6211ed7[.]random[.]vickylastra[.]com[.]cdn[.]hstgr[.]net
- e9cd8849-0398-4486-9f24-016905b0be92[.]random[.]kakaeosopen0[.]kr[.]cdn[.]hstgr[.]net
- easybestshoponline[.]com
- edgeinsightsllc[.]com
- f3d30855-b968-48c0-ab87-623e96d7b7be[.]random[.]prefabprefect[.]com[.]cdn[.]hstgr[.]net
- f9ccb1e3-5b4e-4e22-92e2-73d4fd25d146[.]random[.]zemzemofset[.]com[.]cdn[.]hstgr[.]net
- factsandfiguresconsulting[.]com
- gadgetsplaza[.]com
- gamefur[.]xyz
- gamesplay[.]digital
- h31game[.]net
- h5hub[.]site
- hakeemphotos[.]co[.]uk[.]cdn[.]hstgr[.]net
- icefoundation-int[.]org
- icefoundation-int[.]org[.]cdn[.]hstgr[.]net
- ideaoman[.]shop
- janfilms[.]com

- jasvantsoap[.]com
- jawedlimitedliabilitycompany[.]com
- k2game[.]net
- kaaseb[.]sa
- kabarpolitik[.]com
- lalithatraders[.]com
- lamitrims[.]com
- lapalmabeautyhouse[.]com
- macrotrade[.]live
- madhavmunjal[.]com
- magicalmg[.]com
- nabroh[.]com
- nakshatra-kukatpally[.]com
- nationaltrailerstore[.]com
- oceantransit[.]click
- odoasem[.]com
- odontologicamente[.]com
- pagevisitcounter[.]com
- paintcolorcombos[.]com
- pakunique[.]com
- qualitywoodcrafting[.]com[.]cdn[.]hstgr[.]net
- quantumailiveinvestment[.]pro
- queuekart[.]com
- raghavacapital45[.]com
- raghavacinq[.]com
- raksha-anirveda[.]com
- s55game[.]com
- sacmobilewelding[.]com
- safetycrave[.]com
- t-unlocking[.]com
- taimar[.]net
- tampabayedm[.]com
- uem[.]com[.]br
- ukfreegm[.]site
- ultracleansolutions[.]info
- valleetravel[.]com
- vayalmart[.]com
- verbalizado[.]com
- w567app[.]com
- w567game[.]com
- w567game[.]net
- xs135[.]xs[.]to
- xs73[.]xs[.]to
- xtoyshub[.]com
- yancechilds[.]com
- yk-accessory[.]com
- yuecon[.]com
- zainabfamilymart[.]com
- zamzafashion[.]com
- zapthatpdf[.]com

Sample String-Connected Domains

- k2ioeasm874fnacr9x[.]ph
- pyej17uw09d1bqlndg[.]ws
- usermanualsonline[.]xyz