WhoisXMLAPI
The Who Behind Domain, IP & Cyber Threat Intelligence

DNS Deep Dive: LummaStealer + CastleLoader = Larger Threat

Threat Report

Table of Contents

Executive Report

LummaStealer reportedly got a second lease on life after years of being considered the world's most prolific information stealer. Even after a significant law-enforcement disruption in 2025, LummaStealer operations continued, demonstrating the malware's resilience aided by rapidly migrating to new hosting providers and adapting alternative loaders and delivery techniques like ClickFix.

Bitdefender uncovered a new LummaStealer campaign that used CastleLoader as its central delivery mechanism. This combination allowed the infostealer to use in-memory execution, heavy obfuscation, and flexible payload deployment to evade detection and enable massive distribution.

The researchers identified several network IoCs in their report. After extracting domains from the subdomains tagged as IoCs and excluding those that belonged to legitimate organizations, we collated 211 IoCs comprising two subdomains, 180 domains, and 29 IP addresses for further analysis, which led to these discoveries:

- Three domains classified as IoCs were bulk-registered with 2–5 look-alikes each
- 49 domains named as IoCs seemed to have been registered with malicious intent from the get-go
- 103,038 unique potential victim IP addresses communicated with 10 IP addresses categorized as IoCs
- 129 email-connected domains, 26 of which were deemed malicious
- 200 additional IP addresses, 196 of which turned out to be malicious
- 813 IP-connected domains, 229 of which have already been weaponized for attacks
- 404 string-connected domains

More Information on the Subdomains Identified as IoCs

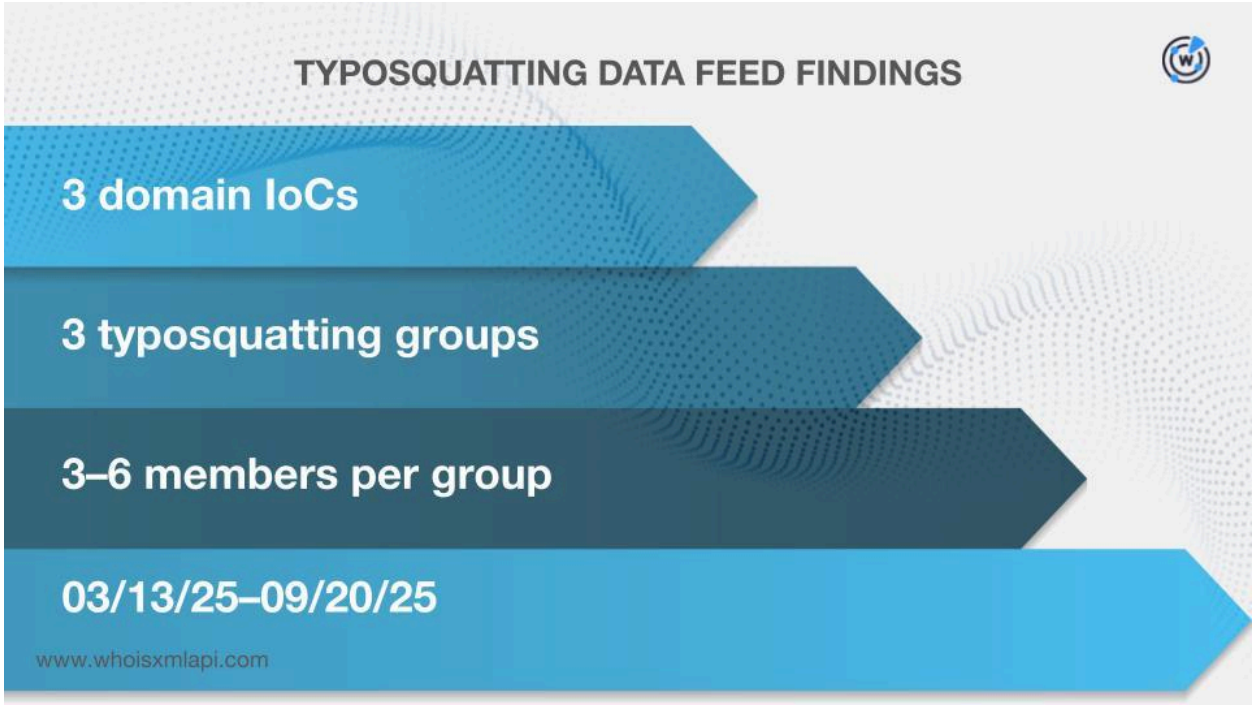
We began our investigation by looking for more information on the two subdomains tagged as IoCs via the WhoisXML API MCP Server. And we discovered that:

- The naming convention applied to the subdomain confvx[.]windowmv[.]com is characteristic of malware C&C infrastructure or phishing domains. It has a random-looking subdomain combined with a domain mimicking a legitimate software name, in this case potentially spoofing "Windows," which are commonly used in malicious campaigns.
- The randomly generated-looking strings for both the subdomain and the base domain in suzoo[.]ryxuz[.]com, meanwhile, is a hallmark of being part of a DGA infrastructure that is commonly used by malware to evade blocklists.

Additional Facts about the Domains Tagged as IoCs

We then shifted our focus on the 180 domains identified as IoCs.

Our searches on the Typosquatting Data Feed revealed that three of the domains classified as IoCs appeared in three typosquatting groups with 3–6 members each (i.e., one IoC and 2–5 look-alikes). They were registered between 13 March and 20 September 2025.

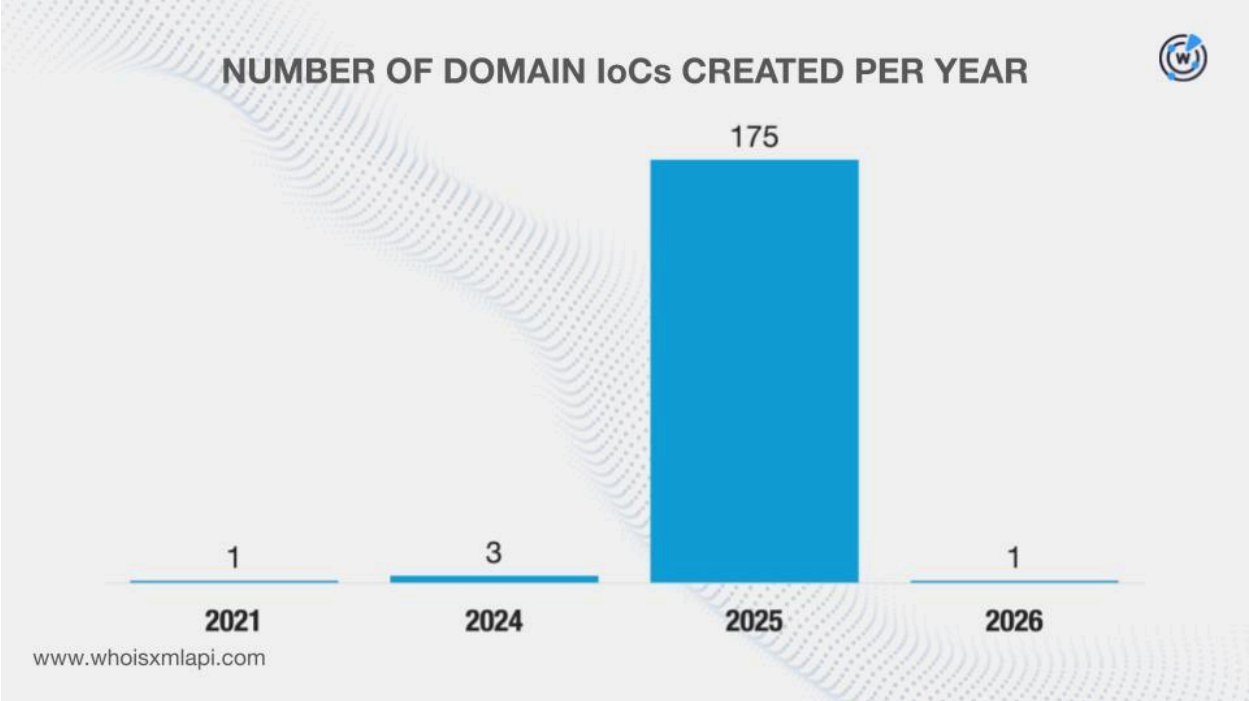


Our First Watch Malicious Domains Data Feed search results showed that 49 of the domains named as IoCs could have been registered with malicious intent. They were deemed likely to turn malicious 43–432 days before being dubbed as IoCs on 11 February 2026. Take a look at five examples below.

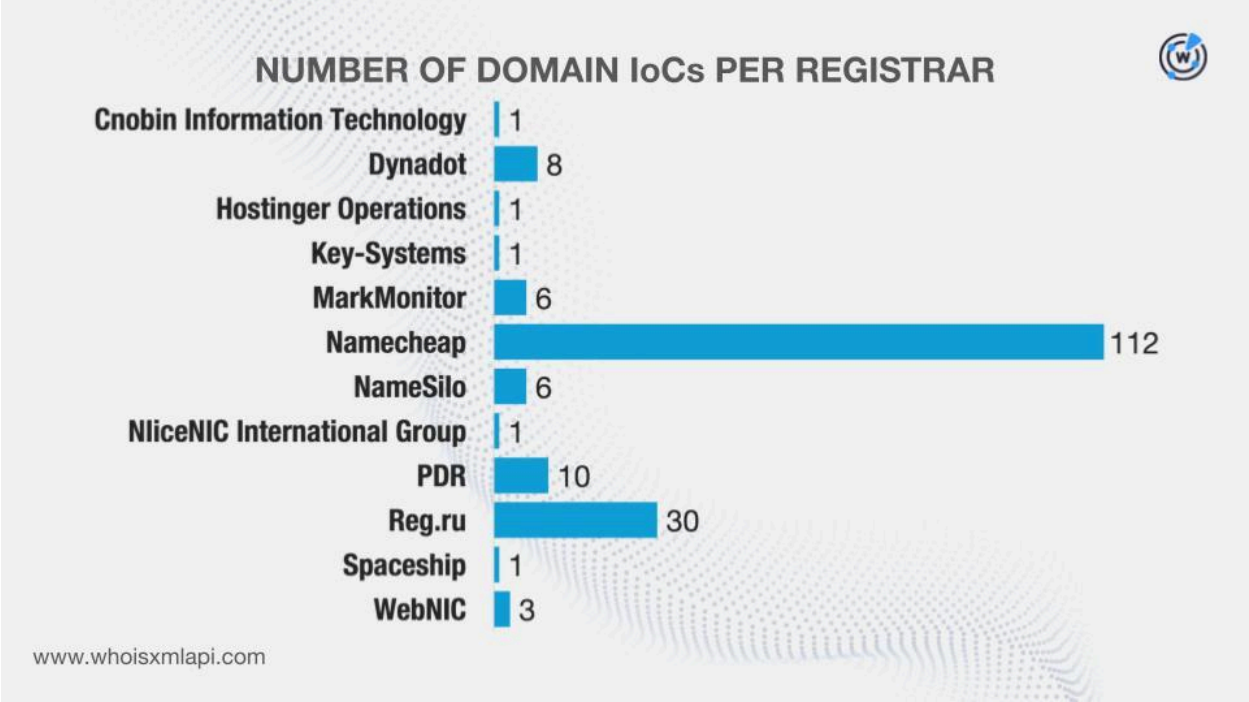
DOMAIN IoC	FIRST WATCH DATE	NUMBER OF DAYS BEFORE THE REPORT DATE
diffuculttan[.]xyz	12/06/24	432
effecterectz[.]xyz	12/06/24	432
mannelaeksug[.]top	01/17/25	390
sterilizeflow[.]top	01/17/25	390
weighcobbweo[.]top	01/17/25	390

Next, we queried the domains on WHOIS API. We found out that one did not have current WHOIS registration data but we did obtain historical information from Domain Info API. Our searches led to these findings:

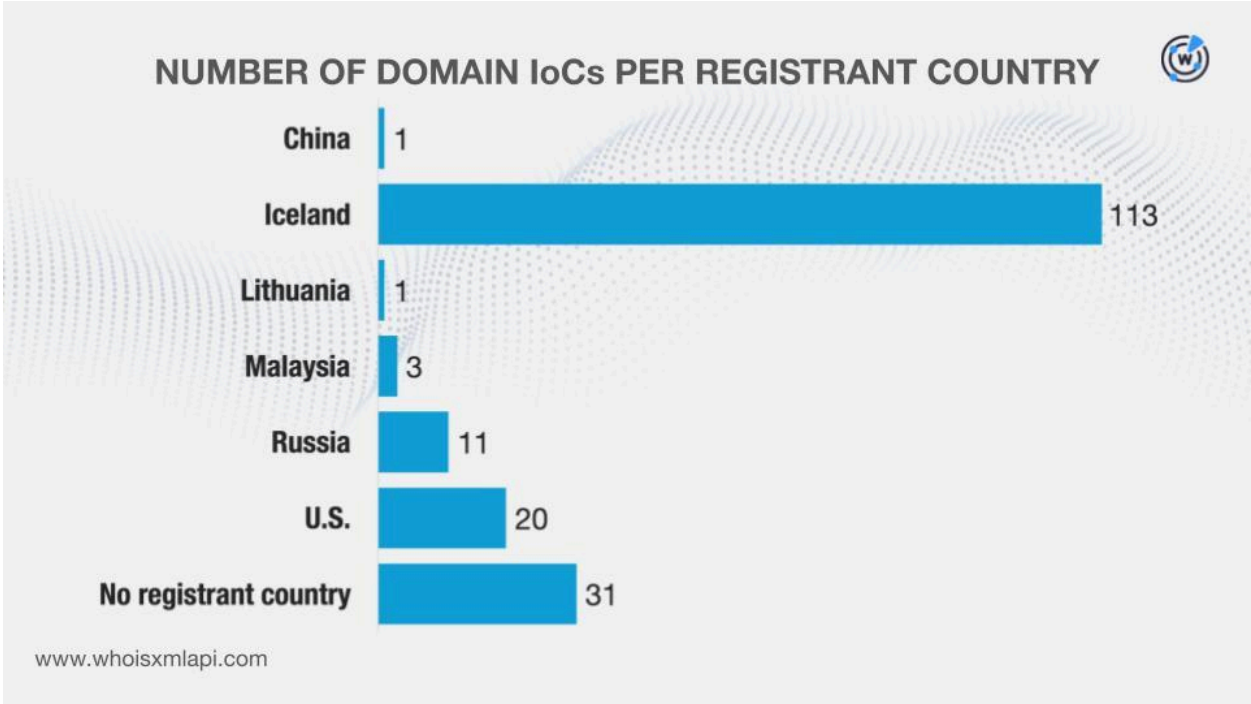
- They were created between 7 June 2021 and 1 January 2026.



- They were administered by 12 different registrars.



- And while 31 of them did not have registrant countries on record, the remaining 149 were registered in six different countries.



Last but not least, we queried the domains on DNS Chronicle API and found out that 161 had 2,944 historical domain-to-IP resolutions over time. Here are more details on five of them.

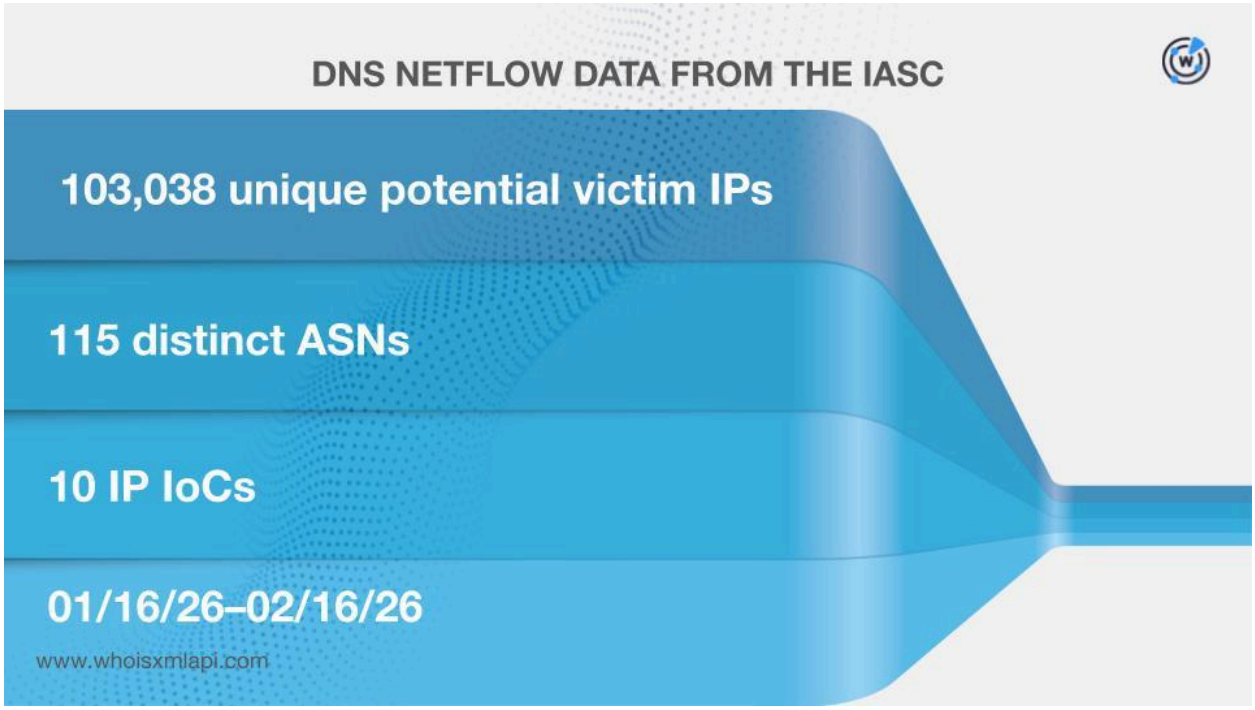
DOMAIN IoC	NUMBER OF DOMAIN-TO-IP RESOLUTIONS	DATES SEEN
whitepepper[.]su	477	07/01/17–02/08/26
rifledog[.]xyz	11	01/08/18–01/20/26
sealake[.]info	227	04/16/18–02/16/26
tailcoat[.]xyz	81	04/19/19–02/07/26
hatwomen[.]info	69	12/08/19–02/16/26

A closer look at the historical domain-to-IP resolutions also showed that a majority of the domains categorized as IoCs, 148 to be exact, first recorded resolutions in 2025.

Further Insights into the IP Addresses Named as IoCs

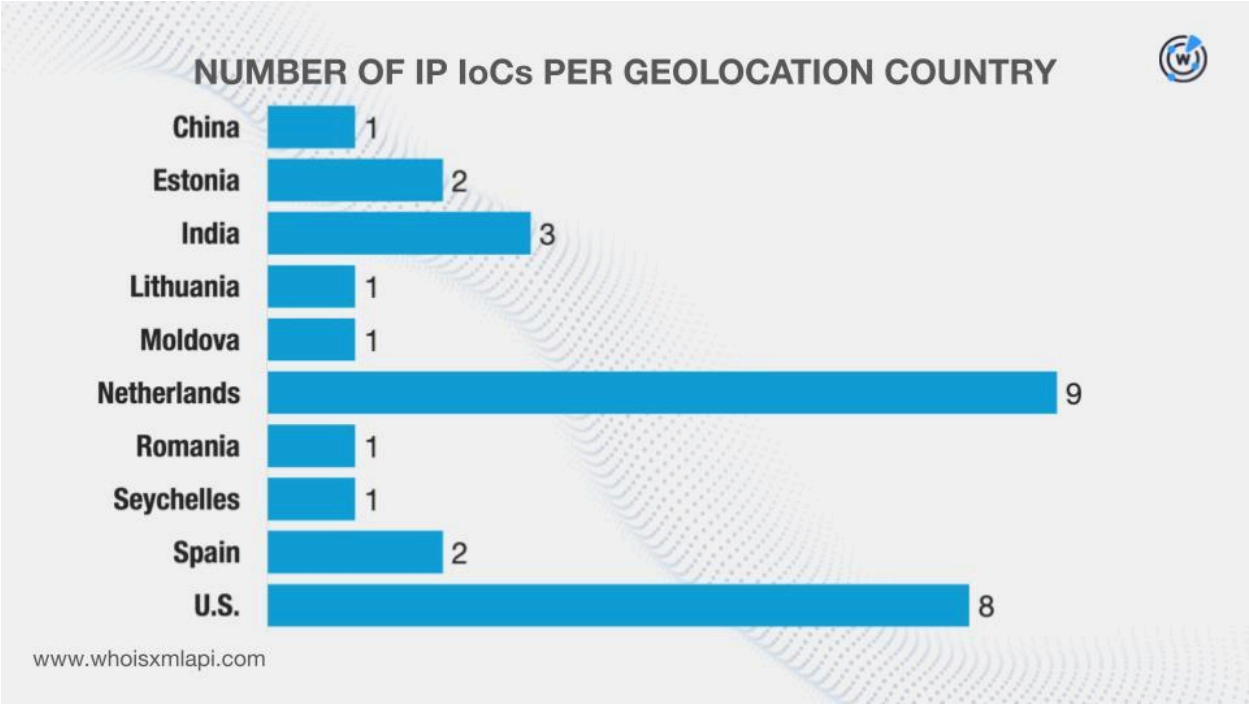
After that, we zoomed in on the 29 IP addresses identified as IoCs.

Sample network traffic data from the IASC revealed that 103,038 unique potential victim IP addresses under 115 distinct ASNs communicated with 10 of the IP addresses tagged as IoCs between 16 January and 16 February 2026.

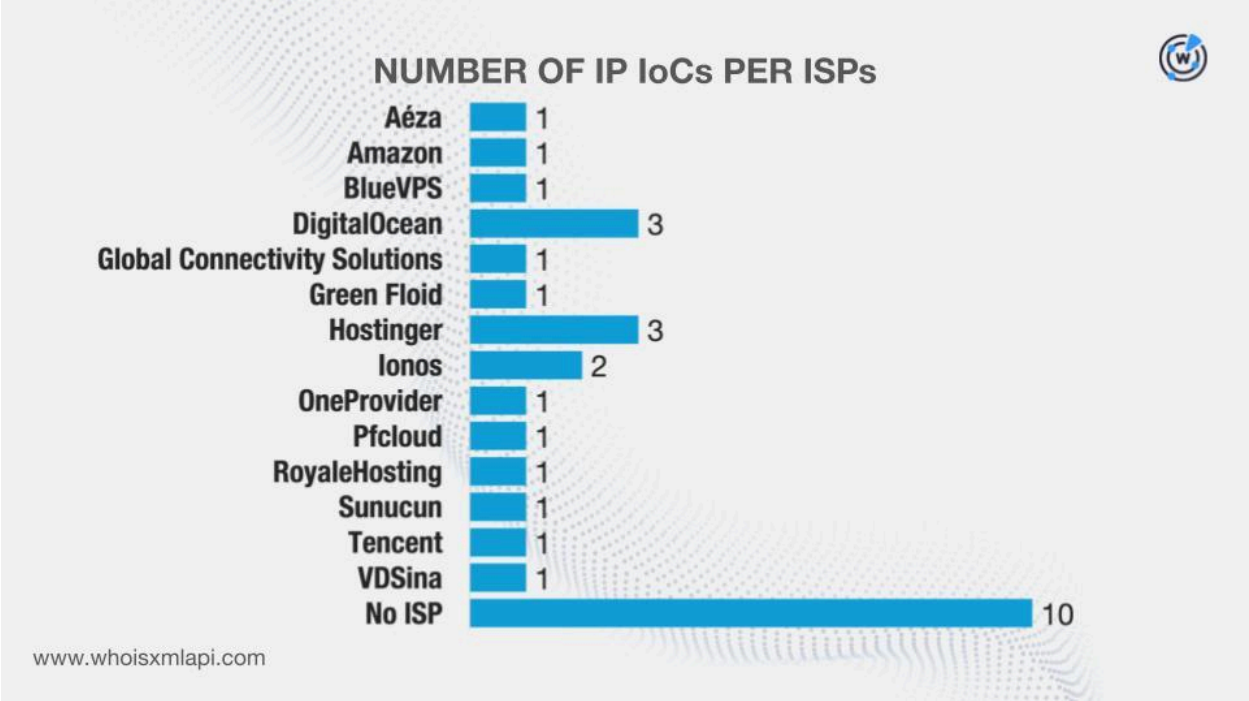


Next, we queried them on Bulk IP Geolocation Lookup and discovered that:

- They were geolocated in 10 different countries. It is worth noting that three of the geolocation countries—China, Lithuania, and the U.S.—were also named as registrant countries earlier.



- While 10 did not have ISPs on record, the remaining 19 were administered by 14 different ISPs.



Our DNS Chronicle API queries for the IP addresses, meanwhile, revealed that 24 had 2,869 historical IP-to-domain resolutions over time. Take a look at more information for five examples below.

IP IoC	NUMBER OF IP-TO-DOMAIN RESOLUTIONS	DATES SEEN
85[.]90[.]196[.]155	266	02/04/17–01/12/26
185[.]121[.]233[.]78	217	02/06/17–02/04/22
31[.]220[.]109[.]219	46	09/23/17–12/12/25
144[.]172[.]115[.]212	214	07/23/18–12/08/25
206[.]189[.]97[.]184	308	08/17/18–02/12/26

In comparison to the domains categorized as IoCs, eight of the IP addresses dubbed as IoCs recorded their first resolutions in 2025.

DNS Deep Diving for New Artifacts

Our hunt for other LummaStealer-connected artifacts started with WHOIS History API queries for the 180 domains identified as IoCs. We discovered that 165 of them had 159 unique email addresses in their historical WHOIS records. Further scrutiny showed that 15 were public email addresses.

The results of our Reverse WHOIS API queries for the 15 public email addresses revealed that one could belong to a domainer, excluding it from further analysis. This step led to the discovery of 129 unique email-connected domains after those already tagged as IoCs were filtered out.

Threat Intelligence API queries for the email-connected domains showed that 26 have already been confirmed as malicious. Here are more details for five examples.

MALICIOUS EMAIL-CONNECTED DOMAIN	ASSOCIATED THREAT	DATES SEEN
advennture[.]top	Malware distribution	03/23/25–02/16/26
boustrn[.]su	Malware distribution	09/26/25–02/16/26

consnbx[.]su	Malware distribution	09/09/25–02/16/26
cornerdurv[.]top	Malware distribution	05/20/25–02/16/26
coverxyzer[.]su	Malware distribution	01/07/26–02/16/26

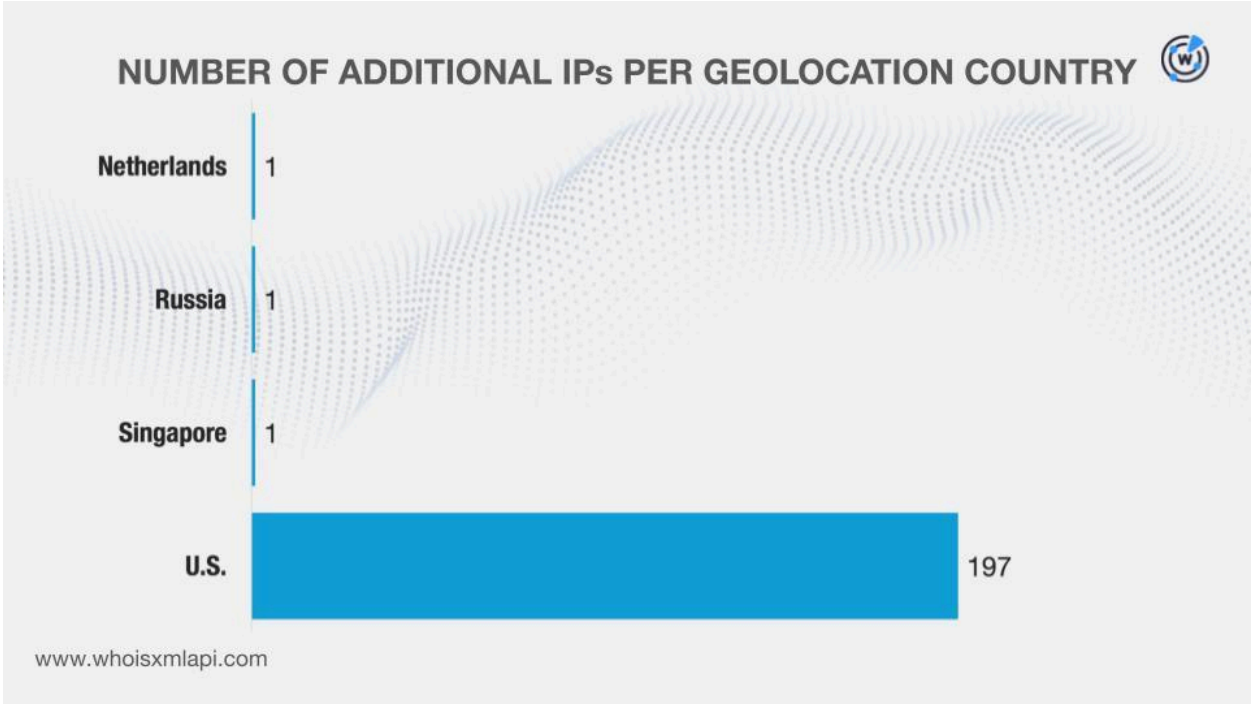
Next, we queried the domains dubbed as IoCs on DNS Lookup API and found out that 125 actively resolved to 200 unique additional IP addresses.

Threat Intelligence API queries for the additional IP addresses showed that 196 have already figured in several malicious campaigns. Take a look at more details about five examples below.

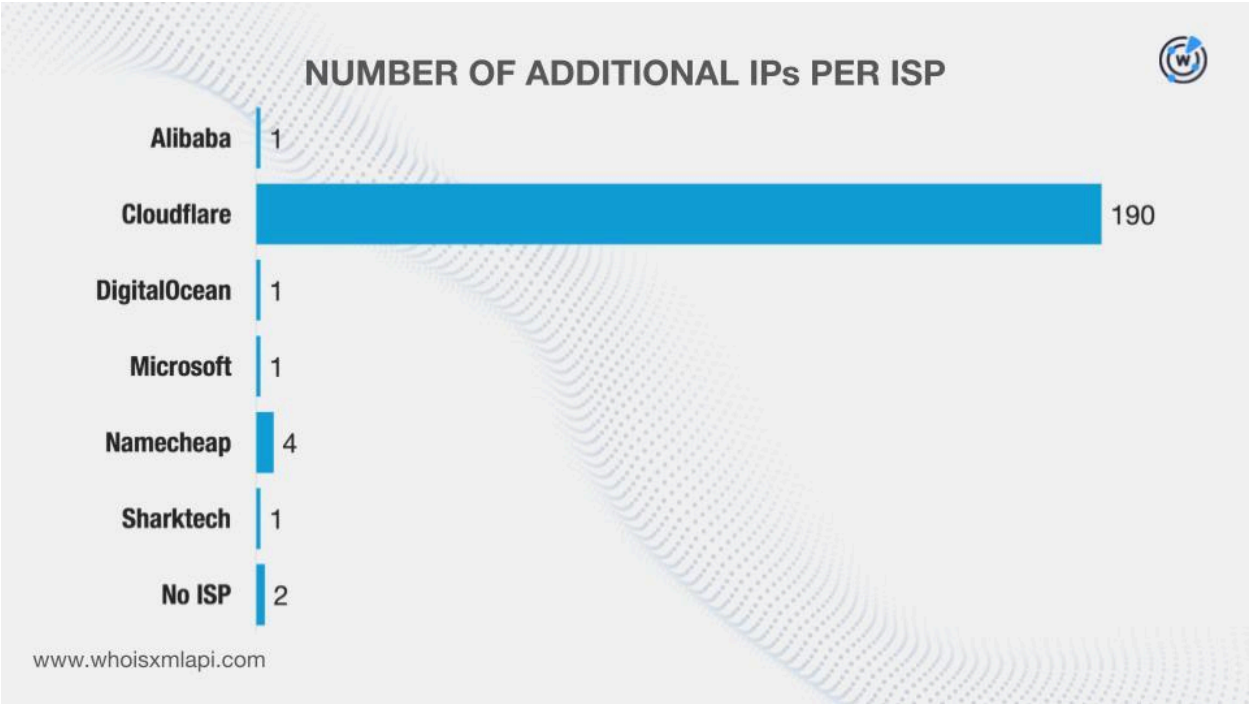
MALICIOUS ADDITIONAL IP ADDRESS	ASSOCIATED THREAT	DATES SEEN
104[.]21[.]2[.]220	Phishing Malware distribution C&C Generic threat	03/29/23–02/16/26 03/09/23–02/15/26 04/06/23–02/15/26 04/04/23–02/15/26
172[.]67[.]189[.]196	Malware distribution Generic threat C&C Phishing	03/09/23–02/16/26 03/28/23–02/15/26 04/06/23–02/15/26 12/02/23–01/26/26
104[.]21[.]13[.]76	Phishing Malware distribution Suspicious activity	05/24/23–02/16/26 11/26/24–02/15/26 04/25/25–01/28/26
104[.]21[.]16[.]209	Generic threat Phishing Malware distribution	03/28/23–02/16/26 03/03/24–02/14/26 11/07/24–01/21/26
104[.]21[.]19[.]222	Phishing Malware distribution Generic threat	04/16/23–02/15/26 09/27/23–02/15/26 12/31/24–12/09/25

We then queried the additional IP addresses on Bulk IP Geolocation Lookup and discovered that:

- They were geolocated in four different countries. The Netherlands and the U.S. also appeared in the list of geolocation countries for the IP addresses named as IoCs.



- While two of them did not have ISPs on record, the remaining 198 were administered by six different ISPs. Note that DigitalOcean was also in the list of ISPs for the IP addresses categorized as IoCs.



We now had 229 IP addresses (i.e., 29 named as IoCs and 200 additional) for further analysis. We queried them on Reverse IP API and discovered that 19 could be dedicated hosts. Together, they hosted 813 unique IP-connected domains after those already identified as IoCs and the email-connected domains were filtered out.

Threat Intelligence API queries for the IP-connected domains revealed that 229 have already been weaponized for various attacks. Here are five examples.

MALICIOUS IP-CONNECTED DOMAIN	ASSOCIATED THREAT	DATES SEEN
4teentech[.]com	Phishing	07/27/25–01/26/26
absoluod[.]cyou	Malware distribution	01/24/26–02/16/26
aliengp[.]cyou	Malware distribution	01/30/26–02/16/26
amerimq[.]cyou	Malware distribution	01/30/26–02/16/26
annonalc[.]cyou	Malware distribution	01/06/26–02/16/26

Lastly, we looked for domains that started with the same strings as those tagged as IoCs. Our Domains & Subdomains Discovery searches turned up 404 unique string-connected domains after those already named as IoCs and the email- and IP-connected domains were filtered out. They started with 94 distinct text strings extracted from the IoCs, such as:

- airplanemove.
- backfruit.
- cabbagecircle.
- diadtuky.
- exampleporter.
- familyriwo.
- hairlace.
- inkseed.
- liquidtoes.
- maidtin.
- needleexperience.
- ozonelf.
- pailchange.
- readingpart.
- sealake.
- tailcoat.
- uploadtree.
- verserun.
- weatherforce.
- yamakrug.

Note that the string-connected domains only serve to reflect the overall popularity of the strings extracted from the IoCs. As such, determining their legitimacy may require further investigation.

Summing Up

Our analysis of the campaign leveraging the LummaStealer-CastleLoader malware combination revealed that three of the domains identified as IoCs were bulk-registered with 2–5 look-alikes each. We also learned that 49 of the domains tagged as IoCs could have been registered with malicious intent from the get-go. In addition, 103,038 unique potential victim IP addresses communicated with 10 of the IP addresses dubbed as IoCs.

On top of all that, we uncovered 1,546 new artifacts comprising 129 email-connected domains, 200 additional IP addresses, 813 IP-connected domains, and 404 string-connected domains. It is also worth noting that 451 of the additional artifacts have already figured in various malicious campaigns.

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

- advennture[.]top
- boustrn[.]su
- consnbx[.]su
- cornerdurv[.]top
- coverxyzer[.]su
- descroej[.]su
- desigvndeta[.]top
- emphatakpn[.]bet
- esccapewz[.]run
- featurlyin[.]top
- fittinvgfie[.]top
- gettoknwg[.]life
- gogetxto[.]life
- haircuirfm[.]top
- holidamyup[.]today
- iosif-brodskiy[.]su
- korney-chukovsky[.]su
- leasegjjr[.]digital
- lumma-market[.]su
- moluntmarke[.]top
- operateoxasi[.]top
- phrupmv[.]su
- posseswsnc[.]top
- saxecocnak[.]live
- telephoned[.]su
- triplooqp[.]world

Sample Additional IP Addresses

- 104[.]21[.]2[.]220
- 172[.]67[.]189[.]196
- 104[.]21[.]13[.]76
- 104[.]21[.]16[.]209
- 104[.]21[.]19[.]222
- 104[.]21[.]20[.]113
- 104[.]21[.]24[.]8
- 104[.]21[.]29[.]13
- 104[.]21[.]39[.]176
- 104[.]21[.]39[.]221
- 104[.]21[.]41[.]66
- 104[.]21[.]47[.]93
- 104[.]21[.]5[.]4
- 104[.]21[.]50[.]53
- 104[.]21[.]56[.]84
- 104[.]21[.]58[.]119
- 104[.]21[.]58[.]182
- 104[.]21[.]59[.]2
- 104[.]21[.]61[.]214
- 104[.]21[.]63[.]208
- 104[.]21[.]64[.]81
- 104[.]21[.]66[.]232
- 104[.]21[.]70[.]150
- 104[.]21[.]73[.]236
- 104[.]21[.]73[.]41

Sample IP-Connected Domains

- 4teentech[.]com
- absoluod[.]cyou
- aliengp[.]cyou
- amerimq[.]cyou
- annonalc[.]cyou
- apomlwi[.]click
- apostrwz[.]cyou
- assumhw[.]cyou
- atalozv[.]qpon
- audioza[.]cyou
- backsan[.]cyou
- ballisi[.]cyou

- baronns[.]click
- batonra[.]qpon
- belloww[.]cyou
- bemuseqy[.]cyou
- bimonwz[.]cyou
- blushwb[.]cyou
- bondixa[.]qpon
- botanyh[.]cyou
- braxttp[.]cyou
- cacodsq[.]click
- cancellationdrivingtest[.]com
- capitamx[.]cyou
- caressv[.]qpon

Sample String-Connected Domains

- airplanemove[.]casa
- airporticicle[.]ph
- apparatustruck[.]club
- auntedge[.]bid
- backfruit[.]club
- bathsmile[.]co[.]uk
- battlefi[.]app
- bedroomeyes[.]art
- bendavo[.]com
- boyfoot[.]bid
- broguenko[.]ws
- cabbagecircle[.]bid
- cablecanvas[.]com
- circlewar[.]com
- clothcrib[.]com
- coalcreator[.]xyz
- coasttreatment[.]ca
- coatberry[.]ph
- conxmsw[.]ph
- creatorthread[.]com
- cubmilk[.]science
- diadtuky[.]ph
- exampleporter[.]pw
- exposqw[.]ph
- familyriwo[.]ph
- fangbear[.]bid
- fieldfly[.]au
- fogbed[.]com
- frameneck[.]bid
- fruitroot[.]co
- hairlace[.]ca
- hammernew[.]com
- hatstart[.]club
- hatwomen[.]biz
- heataction[.]com
- hillcelery[.]ph
- horsesink[.]com
- hoursuhouy[.]ph
- inkseed[.]app
- liquidtoes[.]host
- lunchstar[.]co[.]kr
- maidtin[.]date
- needleexperience[.]ph
- needporter[.]com
- ozonelf[.]ph
- pailchange[.]ph
- paperbee[.]ai
- pickleblade[.]com
- pizzasreason[.]icu
- plasticjoin[.]com
- potatotoothpaste[.]club
- producesound[.]com
- profitfact[.]com
- projectamelie[.]be
- pumpbottle[.]com
- readingpart[.]top
- rewardscience[.]bid
- rhussois[.]ph
- ricestar[.]cn
- rifledog[.]com
- roofcakes[.]bid
- runhouses[.]com
- ryxuz[.]world
- sealake[.]au

- shameairport[.]fun
- shipfang[.]online
- skirtgrippys[.]ph
- squatje[.]ph
- stolewnica[.]ph
- streetway[.]asia
- structuredetail[.]faith
- suggestyuoz[.]ws
- tailcoat[.]at
- talkpump[.]com
- teachingbutter[.]online
- tenttiger[.]com
- theoryfood[.]bid
- tiltyufaz[.]ph
- toothpastesense[.]bid
- toppyneedus[.]ph
- tubvalue[.]website
- uploadtree[.]ph
- verserun[.]com
- vishneviyjazz[.]ph
- visokiywkaf[.]ph
- weatherforce[.]ca
- weightguide[.]club
- whitepepper[.]agency
- winedebt[.]cfd
- yamakrug[.]ph
- yardyak[.]com
- yrokistorii[.]com