WhoisXMLAPI
The Who Behind Domain, IP & Cyber Threat Intelligence

DNS Deep Dive: Pushpaganda Network IoCs

Threat Report

Table of Contents

Executive Report

HUMAN's Satori Threat Intelligence and Research Team recently uncovered a novel ad fraud, social engineering, and scareware threat that they dubbed "Pushpaganda." The attackers tricked users into enabling push notifications—from which the operation was named—to address issues presented via alarming messages.

The campaign abused Google's Discovery feeds. How? The threat actors use advanced SEO techniques and AI-generated content to inject deceptive news into Android and Chrome users' personalized content streams. The final payload? Users were served scareware messages. Some also received fake legal threats or were lured into financial scams.

The in-depth Pushpaganda analysis publicized 113 domain IoCs. Aided by the WhoisXML API MCP Server, we determined that some were owned by legitimate entities so they were excluded from our investigation. That said, we limited our analysis to 90 domain IoCs.

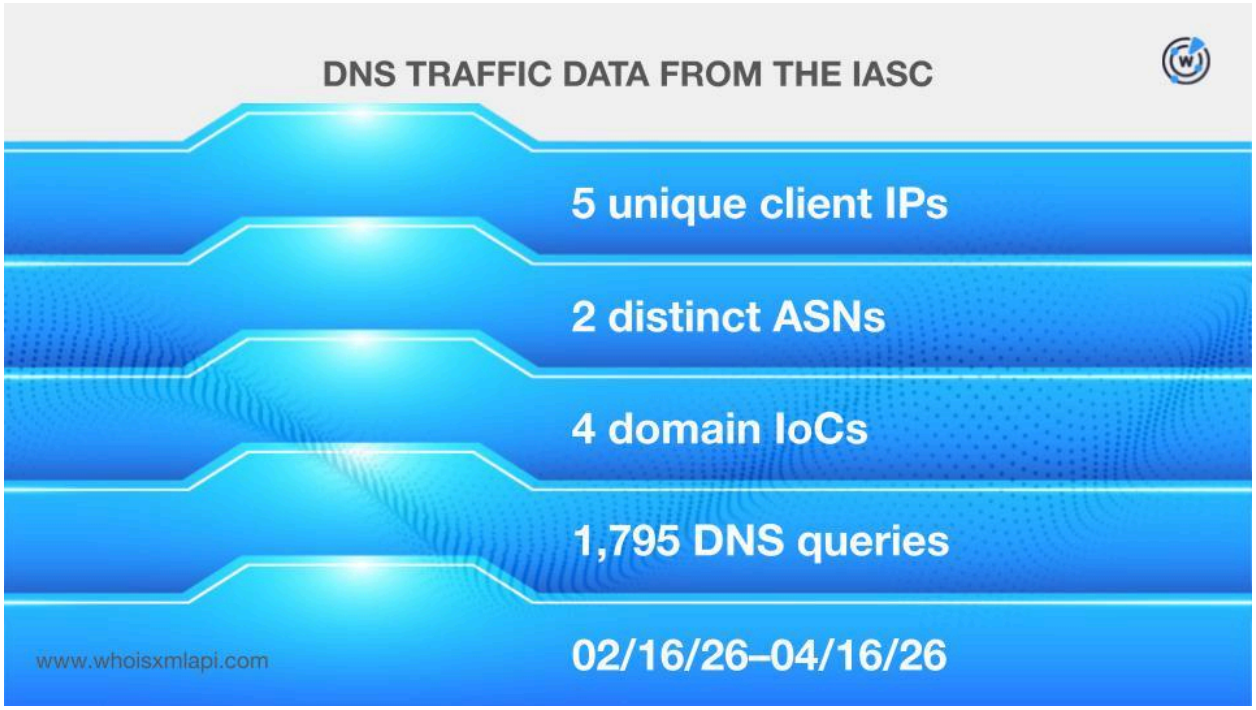
Our DNS deep dive led to these discoveries:

- Five unique client IP addresses communicated with four domain IoCs
- One domain IoC was bulk-registered with two look-alikes
- Eight domain IoCs were likely registered with malicious intent
- 1,055 email-connected domains
- 162 IP addresses, 101 were confirmed malicious
- Eight IP-connected domains
- 858 string-connected domains, one was confirmed malicious

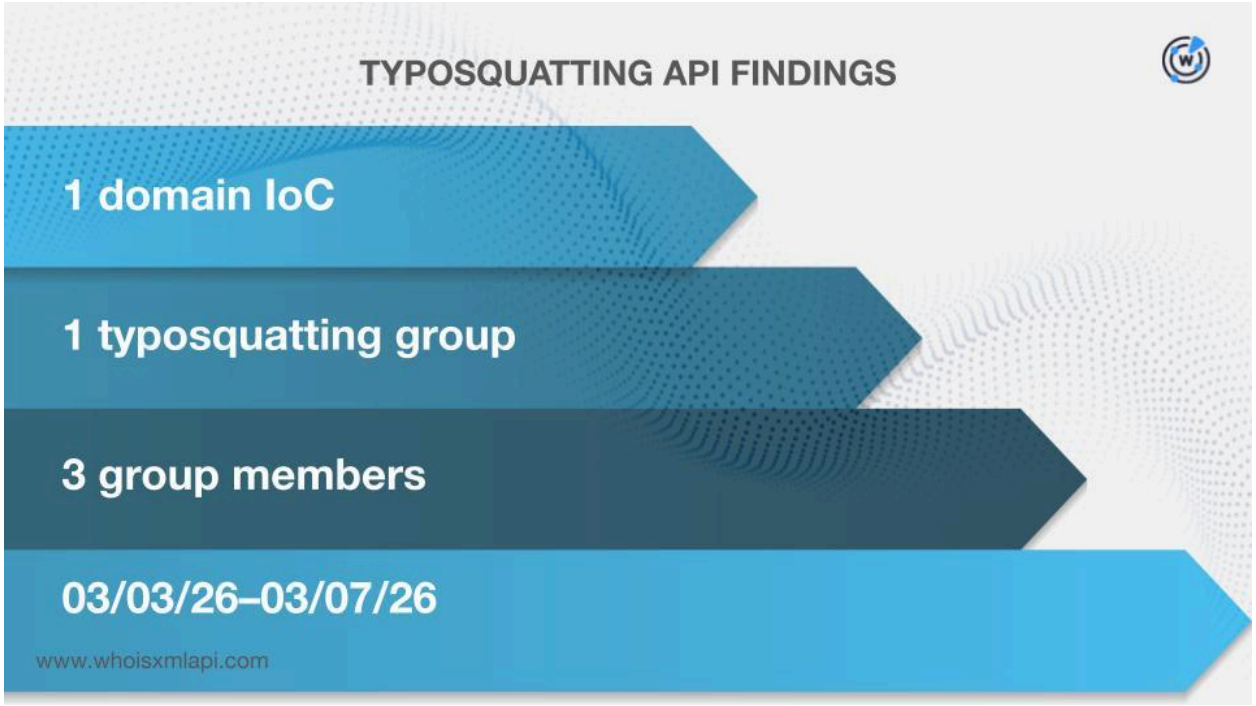
Examining the Pushpaganda Domain IoCs

We started our deep dive by taking a closer look at the 90 domain IoCs.

Sample network traffic data from the IASC, for one, revealed that five unique client IP addresses under two distinct ASNs communicated with four of the domain IoCs via 1,795 DNS queries made between 16 February and 16 April 2026.



We then queried the domain IoCs on Typosquatting API and discovered that the domain IoC triplek[.]co[.]za was bulk-registered with two look-alikes—triplex[.]industries and triplea[.]pl.

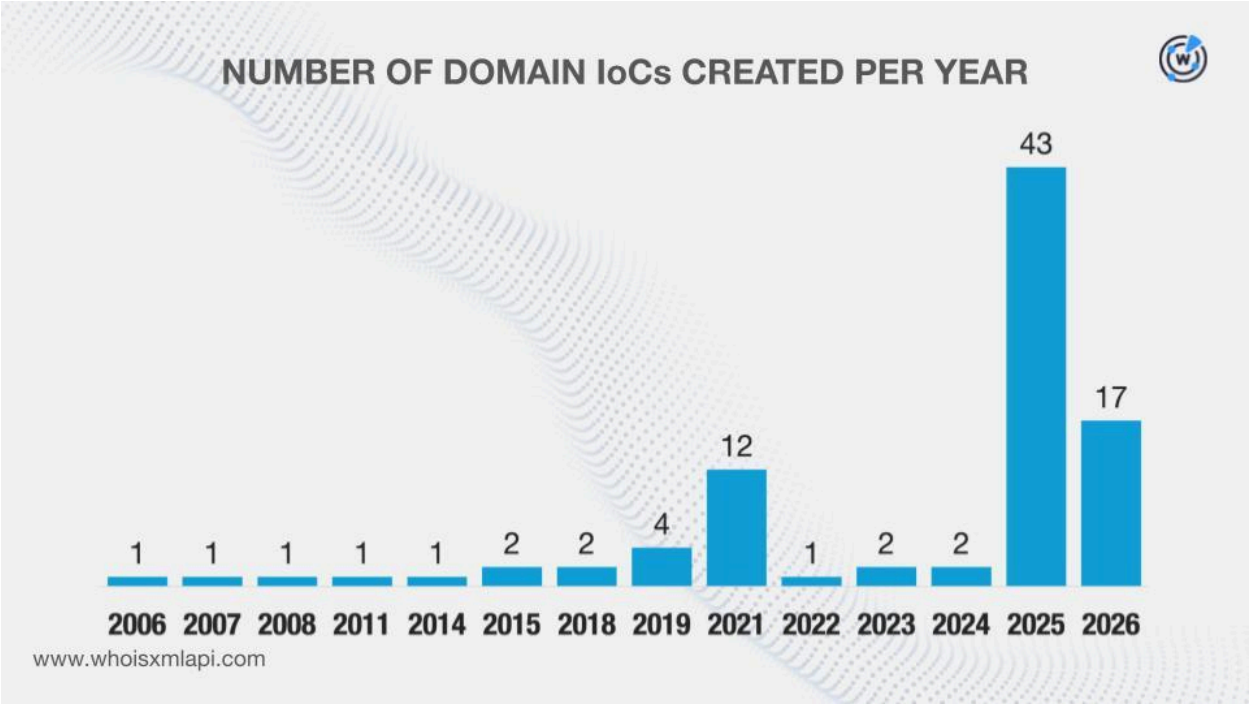


Next, we determined that eight of the domain IoCs appeared on the First Watch Malicious Domains Data Feed 67–465 days prior to being dubbed as such on 14 April 2026. They were likely registered with malicious intent between 4 January 2025 and 6 February 2026. Here are more details on five examples.

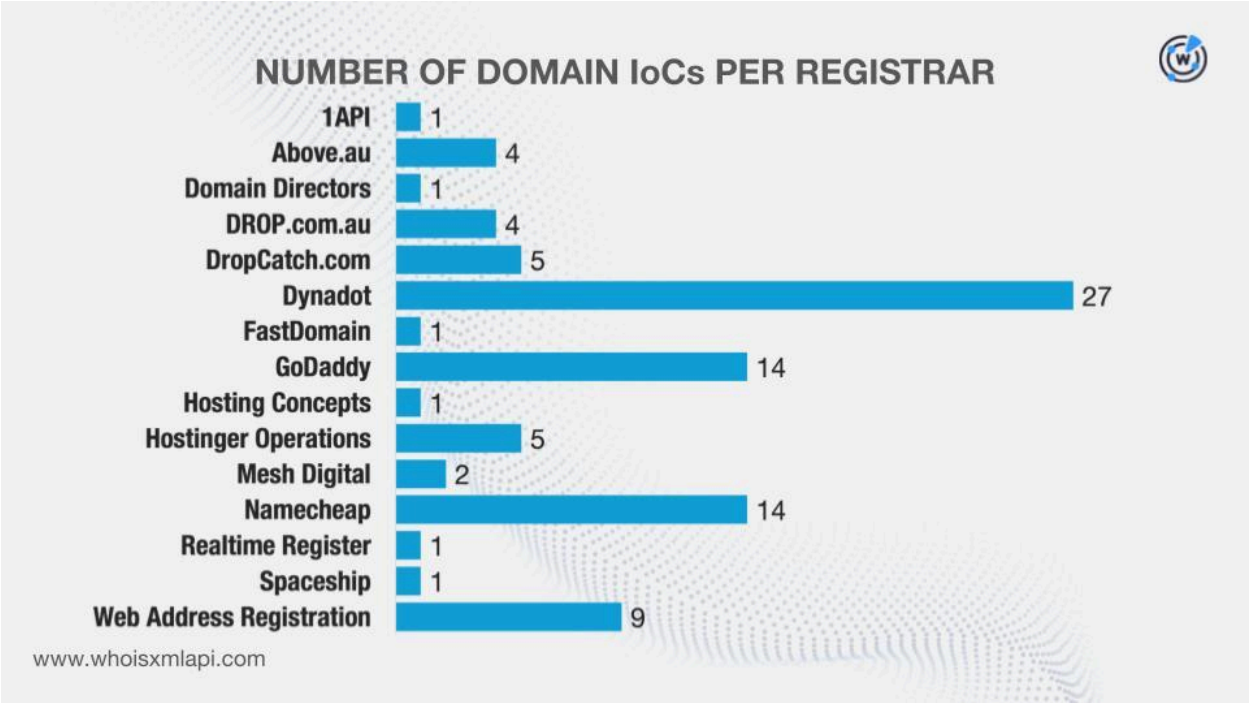
DOMAIN IoC	FIRST WATCH DATE	NUMBER OF DAYS BEFORE THE REPORT DATE
harvardglobalcollege[.]co[.]za	01/04/25	465
alakamahabidyalaya[.]org	05/22/25	327
shastrijimahilavidyaniketan[.]org	05/28/25	321
behavioralhealthworkforce[.]org	09/16/25	210
northcoastradio104[.]co[.]za	09/26/25	200

We then queried the domain IoCs on WHOIS API and completed missing information in their current WHOIS records from their historical records with the help of Domain Info API. We found out that:

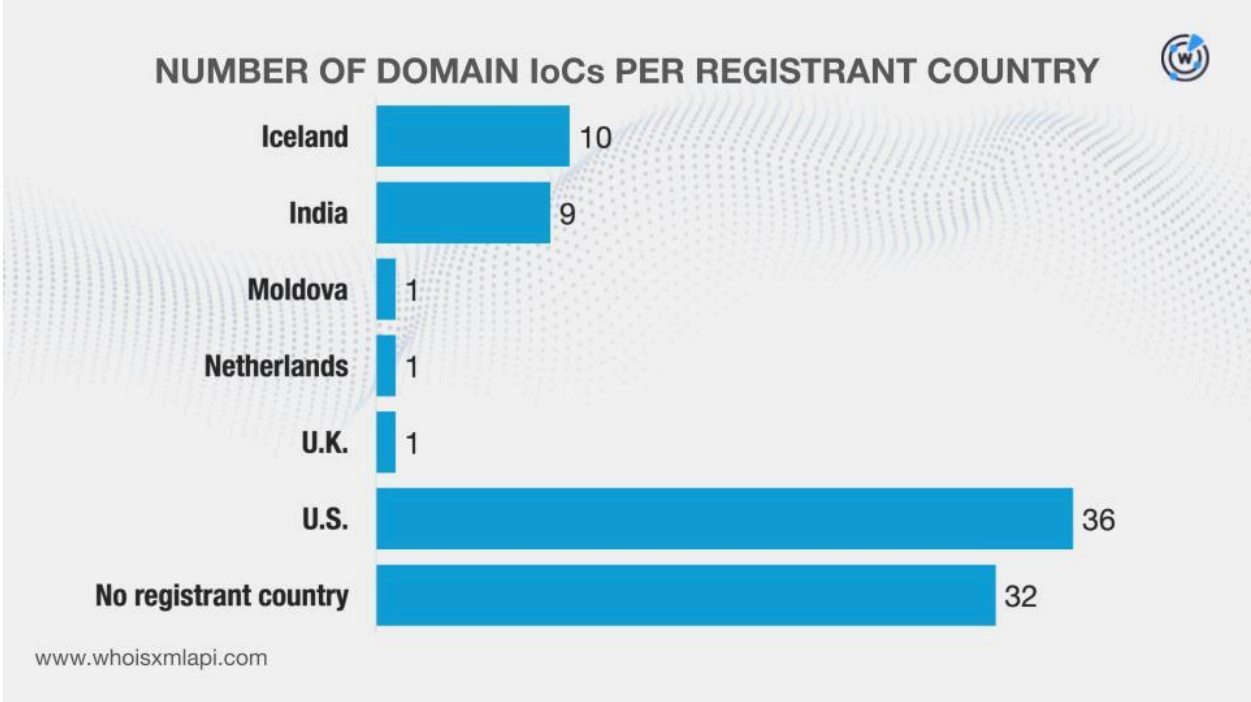
- They were a mix of old and new domains created between 18 October 2006 and 10 April 2026, possibly indicating that the attackers did not have a specific domain age preference.



- They were administered by 15 different registrars.



- While 32 did not have registrant countries on record, the remaining 58 were registered in six different countries.



Finally, we queried the domain IoCs on DNS Chronicle API and discovered that together they posted 21,880 historical domain-to-IP resolutions over time. Here are more details on five examples.

DOMAIN IoC	NUMBER OF DOMAIN-TO-IP RESOLUTIONS	DATES SEEN
thrillscranton[.]com	1,952	02/7/17–02/08/26
publishedreporter[.]com	1,799	01/11/19–04/16/26
jasminsgranville[.]com[.]au	732	11/30/19–01/30/26
englishproject[.]org	608	04/17/17–02/14/26
cisda[.]org	524	02/04/18–04/02/26

Seven of the domain IoCs—alakamahabidyalaya[.]org, apacollege[.]org, assessmentsonline[.]co[.]za, behavioralhealthworkforce[.]org, brokenhillcottages[.]com[.]au, crmcateringcollege[.]com, and gardn[.]org[.]au—started recording resolutions on 5 February 2017.

Uncovering New Pushpaganda-Connected Artifacts

We began our hunt for new artifacts by querying the 90 domain IoCs on WHOIS History API and discovered that 44 had 125 unique email addresses in their historical WHOIS records. Closer examination allowed us to determine that 38 were public email addresses.

Reverse WHOIS API queries for the public email addresses showed that 34 were used to register 1,055 unique email-connected domains after those already tagged as IoCs were filtered out.

We then queried the domain IoCs on DNS Lookup API and found out that 82 actively resolved to 162 unique IP addresses.

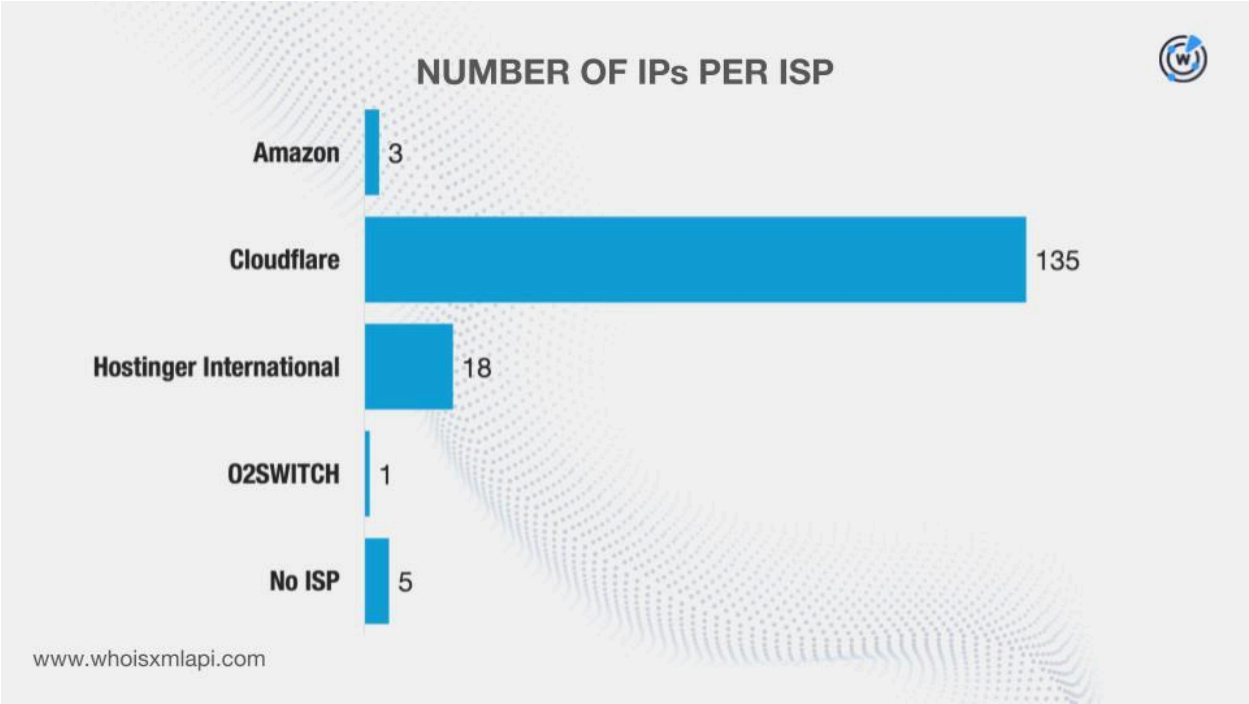
Threat Intelligence API queries for the IP addresses revealed that 101 have already been weaponized for various attacks. Here are more details on five examples.

MALICIOUS IP ADDRESS	ASSOCIATED THREAT	DATES SEEN
15[.]197[.]148[.]33	Malware distribution Phishing Generic threat Suspicious activity C&C Spam campaign	05/05/23–04/15/26 05/05/23–04/15/26 05/03/23–04/15/26 04/29/23–04/14/26 05/03/23–04/14/26 02/17/24–02/10/26
185[.]53[.]179[.]128	Phishing Suspicious activity Malware distribution Generic threat Spam campaign	01/21/26–04/16/26 03/18/26–04/15/26 12/12/25–04/15/26 02/04/26–04/14/26 02/10/26–04/01/26
103[.]224[.]182[.]250	Phishing Malware distribution Spam campaign Generic threat	04/10/23–04/16/26 03/09/23–04/15/26 06/30/24–02/10/26 03/28/23–02/08/26
103[.]224[.]212[.]205	Malware distribution Phishing Suspicious activity	03/25/25–04/15/26 03/25/25–04/13/26 03/25/25–04/07/26
104[.]21[.]10[.]78	Malware distribution Phishing	09/29/24–04/14/26 04/16/23–04/04/26

Next, we sought out more information regarding the IP addresses using Bulk IP Geolocation Lookup and discovered that:

- They were geolocated in five different countries and two—India and the U.S.—were among the domain IoCs' registrant countries.

- While five did not have ISPs on record, the remaining 157 were administered by four different ISPs.



We then queried the IP addresses on Reverse IP API and found out that only one could be a dedicated host. This led to the discovery of eight unique IP-connected domains after those already named as IoCs and the email-connected domains were filtered out.

Lastly, we further scrutinized the domain IoCs and extracted 56 unique text strings that according to Domains & Subdomains Discovery appeared at the start of 858 unique string-connected domains. These strings included but were not limited to:

- 14north108east.
- acento.
- basicsteeladelaide.
- cisda.
- dentalimplantkolkata.
- englishproject.
- farsirestaurant.
- gardn.
- harvardglobalcollege.
- i2apm.
- jasminsgranville.
- khariarautocollege.
- laposadadelsolsac.
- macgmagazine.
- ncpublichealthnursing.
- occasionalsettings.
- pacafdivertmarianaseis.
- reloadbar.
- sacreblue.
- taas.
- ucsportsnation.
- vacuumpouch.
- wyd2022.
- yourhealthydrinks.

Threat Intelligence API queries for the string-connected domains showed that one—newsfirst[.]io—has already figured in a malicious campaign. It was specifically associated with malware distribution between 9 March 2023 and 14 April 2026.

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 in-depth investigation of Pushpaganda revealed that five unique client IP addresses communicated with four domain IoCs. Also, one domain IoC was bulk-registered with two look-alikes. And eight domain IoCs were likely registered with malicious intent.

We also uncovered 2,083 new artifacts comprising 1,055 email-connected domains, 162 IP addresses, eight IP-connected domains, and 858 string-connected domains. It is also worth noting that to date, 102 of these have already been confirmed malicious.

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

- 100cap[.]com
- 1january2016images[.]com
- 2am[.]xyz
- aandanaturalproducts[.]com
- aap-mumbai[.]com
- aarjogroup[.]com
- backwaters[.]xyz
- bamracollege[.]org
- bangaloregirls[.]xyz
- calcinaconstructora[.]com
- callallicolca[.]com
- calquipa[.]com
- daddysdazzlingdiva[.]com
- daffodildesign[.]net
- dailyghotalaaajtak[.]com
- e-aryantech[.]com
- eagleeyewhalewatching[.]com
- eastindiaassociates[.]com
- facehospitals[.]com
- faceprofessor[.]com
- factoryunlockexpress[.]com
- g3fashionsurat[.]com
- gajapatihealthcare[.]org
- galaxyroyale[.]com
- h2krealestate[.]com
- haffkineinstitute[.]org
- hailtosc[.]com
- iammywebsite[.]com
- iandimirissa[.]com
- iba-co[.]com
- jaiapparels[.]com
- jainyuvasanghmumbai[.]com
- jamindarspalace[.]com
- kadapa[.]xyz
- kakinada[.]xyz
- kalingagroups[.]com
- labelawines[.]com
- lakmejeans[.]com
- lakshadeep[.]xyz
- m4infoservices[.]com
- macacolca[.]com
- macgproductions[.]com
- nagercoil[.]xyz
- nagore[.]xyz
- nagpurbazarmatka[.]com
- objecteffect[.]com
- oddanchatram[.]xyz
- odishadocsynapse[.]com
- pakssd[.]com
- palani[.]xyz
- pallishree[.]org
- qhapaqcolca[.]com
- qlinkint[.]com
- qomqg[.]xyz
- raghuramagarbatti[.]com
- rajarshicollege[.]co[.]in
- rakutechnology[.]com
- saasindia[.]org
- sabarimala[.]xyz
- safafoodservice[.]com
- t20worldcup2016livescores[.]com
- t20worldcup2016prediction[.]com
- t20worldcup2016schedules[.]com
- ucreview[.]com
- udupi[.]xyz
- udyogasanjeevini[.]com
- valenciaivf[.]com
- vanamsei[.]com
- vandsclearing[.]com
- watersportssrilanka[.]com
- webbaystore[.]com
- webrutfilms[.]com
- xcapitalinvestments[.]org
- xdomain[.]xyz

- xdomains[.]xyz
- yadhavarmurasu[.]com
- yashvifilms[.]com
- yeomanexim[.]com
- zavaletcon[.]com
- zenzii[.]net
- zeroandcompany[.]com

Sample IP Addresses

- 103[.]224[.]182[.]250
- 104[.]21[.]10[.]78
- 15[.]197[.]148[.]33
- 172[.]67[.]129[.]145
- 185[.]53[.]179[.]128
- 2[.]57[.]91[.]91
- 3[.]33[.]130[.]190
- 34[.]195[.]60[.]139
- 92[.]112[.]198[.]161

Sample IP-Connected Domains

- ftp[.]birthday-stock[.]com
- germanshepherdss[.]com
- indiapet[.]in
- mysterydogrescue[.]org
- prayaasstudypoint[.]com

Sample String-Connected Domains

- 14north108east[.]au
- acento[.]agency
- acento[.]ai
- acento[.]app
- apacollege[.]ac[.]in
- apacollege[.]asia
- apacollege[.]co[.]uk
- arariacollege[.]ac[.]in
- arariacollege[.]com
- arariacollege[.]in
- assamchess[.]club
- assamchess[.]com
- assamchess[.]ml
- assessmentsonline[.]biz
- assessmentsonline[.]ca
- assessmentsonline[.]co[.]uk
- asspratapgarh[.]org
- basicsteeladelaide[.]au
- basicsteeladelaide[.]online
- behavioralhealthworkforce[.]com
- behavioralhealthworkforce[.]net
- blackeyetech[.]cn
- blackeyetech[.]co[.]in
- blackeyetech[.]com
- cisda[.]ca
- cisda[.]cn
- cisda[.]co[.]uk
- cosmicroots[.]ca
- cosmicroots[.]ch
- cosmicroots[.]co
- crdp[.]accountant
- crdp[.]app
- crdp[.]aquila[.]it
- dentalimplantkolkata[.]co[.]in
- englishproject[.]biz
- englishproject[.]cf
- englishproject[.]cl
- farsirestaurant[.]co[.]uk
- farsirestaurant[.]com
- farsirestaurant[.]de

- ffesp[.]com
- ffesp[.]com[.]br
- ffesp[.]info
- gardn[.]ai
- gardn[.]app
- gardn[.]at
- hueys[.]aquila[.]it
- hueys[.]ca
- hueys[.]cc
- i2apm[.]tk
- i2apm[.]ws
- jjiaa[.]ac[.]in
- jjiaa[.]com
- khariarautocollege[.]org
- kncs[.]accountant
- kncs[.]aquila[.]it
- kncs[.]arab
- motorhomeinsider[.]co[.]uk
- newsfirst[.]ai
- newsfirst[.]app
- newsfirst[.]asia
- nhcouncilonasd[.]info
- prakash-college[.]org
- reloadbar[.]ca
- reloadbar[.]co[.]uk
- reloadbar[.]com
- rmcautomotive[.]co[.]uk
- rmcautomotive[.]com
- rmcautomotive[.]nl
- rsc2018[.]com
- sacreblue[.]co[.]uk
- sacreblue[.]com
- sacreblue[.]me
- sahakarvidyamandir[.]co[.]in
- sahakarvidyamandir[.]com
- sahakarvidyamandir[.]net
- santgajananbhaktpariwar[.]com
- sdsuvrishikesh[.]ac[.]in
- seemasonline[.]com
- snvglobal[.]com
- snvglobal[.]edu[.]in
- snvglobal[.]net
- sonutradingcompany[.]com
- sonutradingcompany[.]in
- srikrnaiducollegeofnursing[.]com
- sta-bil[.]cn
- sta-bil[.]co[.]uk
- sta-bil[.]com
- staugustinesprimary[.]co[.]uk
- staugustinesprimary[.]com
- staugustinesprimary[.]com[.]ph
- synergistix[.]ai
- synergistix[.]ca
- synergistix[.]co
- taas[.]ac[.]cn
- taas[.]ac[.]th
- taas[.]ae
- taifujudo[.]ru
- thaitan[.]bid
- thaitan[.]biz
- thaitan[.]co[.]uk
- theclockdoc[.]biz
- theclockdoc[.]com
- theclockdoc[.]info
- thelifecarehospital[.]co[.]in
- thelifecarehospital[.]in
- timbabuild[.]co[.]uk
- timbabuild[.]com
- timbabuild[.]fr
- triplek[.]at
- triplek[.]biz
- triplek[.]ca
- twistarsgymnastics[.]co
- twistarsgymnastics[.]com
- twistarsgymnastics[.]in
- tyreworld[.]ae
- tyreworld[.]au
- tyreworld[.]cn
- vacuumpouch[.]co[.]uk
- vacuumpouch[.]com
- vacuumpouch[.]nom[.]za
- wyd2022[.]cn

- wyd2022[.]com
- wyd2022[.]org