Covert Channel Allegation: New Data Analysis Results

APRIL 2020

ankura

TABLE OF CONTENTS

INTRODUCTION

Kirkland & Ellis LLP, on behalf of Alfa-Bank JSC (Alfa-Bank), engaged Ankura Consulting Group to investigate and independently review newly identified evidence regarding the historical DNS records of servers alleged to have operated as a "secret server" back channel for Russian interest access to the Trump Organization, during the run-up to the 2016 U.S. Presidential election. In its recent review of the FBI's "Crossfire Hurricane" Investigation, the U.S. DOJ Inspector General (IG) stated: "The FBI investigated whether there were cyber links between the Trump Organization and Alfa Bank, but had concluded by early February 2017 that there were no such links."[1] While the IG's report is clear with respect to the FBI's finding on this issue, the report did not include the underlying technical evidence and analysis supporting this conclusion.

Ankura's detailed review of this matter, including newly identified data, sheds new light on the server allegations and includes findings supporting the FBI's conclusion debunking the alleged covert cyber links between Alfa-Bank and the Trump Organization. Additionally, Ankura's analysis of the DNS records and the overt nature of the DNS activity, suggest that a likely scenario is that threat actors may have artificially created DNS activity to make it appear as though a connection existed, for "discovery" later. If true, this would constitute a potential violation of various US federal laws.

This document summarizes the analysis that Ankura's Cyber Threat Analysis and Pursuit Team (CTAPT) undertook to assess the data provided by Kirkland & Ellis along with other information sourced by Ankura, including open source data, information obtained from various passive Domain Name System (DNS) data providers, threat intelligence analytics, and Internet Protocol (IP) registrations.

EXECUTIVE SUMMARY

OVERVIEW

For this investigation Ankura's CTAPT relied on recently identified SecurityTrails DNS records, DomainTools passive DNS databases, and PassiveTotal archives for inquiry into Cendyn, Internap, Listra, and Trump related entities. CTAPT concluded that the available DNS records do not provide any support whatsoever for the allegation of a "secret server" or covert "cyber links" between Alfa-Bank and the Trump Organization. The three sources of DNS records reflect that servers attributed to the Trump Organization were actually owned and operated by a hotel marketing related company named "Central Dynamics" (Cendyn). DNS records also show Cendyn was engaged in legitimate marketing activity for numerous global hotel chains, including Trump Hotels.

CTAPT's investigation discovered the Cendyn company and its servers have a long history of providing marketing solutions for hotel chains. Relevant here, the relationship between Cendyn and Trump Hotels goes back to at least 2009. We come to this understanding after considering multiple passive DNS sources, reviewing previous reporting, and assessing the original allegations as reported via multiple news outlets and blogs.

[1]https://www.justice.gov/storage/120919-examination.pdf

Cendyn's Trump Organization related marketing activity, including the activity alleged in 2016 to be associated with covert communications, was in fact hardly confidential. Available DNS records clearly attribute Cendyn activities to publicly resolvable domain names and IP address registrations to Trump related entities, with no effort to conceal the connection. Alfa-Bank's publicly attributable domains and IPs were also clearly in the DNS and IP registration records, which is the opposite of secret or covert. Additionally, CTAPT's research and analysis demonstrate it is possible -- indeed likely -- that threat actors may have conducted some inauthentic DNS activity to force a "connection" between Alfa-Bank and the Trump Organization, only to then later "discover" the connection.

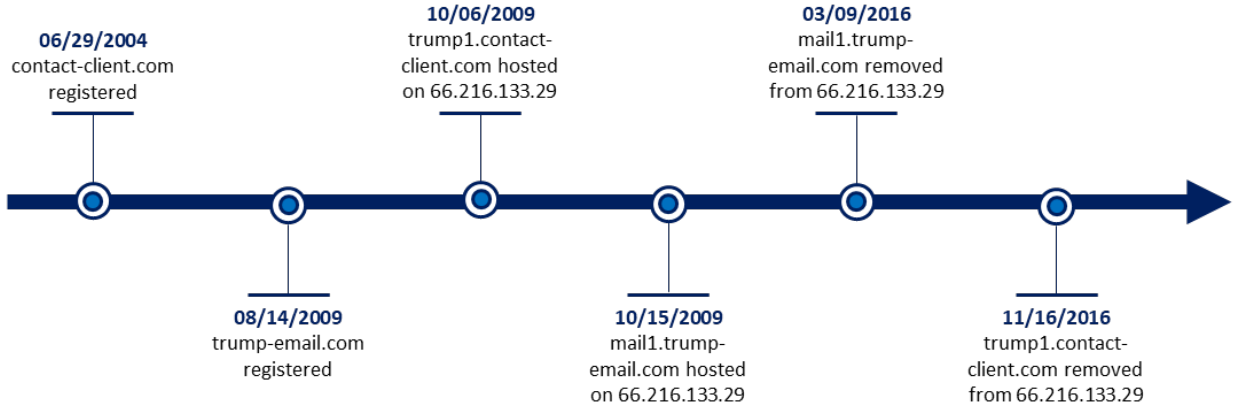
KEY CONSIDERATIONS

- The DNS query and response process typically involves an entity sending a domain query to a name server and, in return, receiving the hosting IP addresses where the domain of interest can be found. The DNS lookup process does not necessarily connect to the domain being translated to an IP address. The system originating the query may or may not use that delivered IP from the DNS process to then navigate to the IP address. DNS queries are not evidence of an actual communication taking place between a DNS requestor and the requested domain. One fallacy that is common is to assume the DNS lookup process connects with the domain of interest.

- The Sender Policy Framework (SPF) records for both trump-email[.]com and contact-client[.]com were configured in a way that a threat actor could send spoofed emails or inauthentic DNS queries masquerading as these domains to Alfa-Bank. As a result, this inauthentic activity could force Alfa-Bank servers to repeatedly query DNS records for both of these domains even if Alfa-Bank never received a legitimate marketing email.

MULTI-THREADED DNS ANALYSIS

TIMELINE



Historical DNS records were collected from a total of three (3) sources for DNS entries related to *trump-email.com and *contact-client.com. CTAPT analysis of multiple DNS sources, data available published online, and other research activities revealed no evidence that mail1.trump-email[.]com and trump1.contact-client[.]com were used by Alfa-Bank and the Trump Organization for covert communications.

SecurityTrails[2,3], Domaintools[4,5], and PassiveTotal[6,7] were queried for all available historical DNS data for both *.trump-email[.]com and *.contact-client[.]com domains. However, the historical DNS data retrieved from SecurityTrails did not match completely with what was retrieved from additional passive DNS providers, namely PassiveTotal and DomainTools. This issue highlights why attempting to make assertions using only one DNS source can lead to analysis errors. DNS record discrepancies exist because different passive DNS providers often leverage unique sensors and data points to collect and populate their DNS data. For example, PassiveTotal utilizes a variety of open and proprietary sensors and sources including 360CN, Emerging Threats, Farsight, Kaspersky, Mnemonic, OpenDNS, Pingly, and Virustotal:

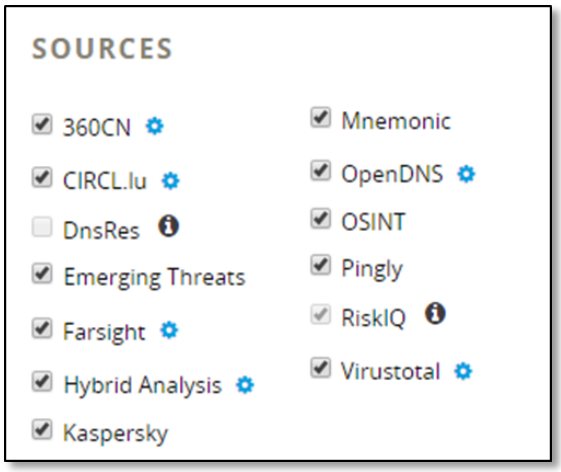


Figure 1: Screenshot showing PassiveTotal user options for passive DNS source

Mail1.trump-email[.]com

During review of the *.trump-email[.]com DNS artifacts, we noted an example of DNS discrepancies related to this domain's "A" record. A key data point missing from SecurityTrails, yet available from other sources, was that mail1.trump-email[.]com did, in fact, have an A record prior to 03/08/2017, the first date that SecurityTrails identified it as having an A record. PassiveTotal records show that this fully qualified domain name (FQDN) had an A record pointing to 66.216.133[.]29 beginning on 10/15/2009 and running through 03/09/2016. This fact illustrates the historical and overt use of Cendyn infrastructure for Trump Hotel related marketing. The PassiveTotal information listing the A record expiration in March 2016 also supports the timeline in the New Yorker article[8] that Cendyn was

[2]https://securitytrails.com/domain/trump-email.com/history/a
[3]https://securitytrails.com/domain/contact-client.com/history/a
[4]https://research.domaintools.com/iris/search/?q=trump-email.com
[5]https://research.domaintools.com/iris/search/?q=contact-client.com
[6]https://community.riskiq.com/search/trump-email.com
[7]https://community.riskiq.com/search/contact-client.com
[8]https://www.newyorker.com/magazine/2018/10/15/was-there-a-connection-between-a-russian-bank-and-the-trump-campaign

no longer used by the Trump Organization as a marketing provider after March 2016. However, this new observation challenges the same New Yorker article's claim that mail1.trump-email[.]com was removed from 66.216.133.29 on or about September 23, 2016, after the story surfaced in the media. The article states: "The Trump domain vanished from the Web on the morning of Friday, September 23rd, two days after the Times presented its data to B.G.R., Alfa Bank's lobbyists in Washington, but before it called Trump or Cendyn." The Trump related domain did not actually vanish, after the Times presented its data, but was changed months before. According to multiple passive DNS sources, the domain actually "vanished" from the web on March 9, 2016. The change was more likely done in accordance with marketing activity, as the New Yorker pointed out, because Cendyn was no longer used by the Trump organization in March 2016. Cendyn corroborated this when it told CNN that it "stopped sending e-mails for the Trump Organization in March 2016, before the peculiar activity began."[9]

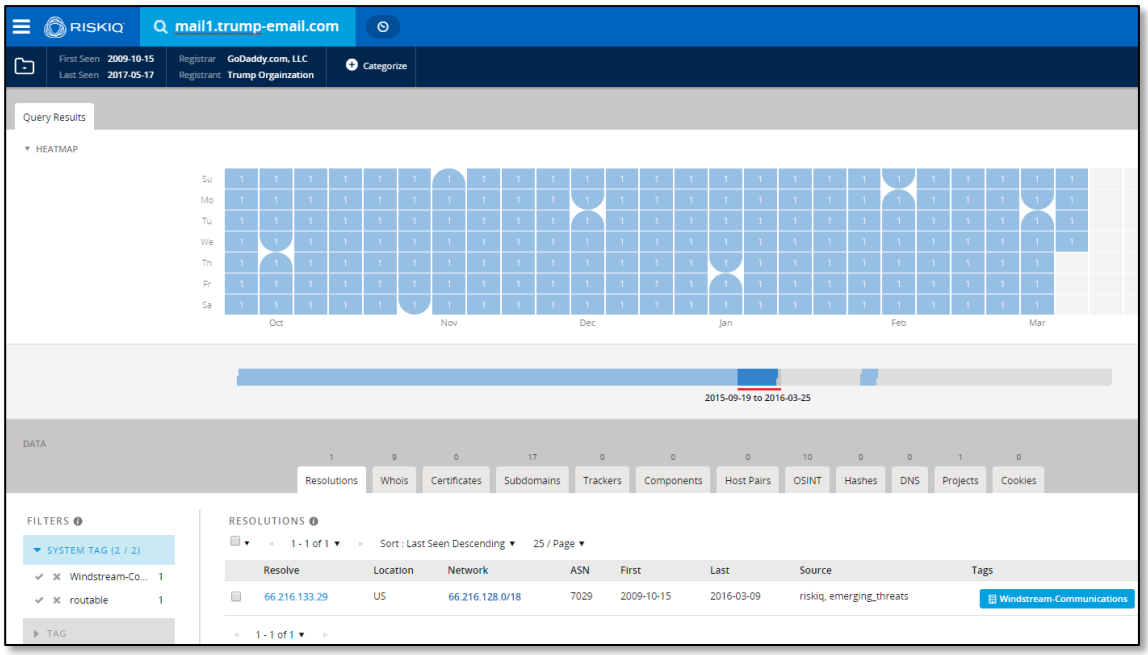


Figure 2: Screenshot from PassiveTotal showing A record for mail1-trump-email[.]com

Additionally, DomainTools passive DNS records show different dates pertaining to A records for mail1.trump-email[.]com. DomainTools queries different sources and sensors for DNS records. DomainTools passive DNS history shows the following records:[10]

Query	Type	Source	Response	First Seen	Last Seen
mail1.trump-email.com	A	B	66.216.133.29	2014-12-04, 20:07	2016-09-13, 01:47
mail1.trump-email.com	A	A	66.216.133.29	2014-12-04, 19:54	2016-09-23, 13:45
mail1.trump-email.com	A	D	66.216.133.29	2010-07-02, 19:02	2016-09-13, 01:47
mail1.trump-email.com	A	D	66.216.133.29	2017-03-08, 04:32	2017-07-16, 20:53

[9]https://www.newyorker.com/magazine/2018/10/15/was-there-a-connection-between-a-russian-bank-and-the-trump-campaign

[10]https://research.domaintools.com/iris/investigations/464456/search/dc3e5548-e445-4756-ba19-9397bcfc816e/fb0a15ed-ea6d-440e-9d1f-29aa59a338c4

The records above demonstrate the challenges of relying on one source for DNS analysis. If the original "researchers" and news media outlets used a single point of collections or DNS historical data, it is likely they missed additional clarifying context, or chose the data source that best met the intended message.

Trump1.contact-client[.]com

Another key data point to consider is that one of the DNS providers did not return any records for the trump1.contact-client[.]com domain.[11] If analysis relied solely on this source, the results would reflect that an A record for this FQDN never existed, as potentially seen in the New Yorker article[12] which stated that trump1.contact-client[.]com "does not appear to have been previously active." The article states: “On the night of Tuesday, September 27th, ten minutes after the bank made its last failed attempt, it looked up the domain name trump1.contact-client.com—which was, it turned out, another route to the same Trump server. The alternative domain name does not appear to have been previously active; no one has produced an e-mail sent from it. So how did Alfa find it?” In contrast, PassiveTotal records show that trump1.contact-client[.]com did have an A record pointing to 66.216.133[.]29 from 10/06/2009 through 11/16/2016. Both mail1.trump-email[.]com and trump1.contact-client[.]com had the same A record IP address over most of the same time span[13] and answers the question about how an Alfa-Bank DNS request “found it.”

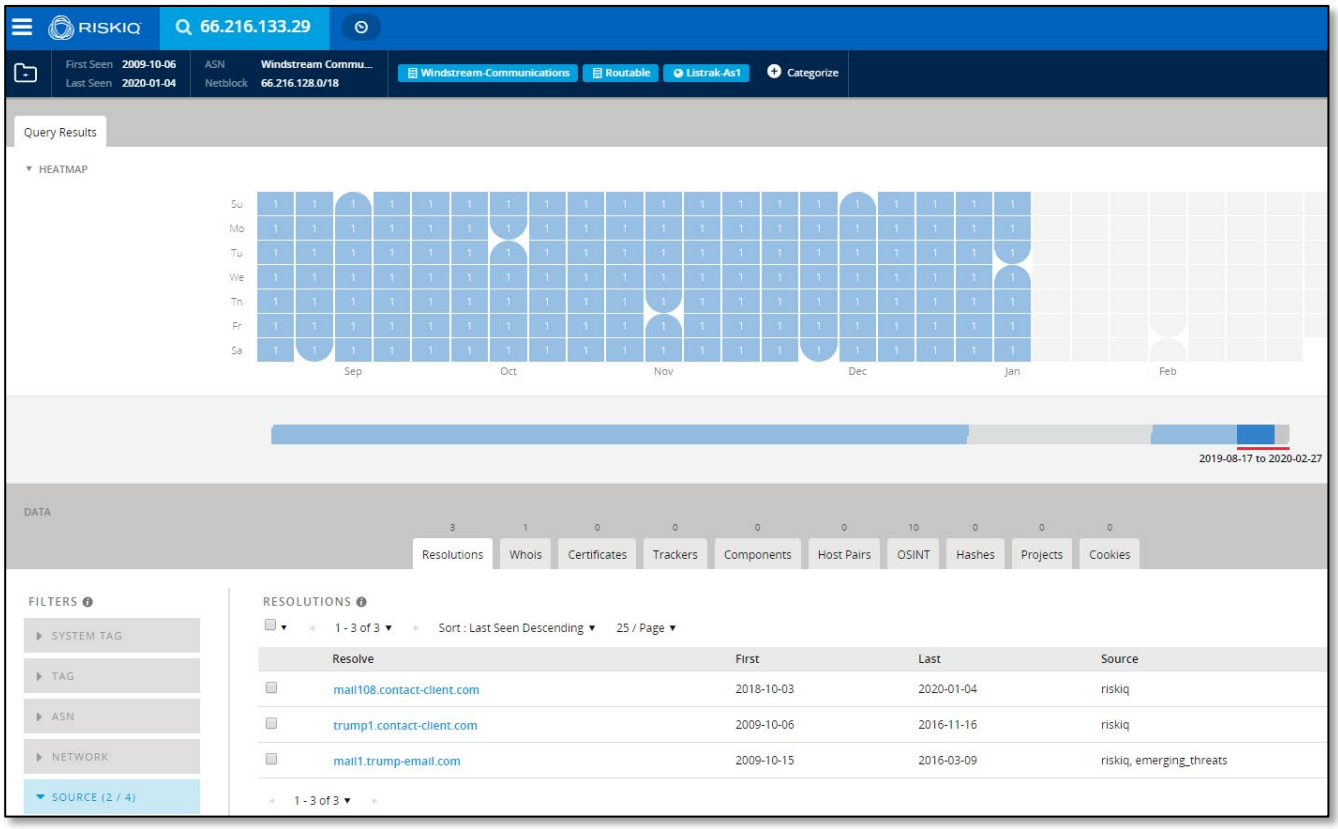


Figure 3: Screenshot from PassiveTotal showing overlap between trump1.contact-client[.]com & mail1.trump-email[.]com

[11] https://securitytrails.com/domain/contact-client.com/history/a

[12]https://www.newyorker.com/magazine/2018/10/15/was-there-a-connection-between-a-russian-bank-and-the-trump-campaign

[13] https://community.riskiq.com/search/66.216.133.29

MARKETING INFRASTRUCTURE DETAILS

CTAPT's review of the publicly available SecurityTrails[14] DNS records concluded that Cendyn server DNS configurations were consistent with marketing infrastructure for the hotel industry, including Trump Hotels. However, SecurityTrails doesn't tell as complete a picture as DomainTools and PassiveTotal both do. One example of SecurityTrails' lack of resolution is where additional sources prove Cendyn was operating in a marketing capacity for the Trump Organization as far back as 2009, countering key claims of some of the initial DNS analysis in the press. For example, mail1.trump-email[.]com and trump1.contact-client[.]com, both registered by Cendyn and both hosted on the same Listrak IP address beginning in 2009 through 2016, were according to DNS records, reachable for nearly seven (7) years. This type of static activity is typically employed by marketing entities to avoid interruptions and misconfiguration impacts when emails are marked as spam or websites become unreachable.

Cendyn company (Central Dynamics) infrastructure and configuration management played key roles for both trump-email[.]com and contact-client[.]com. Cendyn is reported to be a services and software company focused on serving the global hospitality industry. According to their website, they serve clients in 143 different countries and have delivered over 1.5 billion communications on behalf of their customers every year.[15]

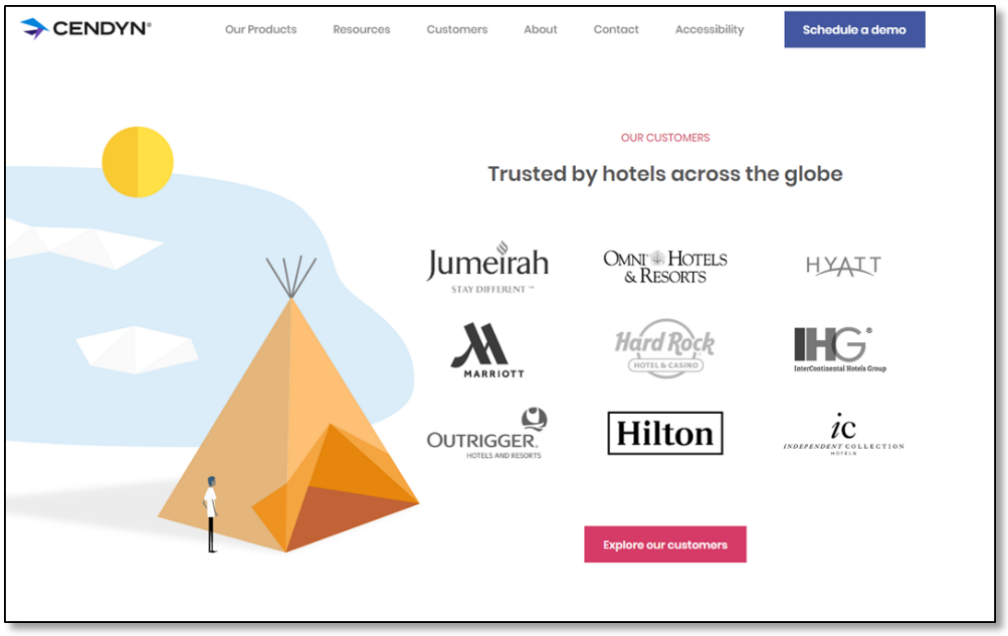


Figure 4: Screenshot of Cendyn's website listing some of their hospitality clients.

CTAPT review of DomainTools' historical WHOIS records shows that both trump-email[.]com and contact-client[.]com domains were registered to and owned by Cendyn related entities into 2016. Specifically, Trump1.contact-client[.]com was active and discoverable before and during the time that the alleged "secret" server was in operation.

[14]https://securitytrails.com/domain/contact-client.com/history/a
[15]https://www.cendyn.com/company/

	2016-02-27		2016-07-01
1	Domain Name: CONTACT-CLIENT.COM	1	Domain Name: CONTACT-CLIENT.COM
2	Registry Domain ID: 123709352_DOMAIN_COM-VRSN	2	Registry Domain ID: 123709352_DOMAIN_COM-VRSN
3	Registrar WHOIS Server: whois.godaddy.com	3	Registrar WHOIS Server: whois.godaddy.com
4	Registrar URL: http://www.godaddy.com	4	Registrar URL: http://www.godaddy.com
5	Update Date: 2011-07-18T04:28:07Z	5	Update Date: 2011-07-18T04:28:07Z
6	Creation Date: 2004-06-29T14:41:05Z	6	Creation Date: 2004-06-29T14:41:05Z
7	Registrar Registration Expiration Date: 2021-06-28T14:41:05Z	7	Registrar Registration Expiration Date: 2021-06-28T14:41:05Z
8	Registrar: GoDaddy.com, LLC	8	Registrar: GoDaddy.com, LLC
9	Registrar IANA ID: 146	9	Registrar IANA ID: 146
10	Registrar Abuse Contact Email: abuse@godaddy.com	10	Registrar Abuse Contact Email: abuse@godaddy.com
11	Registrar Abuse Contact Phone: +1.4806242505	11	Registrar Abuse Contact Phone: +1.4806242505
12	Domain Status: clientTransferProhibited http://www.icann.org/epp#clientTransferProhibited	12	Domain Status: clientTransferProhibited http://www.icann.org/epp#clientTransferProhibited
13	Domain Status: clientUpdateProhibited http://www.icann.org/epp#clientUpdateProhibited	13	Domain Status: clientUpdateProhibited http://www.icann.org/epp#clientUpdateProhibited
14	Domain Status: clientRenewProhibited http://www.icann.org/epp#clientRenewProhibited	14	Domain Status: clientRenewProhibited http://www.icann.org/epp#clientRenewProhibited
15	Domain Status: clientDeleteProhibited http://www.icann.org/epp#clientDeleteProhibited	15	Domain Status: clientDeleteProhibited http://www.icann.org/epp#clientDeleteProhibited
16	Registry Registrant ID: Not Available From Registry	16	Registry Registrant ID: Not Available From Registry
17	Registrant Name: Charles Deyo	17	Registrant Name: Charles Deyo
18	Registrant Organization:	18	Registrant Organization:
19	Registrant Street: 1515 N. Federal Hwy	19	Registrant Street: 1515 N. Federal Hwy
20	Registrant City: Boca Raton	20	Registrant City: Boca Raton
21	Registrant State/Province: Florida	21	Registrant State/Province: Florida
22	Registrant Postal Code: 33432	22	Registrant Postal Code: 33432
23	Registrant Country: US	23	Registrant Country: US
24	Registrant Phone:	24	Registrant Phone:
25	Registrant Phone Ext:	25	Registrant Phone Ext:
26	Registrant Fax:	26	Registrant Fax:
27	Registrant Fax Ext:	27	Registrant Fax Ext:
28	Registrant Email: nocontactsfound@secureserver.net	28	Registrant Email: nocontactsfound@secureserver.net
29	Registry Admin ID: Not Available From Registry	29	Registry Admin ID: Not Available From Registry
30	Admin Name: Charles Deyo	30	Admin Name: Charles Deyo
31	Admin Organization:	31	Admin Organization:
32	Admin Street: 1515 N. Federal Hwy	32	Admin Street: 1515 N. Federal Hwy
33	Admin City: Boca Raton	33	Admin City: Boca Raton
34	Admin State/Province: Florida	34	Admin State/Province: Florida
35	Admin Postal Code: 33432	35	Admin Postal Code: 33432
36	Admin Country: US	36	Admin Country: US
37	Admin Phone: 561-555-3143	37	Admin Phone: 561-555-3143
38	Admin Phone Ext:	38	Admin Phone Ext:
39	Admin Fax:	39	Admin Fax:
40	Admin Fax Ext:	40	Admin Fax Ext:
41	Admin Email: emcmullin@cendyn.com	41	Admin Email: emcmullin@cendyn.com
42	Registry Tech ID: Not Available From Registry	42	Registry Tech ID: Not Available From Registry
43	Tech Name: Charles Deyo	43	Tech Name: Charles Deyo
44	Tech Organization:	44	Tech Organization:
45	Tech Street: 1515 N. Federal Hwy	45	Tech Street: 1515 N. Federal Hwy
46	Tech City: Boca Raton	46	Tech City: Boca Raton
47	Tech State/Province: Florida	47	Tech State/Province: Florida
48	Tech Postal Code: 33432	48	Tech Postal Code: 33432

Figure 5: Screenshot of historical WHOIS record history for contact-client[.]com[16]

Figure 5 shows two (2) side by side WHOIS records for contact-client[.]com, dated 02/27/2016 and 07/01/2016. These dates were chosen because the earlier date is before the alleged "secret" server activity began and the later date is after the alleged activity commenced. No ownership changes were documented during this activity or at any other time during the domain's existence.

[16]https://research.domaintools.com/research/whois-history/search/?q=contact-client.com#changes

	2016-05-03		2016-06-29
1	Domain Name: TRUMP-EMAIL.COM	1	Domain Name: TRUMP-EMAIL.COM
2	Registry Domain ID: 1565681481_DOMAIN_COM-VRSN	2	Registry Domain ID: 1565681481_DOMAIN_COM-VRSN
3	Registrar WHOIS Server: whois.godaddy.com	3	Registrar WHOIS Server: whois.godaddy.com
4	Registrar URL: http://www.godaddy.com	4	Registrar URL: http://www.godaddy.com
5	Update Date: 2015-06-26T17:27:59Z	5	Update Date: 2016-06-29T14:27:44Z
6	Creation Date: 2009-08-14T20:06:37Z	6	Creation Date: 2009-08-14T20:06:37Z
7	Registrar Registration Expiration Date: 2016-07-01T03:59:59Z	7	Registrar Registration Expiration Date: 2017-07-01T03:59:59Z
8	Registrar: GoDaddy.com, LLC	8	Registrar: GoDaddy.com, LLC
9	Registrar IANA ID: 146	9	Registrar IANA ID: 146
10	Registrar Abuse Contact Email: abuse@godaddy.com	10	Registrar Abuse Contact Email: abuse@godaddy.com
11	Registrar Abuse Contact Phone: +1.4806242505	11	Registrar Abuse Contact Phone: +1.4806242505
12	Domain Status: clientTransferProhibited http://www.icann.org/epp#clientTransferProhibited	12	Domain Status: clientTransferProhibited http://www.icann.org/epp#clientTransferProhibited
13	Domain Status: clientUpdateProhibited http://www.icann.org/epp#clientUpdateProhibited	13	Domain Status: clientUpdateProhibited http://www.icann.org/epp#clientUpdateProhibited
14	Domain Status: clientRenewProhibited http://www.icann.org/epp#clientRenewProhibited	14	Domain Status: clientRenewProhibited http://www.icann.org/epp#clientRenewProhibited
15	Domain Status: clientDeleteProhibited http://www.icann.org/epp#clientDeleteProhibited	15	Domain Status: clientDeleteProhibited http://www.icann.org/epp#clientDeleteProhibited
16	Registry Registrant ID: Not Available From Registry	16	Registry Registrant ID: Not Available From Registry
17	Registrant Name: Trump Orgainzation	17	Registrant Name: Trump Orgainzation
18	Registrant Organization: Trump Orgainzation	18	Registrant Organization: Trump Orgainzation
19	Registrant Street: 725 Fifth Avenue	19	Registrant Street: 725 Fifth Avenue
20	Registrant City: New York	20	Registrant City: New York
21	Registrant State/Province: New York	21	Registrant State/Province: New York
22	Registrant Postal Code: 10022	22	Registrant Postal Code: 10022
23	Registrant Country: US	23	Registrant Country: US
24	Registrant Phone: +1.2128322000	24	Registrant Phone: +1.2128322000
25	Registrant Phone Ext:	25	Registrant Phone Ext:
26	Registrant Fax:	26	Registrant Fax:
27	Registrant Fax Ext:	27	Registrant Fax Ext:
28	Registrant Email: emcmullin@cendyn.com	28	Registrant Email: emcmullin@cendyn.com
29	Registry Admin ID: Not Available From Registry	29	Registry Admin ID: Not Available From Registry
30	Admin Name: Emily McMullin	30	Admin Name: Emily McMullin
31	Admin Organization: Cendyn	31	Admin Organization: Cendyn
32	Admin Street: 1515 N Federal Highway	32	Admin Street: 1515 N Federal Highway
33	Admin Street: Suite 419	33	Admin Street: Suite 419
34	Admin City: Boca Raton	34	Admin City: Boca Raton
35	Admin State/Province: Florida	35	Admin State/Province: Florida
36	Admin Postal Code: 33432	36	Admin Postal Code: 33432
37	Admin Country: US	37	Admin Country: US
38	Admin Phone: (561) 750-3173	38	Admin Phone: (561) 750-3173
39	Admin Phone Ext:	39	Admin Phone Ext:
40	Admin Fax:	40	Admin Fax:
41	Admin Fax Ext:	41	Admin Fax Ext:
42	Admin Email: ssl.admin@cendyn.com	42	Admin Email: ssl.admin@cendyn.com
43	Registry Tech ID: Not Available From Registry	43	Registry Tech ID: Not Available From Registry
44	Tech Name: Emily McMullin	44	Tech Name: Emily McMullin
45	Tech Organization: Cendyn	45	Tech Organization: Cendyn
46	Tech Street: 1515 N. Federal Highway	46	Tech Street: 1515 N. Federal Highway
47	Tech Street: Suite 419	47	Tech Street: Suite 419
48	Tech City: Boca Raton	48	Tech City: Boca Raton
49	Tech State/Province: Florida	49	Tech State/Province: Florida

Figure 6: Screenshot showing historical WHOIS history record for trump-email[.]com[17]

The screenshot above shows two (2) side by side WHOIS records for trump-email[.]com, dated 05/03/2016 and 06/29/2016. These dates were chosen because the earlier date is before the alleged "secret" server activity began and the later date was after the alleged activity commenced. The only change showing is an extension of domain ownership for an additional year. This is likely the result of Cendyn extending the domain ownership on behalf of the Trump Organization for another year. As seen in the screenshot below, an ownership change was made on 03/08/2017, which shows that the Trump Organization took full control of the domain.[18]

[17]https://research.domaintools.com/research/whois-history/search/?q=trump-email.com
[18]https://research.domaintools.com/research/whois-history/search/?q=trump-email.com#changes

	2017-03-06		2017-03-08
1	Domain Name: TRUMP-EMAIL.COM	1	Domain Name: TRUMP-EMAIL.COM
2	Registry Domain ID: 1565681481_DOMAIN_COM-VRSN	2	Registry Domain ID: 1565681481_DOMAIN_COM-VRSN
3	Registrar WHOIS Server: whois.godaddy.com	3	Registrar WHOIS Server: whois.godaddy.com
4	Registrar URL: http://www.godaddy.com	4	Registrar URL: http://www.godaddy.com
5	Update Date: 2016-06-29T14:27:44Z	5	Update Date: 2016-06-29T14:27:44Z
6	Creation Date: 2009-08-14T20:06:37Z	6	Creation Date: 2009-08-14T20:06:37Z
7	Registrar Registration Expiration Date: 2017-07-01T03:59:59Z	7	Registrar Registration Expiration Date: 2017-07-01T03:59:59Z
8	Registrar: GoDaddy.com, LLC	8	Registrar: GoDaddy.com, LLC
9	Registrar IANA ID: 146	9	Registrar IANA ID: 146
10	Registrar Abuse Contact Email: abuse@godaddy.com	10	Registrar Abuse Contact Email: abuse@godaddy.com
11	Registrar Abuse Contact Phone: +1.4806242505	11	Registrar Abuse Contact Phone: +1.4806242505
12	Domain Status: clientTransferProhibited http://www.icann.org/epp#clientTransferProhibited	12	Domain Status: clientTransferProhibited http://www.icann.org/epp#clientTransferProhibited
13	Domain Status: clientUpdateProhibited http://www.icann.org/epp#clientUpdateProhibited	13	Domain Status: clientUpdateProhibited http://www.icann.org/epp#clientUpdateProhibited
14	Domain Status: clientRenewProhibited http://www.icann.org/epp#clientRenewProhibited	14	Domain Status: clientRenewProhibited http://www.icann.org/epp#clientRenewProhibited
15	Domain Status: clientDeleteProhibited http://www.icann.org/epp#clientDeleteProhibited	15	Domain Status: clientDeleteProhibited http://www.icann.org/epp#clientDeleteProhibited
16	Registry Registrant ID: Not Available From Registry	16	Registry Registrant ID: Not Available From Registry
17	Registrant Name: Trump Orgainzation	17	Registrant Name: Trump Orgainzation
18	Registrant Organization: Trump Orgainzation	18	Registrant Organization: Trump Orgainzation
19	Registrant Street: 725 Fifth Avenue	19	Registrant Street: 725 Fifth Avenue
20	Registrant City: New York	20	Registrant City: New York
21	Registrant State/Province: New York	21	Registrant State/Province: New York
22	Registrant Postal Code: 10022	22	Registrant Postal Code: 10022
23	Registrant Country: US	23	Registrant Country: US
24	Registrant Phone: +1.2128322000	24	Registrant Phone: +1.2128322000
25	Registrant Phone Ext:	25	Registrant Phone Ext:
26	Registrant Fax:	26	Registrant Fax:
27	Registrant Fax Ext:	27	Registrant Fax Ext:
28	Registrant Email: emcmullin@cendyn.com	28	Registrant Email: generalcounsel@trumporg.com
29	Registry Admin ID: Not Available From Registry	29	Registry Admin ID: Not Available From Registry
30	Admin Name: Emily McMullin	30	Admin Name: The Trump Organization
31	Admin Organization: Cendyn	31	Admin Organization: The Trump Organization
32	Admin Street: 1515 N Federal Highway	32	Admin Street: 725 Fifth Avenue
33	Admin Street: Suite 419	33	Admin City: New York
34	Admin City: Boca Raton	34	Admin State/Province: New York
35	Admin State/Province: Florida	35	Admin Postal Code: 10022
36	Admin Postal Code: 33432		
37	Admin Country: US	36	Admin Country: US
38	Admin Phone: (561) 750-3173	37	Admin Phone: +1.2128322000

Figure 7: Screenshot showing trump-email[.]com ownership change

Analysis of both Trump associated domains during the time period that the alleged "secret" servers were communicating with one another shows that both domains utilized Cendyn name servers. This means that any DNS query would ultimately be handled by one of those name servers. Since Cendyn registered these domains and pointed them at Cendyn name servers for resolution requests, only entities with specialized and non-public access to DNS infrastructure would know that Alfa-Bank and Spectrum Health were sending repeated DNS queries to Trump associated domains, making this tactic a very improbable communications channel.

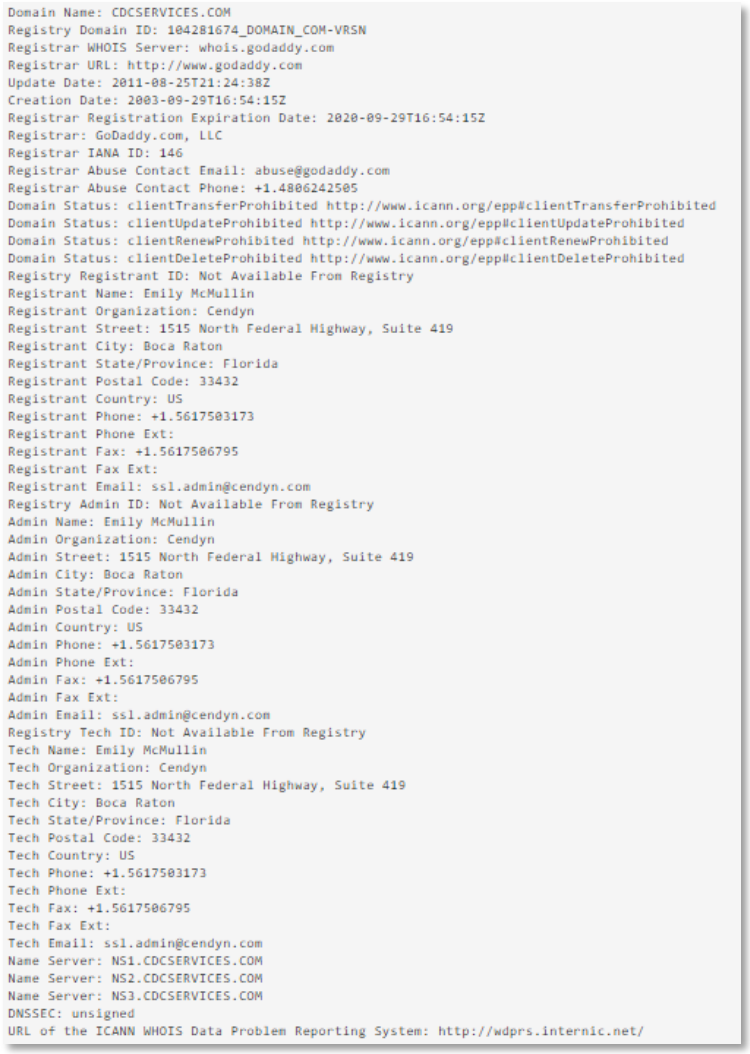
CTAPT performed analysis on the MX and SPF TXT DNS records collected from several passive DNS providers for both trump-email[.]com and contact-client[.]com:

Trump-email[.]com

The following MX DNS records for trump-email[.]com were examined by Ankura:

Source	Mail Servers	Organization	First Seen	Last Seen
Domain Tools	incoming.cdcservices[.]com	Central Dynamics	2015-04-27	2016-09-23
SecurityTrails	incoming.cdcservices[.]com	Central Dynamics	2011-11-14	2016-09-24

These MX DNS records indicate that all incoming emails to the trump-email[.]com domain would be routed to incoming.cdcservices[.]com. According to historical WHOIS records, cdcservices[.]com was registered by Cendyn and used the same Cendyn name servers as trump-email[.]com and contact-client[.]com.



```
Domain Name: CDCSERVICES.COM
Registry Domain ID: 104281674_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.godaddy.com
Registrar URL: http://www.godaddy.com
Update Date: 2011-08-25T21:24:38Z
Creation Date: 2003-09-29T16:54:15Z
Registrar Registration Expiration Date: 2020-09-29T16:54:15Z
Registrar: GoDaddy.com, LLC
Registrar IANA ID: 146
Registrar Abuse Contact Email: abuse@godaddy.com
Registrar Abuse Contact Phone: +1.4806242505
Domain Status: clientTransferProhibited http://www.icann.org/epp#clientTransferProhibited
Domain Status: clientUpdateProhibited http://www.icann.org/epp#clientUpdateProhibited
Domain Status: clientRenewProhibited http://www.icann.org/epp#clientRenewProhibited
Domain Status: clientDeleteProhibited http://www.icann.org/epp#clientDeleteProhibited
Registry Registrant ID: Not Available From Registry
Registrant Name: Emily McMullin
Registrant Organization: Cendyn
Registrant Street: 1515 North Federal Highway, Suite 419
Registrant City: Boca Raton
Registrant State/Province: Florida
Registrant Postal Code: 33432
Registrant Country: US
Registrant Phone: +1.5617503173
Registrant Phone Ext:
Registrant Fax: +1.5617506795
Registrant Fax Ext:
Registrant Email: ssl.admin@cendyn.com
Registry Admin ID: Not Available From Registry
Admin Name: Emily McMullin
Admin Organization: Cendyn
Admin Street: 1515 North Federal Highway, Suite 419
Admin City: Boca Raton
Admin State/Province: Florida
Admin Postal Code: 33432
Admin Country: US
Admin Phone: +1.5617503173
Admin Phone Ext:
Admin Fax: +1.5617506795
Admin Fax Ext:
Admin Email: ssl.admin@cendyn.com
Registry Tech ID: Not Available From Registry
Tech Name: Emily McMullin
Tech Organization: Cendyn
Tech Street: 1515 North Federal Highway, Suite 419
Tech City: Boca Raton
Tech State/Province: Florida
Tech Postal Code: 33432
Tech Country: US
Tech Phone: +1.5617503173
Tech Phone Ext:
Tech Fax: +1.5617506795
Tech Fax Ext:
Tech Email: ssl.admin@cendyn.com
Name Server: NS1.CDCSERVICES.COM
Name Server: NS2.CDCSERVICES.COM
Name Server: NS3.CDCSERVICES.COM
DNSSEC: unsigned
URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
```

Figure 8: Screenshot showing historical WHOIS record from DomainTools[19]

The MX DNS records show that Cendyn controlled the routing for all inbound emails sent to *.trump-email[.]com. This type of configuration adheres to how a legitimate marketing organization would construct their infrastructure. Essentially, any email sent back to *.trump-email.com would be routed through Cendyn infrastructure.

The following SPF TXT DNS records for trump-email[.]com were examined by Ankura:

[19]https://research.domaintools.com/research/whois-history/search/?q=cdcservices.com

trump-email.com	TXT	A	1	ï¿½v=spf1,ip4:198.91.42.0/23,ip4:64.135.26.0/24,ip4:64.95.241.0/24,ip4:206.191.130.0/24,ip4:63.251.151.0/24,ip4:69.25.15.0/24,mx,–all	2016-02-11, 01:08	2016-09-23, 13:48
trump-email.com	TXT	A	1	"Internet,Solution,from,Cendyn.com	2015-12-03, 14:18	2016-01-31, 12:29
trump-email.com	TXT	D	10	"Internet,Solution,from,Cendyn.com."	2014-11-14, 11:17	2016-09-23, 12:59
trump-email.com	TXT	D	10	"v=spf1,ip4:198.91.42.0/23,ip4:64.135.26.0/24,ip4:64.95.241.0/24,ip4:206.191.130.0/24,ip4:63.251.151.0/24,ip4:69.25.15.0/24,mx,–all"	2014-11-14, 11:17	2016-09-23, 12:59

Figure 9: Screenshot showing relevant TXT records extracted from DomainTools[20]

A SPF TXT record is an email authentication technique that is typically used to mitigate email spoofing by specifying which hostnames, IP addresses, and/or IP ranges are permitted to send emails on behalf of a domain. The SPF TXT record captured in the screenshot above will be broken down below to better understand it.

- "v=spf1"
  - This identifies the TXT record as an SPF string. It also indicates the version of SPF being used.
- "ip4:198.91.42.0/23,ip4:64.135.26.0/24,ip4:64.95.241.0/24,ip4:206.191.130.0/24,ip4:63.251.151.0/24,ip4:69.25.15.0/24"
  - This identifies the IP ranges that are authorized to send emails on behalf of trump-email[.]com. When an email from *.trump-email[.]com is delivered to an email server, that server will retrieve the TXT record from trump-email[.]com to examine the SPF record. If the IP address used to send the email from *.trump-email[.]com is in the SPF record, the email should be tagged as genuine and not SPAM. Analysis of these IP address ranges indicate nothing more than typical marketing activity. A breakdown of ownership for these IP address ranges are below. An evaluation of how these IP addresses are currently being utilized can be found in Appendix A.
- "mx"
  - Any domain that hosts email has at least one MX record. These MX records identify which email servers should be used when relaying email. By including "mx" in the TXT record, the servers identified in the MX DNS record for trump-email[.]com are automatically approved and avoids having to re-list them in the TXT record.
- "~all"
  - This indicates that emails sent from an IP address not included in the SPF record should be accepted by the recipient marked as an SPF failure.

The SPF records demonstrate that for the trump-email[.c]om domain, any email sent using the trump-email[.]com domain and originating from one of the IP ranges or MX domains included above are to be considered legitimate by the recipient of the email. However, this SPF configuration also allows for a spoofed email to successfully masquerade as an email from trump-email[.]com. The "~all" flag, also known as a "soft fail"[21] indicates that if a recipient receives an email from trump-email[.]com but it originates from an IP address not included in the SPF record, the recipient should identify it as spam but allow it at their discretion. This option could allow a marketing organization to keep sending legitimate marketing emails in case of a DNS configuration error. It could also allow an attacker to bypass spam identification and deliver mail into an organization. That email could then have links in the body of the message, that could also force DNS lookups if delivered.

The following IP ranges (Figure 10) were explicitly allocated to Cendyn and/or host Cendyn related domains:

[20]https://research.domaintools.com/iris/investigations/463262/search/72fe1f25-d27f-4078-979b-e41c59702f54/7b459b7b-3581-43d6-b2f0-d866198e0d90

[21]https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/how-office-365-uses-spf-to-prevent-spoofing?view=o365-worldwide

IP Range	Ownership Record	Purpose
198.91.42.0/23	Central Dynamics 980 N Federal Hwy Suite 200 Boca Raton, FL 33432	Cendyn has helped hotels around the world drive marketing and sales for over 20 years.[22]
64.135.26.0/24	BroadbandONE, Inc 3500 NW Boca Raton BLVD Boca Raton, FL 33431	Broadband One is an Internet Service Provider located in Boca Raton, Florida.[23]
64.95.241.0/24	Internap Corporation 50 NE 9th Street Miami, FL 33030	Internap (INAP) is a publicly traded internet service provider. According to WHOIS records, this net range is allocated to private INAP customers.
206.191.130.0/24	Internap Corporation 50 NE 9th Street Miami, FL 33030	Internap (INAP) is a publicly traded internet service provider. According to WHOIS records, this net range is allocated to private INAP customers.
63.251.151.0/24	Internap Corporation 50 NE 9th Street Miami, FL 33030	Internap (INAP) is a publicly traded internet service provider. According to WHOIS records, this net range is allocated to private INAP customers.
69.25.15.0/24	Internap Corporation 50 NE 9th Street Miami, FL 33030	Internap (INAP) is a publicly traded internet service provider. According to WHOIS records, this net range is allocated to private INAP customers.

Figure 10: Ownership of IP ranges identified in TXT record for trump-email[.]com

Analysis discovered many of the domains pertain to large hotel or hospitality related companies. Please refer to Appendix A for a list of domains found to be associated with the IPs in Figure 10.

Contact-client[.]com

The following MX DNS records for contact-client[.]com were examined by Ankura:

Source	Mail Servers	Organization	First Seen	Last Seen
PassiveTotal	incoming.cdcservices[.]com	Central Dynamics	2011-11-15	2020-02-27
SecurityTrails	incoming.cdcservices[.]com	Central Dynamics	2011-11-14	2017-05-25
SecurityTrails	incoming.cdcservices[.]com	Central Dynamics	2017-05-25	2020-02-27

These MX DNS records indicate that all incoming emails to the contact-client[.]com domain would be routed to incoming.cdcservices[.]com, the same email server that handled incoming emails for trump-email[.]com. This type of configuration adheres to how a legitimate marketing organization would construct their infrastructure. Essentially, any email sent back to *.contact-client.com would be routed through Cendyn infrastructure.

The following is the SPF TXT record for contact-client[.]com:

[22]https://www.cendyn.com/company/

[23]https://www.linkedin.com/company/broadband-one-inc.

TXT Values	First Seen	Last Seen	Duration Seen
v=spf1 include:spf.contact-client.com -all google-site-verification=6hJrhTYNB12EL88q-Jla9PsavgOMgmLnH4gAEF7FAbs	2017-05-11 (2 years ago)	2020-02-26 (19 hours ago)	2 years
v=spf1 include:spf.contact-client.com ~all google-site-verification=6hJrhTYNB12EL88q-Jla9PsavgOMgmLnH4gAEF7FAbs	2016-06-28 (3 years ago)	2017-05-11 (2 years ago)	10 months
v=spf1 ip4:198.91.42.0/23 ip4:64.135.26.0/24 mx include:listrak.com include:sendgrid.net include:spf.maropost.com ~all google-site-verification=6hJrhTYNB12EL88q-Jla9PsavgOMgmLnH4gAEF7FAbs	2015-11-06 (4 years ago)	2016-06-28 (3 years ago)	7 months

Figure 11: Screenshot showing relevant SPF records for contact-client[.]com extracted from SecurityTrails

The various records are detailed below for clarity:

- "v=spf1"
  - This identifies the TXT record as an SPF string. It also indicates the version of SPF being used.
- "ip4:198.91.42.0/23,ip4:64.135.26.0/24"
  - This identifies the IP ranges that are authorized to send emails on behalf of trump-email[.]com. When an email from *.contact-client[.]com is delivered to an email server, that server will retrieve the TXT record from contact-client[.]com to examine the SPF record. If the IP address used to send the email from *.contact-client[.]com is in the SPF record, the email should be tagged as genuine and not SPAM. Analysis of these IP address ranges indicate nothing more than typical marketing activity. The two IP ranges included in these SPF records overlap with those found in trump-email[.]com SPF record.
- "mx"
  - Any domain that hosts email has at least one MX record. These MX records identify which email servers should be used when relaying email. By including "mx" in the TXT record, the servers identified in the MX DNS record for contact-client[.]com are automatically approved and avoids having to re-list them in the TXT record.
- "include"
  - This includes the SPF record for these domains as valid sending sources. In this particular case, the SPF records for listrak[.]com, sendgrid[.]com, and maropost[.]com are to be included in the SPF record for contact-client[.]com. A breakdown of ownership for these domains is below.
- "~all"
  - This indicates that emails sent from an IP address not included in the SPF record should be accepted by the recipient but marked as an SPF failure.
- "google-site-verification"
  - This identifies that the webmaster has verified ownership with Google.

The SPF records demonstrate that for the contact-client[.]com domain, any email sent using the contact-client[.]com domain and originating from one of the IP ranges or MX domains included above are to be considered legitimate by the recipient of the email. However, this SPF configuration also allows for a spoofed email to be masquerading as contact-client[.]com from an IP address not approved by Cendyn. The "~all" flag, also known as a "soft fail"[24], indicates that if a recipient receives an email from contact-client[.]com but it originates from an IP address not included in the SPF record, the recipient should identify it as spam but allow it at their discretion. This option could allow a marketing organization to keep sending legitimate marketing emails in case of a DNS configuration error. It could also allow an attacker to bypass spam identification and deliver mail into an organization. That email could then have links in the body of the message, that could also force DNS lookups if delivered.

[24]https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/how-office-365-uses-spf-to-prevent-spoofing?view=o365-worldwide

The following is a list of domains that were seen in the "include" section of the SPF record for contact-client[.]com. As explained above, these domains were approved to send emails on behalf of *.contact-client[.]com, to include trump1.contact-client[.]com.

Domain	Ownership	Purpose
Listrak[.]com	Jeff McDonald 529 E. Main Street Lititz, PA 17543	A retail digital marketing automation platform trusted by leading brands for email marketing, mobile messaging, customer insights and cross-channel orchestration.
Sendgrid[.]com	Sendgrid, Inc. 1401 Walnut Street Boulder, CO 80302	Offers automated workflows that leverage automation triggers to set up automated, recurring emails or drip series to customers.
Maropost[.]com	Maropost, Inc. 200 University Avenue Toronto, Ontario	Offers an email marketing platform to create unique experiences for customers. Allows for the segmentation, scheduling, and development of dynamic content based on unified customer data.

Figure 12: Description of domains found in the SPF record for contact-client[.]com

CTAPT's analysis of the domains included in the table above concluded that all of them appear to be legitimate entities utilized by numerous companies for marketing purposes. It should be noted that Listrak also owns the IP address (66.216.133[.]29) that hosted both mail1.trump-email[.]com and trump1.contact-client[.]com. Figures 11-13 are screenshots copied from these platform websites highlighting Listrak customers:

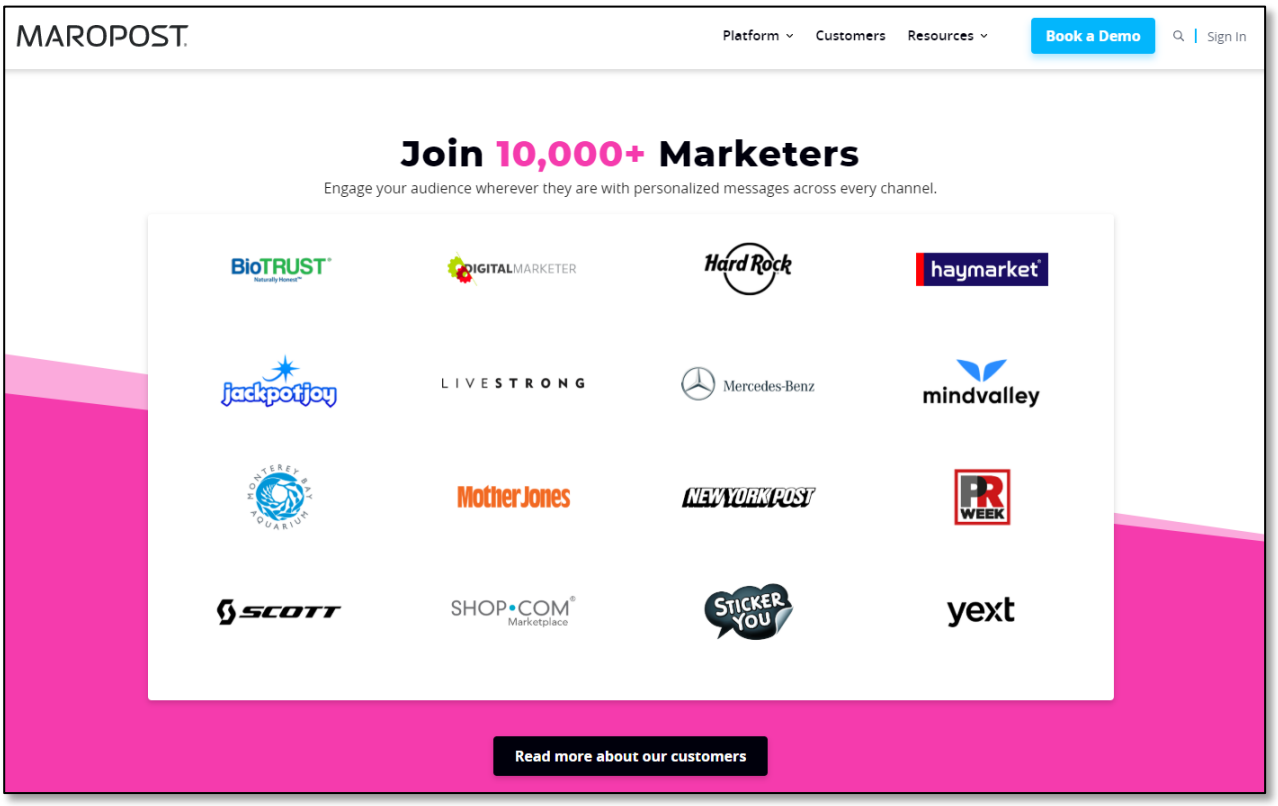


Figure 13: Screenshot from Maropost[.]com

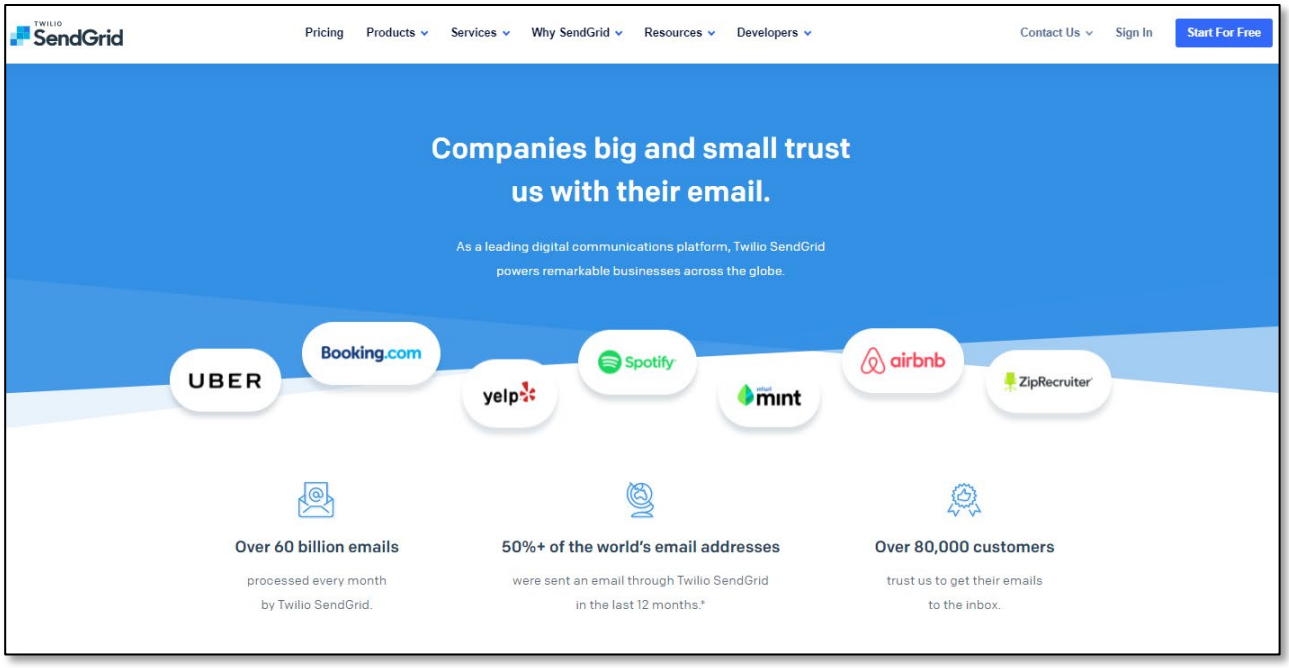


Figure 14: Screenshot from Sendgrid[.]com

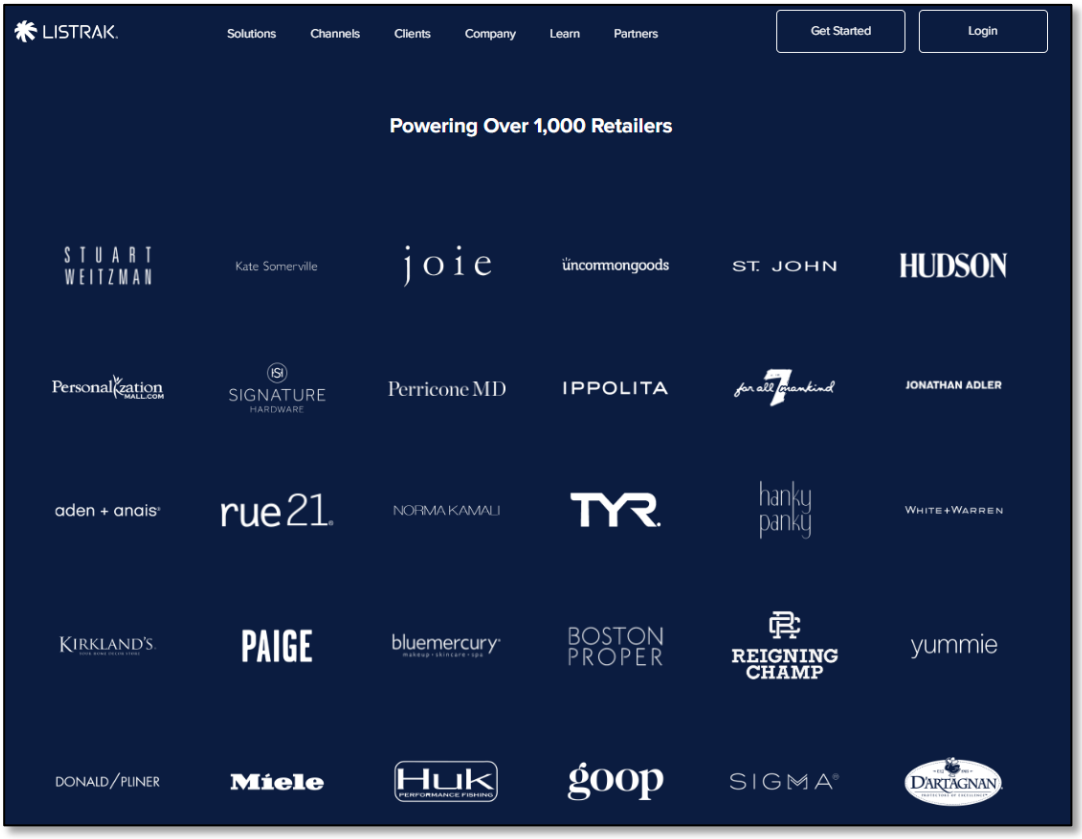


Figure 15: Screenshot from Listrak[.]com

We stress that the analysis performed by CTAPT did not find any support for allegations that either mail1.trump-email[.]com or trump1.contact-client[.]com were ever used as a covert communications channel. Newly identified historical DNS data obtained from SecurityTrails as well as our review of DomainTools and PassiveTotal, clearly strengthen the conclusion that these two domains were used for legitimate marketing purposes beginning as early as 2009.

Moreover, the fact that the SPF records for both domains included "~all" made it possible for malicious actors to have sent crafted SPAM emails, to both Alfa bank and Spectrum Health, spoofing either the mail1.trump-email[.]com or trump1.contact-client[.]com domain as the source. This would likely force the receiving entity's infrastructure to send a DNS record request to Cendyn nameservers to validate that the IP address used to send the email was verified, as per the stored DNS records on the Cendyn servers. These spoofed emails could have been sent at any time.

The passive DNS records specifically challenge the claim made in the New Yorker[25] that Alfa-Bank's servers found trump1.contact-client[.]com on September 27, 2016 as "evidence of direct contact between Alfa-Bank and Trump" since the DNS record shows that the DNS process was working as intended; when the mail1.trump-email[.]com did not resolve, the DNS process resolved to trump1.contact-client[.]com, which was assigned the same IP address. There are a number of scenarios that could be responsible for repeated DNS queries in this case, speculation includes the DNS activity could have been caused when Alfa-Bank blocked the IP address at their firewall and/or flagged that IP address as a source of SPAM. Or if a threat actor, also noticing that mail1.trump-email[.]com no longer resolved to an IP address, began sending spoofed emails masquerading as trump1.contact-client[.]com to Alfa-Bank, these spoofed emails would force Alfa-Bank's email servers to request SPF records from contact-client[.]com. Another possible scenario is a threat actor redirected DNS queries for both mail1.trump-email[.]com and trump1.contact-client[.]com through both Alfa-Bank and Spectrum Health DNS servers, to appear as if those DNS queries originated from Alfa-Bank and Spectrum Health and not the actual sender. This is demonstrated in Appendix B.

ROOT CAUSE ANALYSIS

CTAPT analysis of available DNS records identified the following potential causes for Alfa-Bank servers conducting DNS lookups for Trump related domains:

SPAM Email
As mentioned previously, SPF records for both email-trump[.]com and contact-client[.]com included the string “~all”. This mechanism allows for spoofed emails received by an entity like Alfa-Bank, to compare validated IP addresses from Cendyn and pass them through, since Cendyn servers were configured to respond with a “Softfail”[26] instead of a “Hardfail.” This Cendyn configuration forces the recipient of a marketing or spoof email (Alfa-Bank) to request the SPF DNS record for the alleged sending domain, essentially tricking a recipient of an email to perform a DNS query for a domain it never visited or received a legitimate email from.

DNS Forgery
The CTAPT conducted a test that explored the idea that an outside entity could push a DNS request query to Alfa-Bank’s DNS servers. Additionally, network traffic validation was achieved by capturing network traffic generated from a test DNS server, to see the activity associated with execution of the DIG command.

[25]https://www.newyorker.com/magazine/2018/10/15/was-there-a-connection-between-a-russian-bank-and-the-trump-campaign
[26]https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/how-office-365-uses-spf-to-prevent-spoofing?view=o365-worldwide

To conduct the test, CTAPT used an open source tool named “Scapy” used by penetration testers to craft custom packets. Scapy is often used to bypass restrictive firewalls and other security measures to gain access to targeted networks. Using Scapy we crafted packets to manipulate our test server (mimicking Alfa-Bank’s DNS server) to conduct DNS DIG requests for “Ankura.com.” Our testing confirms it is possible to make an externally crafted request to a DNS server belonging to an entity like Alfa-Bank, and then forcing that server to fulfill the request, making it appear as if Alfa-Bank’s server requested it. Please review Appendix B for details.

Although media stories made numerous assumptions about how Alfa-Bank’s DNS servers were configured in 2016, the findings above, the Stroz Friedberg Investigation Summary dated 07/19/2017,[27] and our testing, support the view that Alfa-Bank’s systems may have been manipulated into sending the DNS requests noted by Tea Leaves, or others.

CONCLUSION

OBSERVATIONS

CTAPT’s investigation relied on recently identified SecurityTrails DNS records, DomainTools passive DNS databases, and PassiveTotal archives for inquiry into Cendyn, Internap, Listra, and Trump related entities. When considered together, the data affirms that the anonymous researchers who initially raised the covert Cyber connection allegation against the Trump Organization and Alfa-Bank, missed, ignored, or didn't have access to a complete record of DNS history. The multiple sources of DNS records the CTAPT reviewed demonstrate that the server alleged to be secret, was in fact an overt email marketing system. Ankura's analysis does not support either mail1.trump-email[.]com or trump1.contact-client[.]com being used as a covert communications channel. Newly identified historical DNS data obtained from SecurityTrails, as well as our review of DomainTools and PassiveTotal, actually strengthen the conclusion that these two domains were used for marketing purposes beginning as early as 2009 through 2016.

Ankura's analysis doesn’t find any support for the allegation of a "secret server" or covert "cyber links" between Alfa-Bank and the Trump Organization and is consistent with the conclusions of the FBI, as reported in the IG's report concerning the FBI's "Crossfire Hurricane" investigation.[28] The three sources of DNS records indicate that servers attributed to the Trump Organization were actually owned and operated by a hotel marketing related company named "Central Dynamics" (Cendyn). DNS records show that Cendyn was engaged in legitimate marketing activity for numerous global hotel chains, including Trump Hotels.

CTAPT's detailed review of DNS records demonstrates that the configuration of Cendyn servers may have enabled a threat actor to send spoofed emails or inauthentic DNS queries that could have generated DNS requests to Trump Organization affiliated domains, from Alfa-Bank and Spectrum Health IP addresses.

Additionally, CTAPT's research did not find evidence of open source reporting from the Information Security (INFOSEC) community, either before or after this allegation arose, that would suggest DNS lookup activity as described by the anonymous researchers offers a means for covert or secret communications. The updated passive DNS analysis coupled with the timing of the underlying allegations, suggest that Alfa-Bank servers may have been

[27] http://i2.cdn.turner.com/cnn/2017/images/07/24/dinh.to.grassley.feinstein.pdf
[28] https://www.justice.gov/storage/120919-examination.pdf

unwitting sources of the DNS requests at the direction of some entity to create a connection between Alfa-Bank and the Trump Organization. If true, this may constitute a violation of one or more U.S. federal criminal laws.

APPENDIX A

DOMAINS HOSTED ON 198.91.42.0/23

IP Address	Domain	Whois Record URL
198.91.42.175	70parkhotelrewards.com	https://whois.domaintools.com/70parkhotelrewards.com
198.91.42.8	95cordova.com	https://whois.domaintools.com/95cordova.com
198.91.42.56	accorproposal.com	https://whois.domaintools.com/accorproposal.com
198.91.42.25	acehotelandswimclubconcierge.com	https://whois.domaintools.com/acehotelandswimclubconcierge.com
198.91.42.25	acehotellondonconcierge.com	https://whois.domaintools.com/acehotellondonconcierge.com
198.91.42.25	acehotellosangelesconcierge.com	https://whois.domaintools.com/acehotellosangelesconcierge.com
198.91.42.25	acehotelnewyorkconcierge.com	https://whois.domaintools.com/acehotelnewyorkconcierge.com
198.91.42.43	acmehotelcompanychi.com	https://whois.domaintools.com/acmehotelcompanychi.com
198.91.42.25	affiniaconcierge.com	https://whois.domaintools.com/affiniaconcierge.com
198.91.42.26	airliecenteremenus.com	https://whois.domaintools.com/airliecenteremenus.com
198.91.42.30	aloftemenus.com	https://whois.domaintools.com/aloftemenus.com
198.91.42.56	aloftproposal.com	https://whois.domaintools.com/aloftproposal.com
198.91.42.25	americantradehotelconcierge.com	https://whois.domaintools.com/americantradehotelconcierge.com
198.91.42.165	amesbostonconcierge.com	https://whois.domaintools.com/amesbostonconcierge.com
198.91.42.43	anantara.info	https://whois.domaintools.com/anantara.info
198.91.42.26	andazemenus.com	https://whois.domaintools.com/andazemenus.com
198.91.42.76	aocmetals.com	https://whois.domaintools.com/aocmetals.com
198.91.42.43	arlohotels.co	https://whois.domaintools.com/arlohotels.co
198.91.42.24	atlantisproposal.com	https://whois.domaintools.com/atlantisproposal.com
198.91.42.43	avanihotels.info	https://whois.domaintools.com/avanihotels.info
198.91.42.56	avtebrochure.com	https://whois.domaintools.com/avtebrochure.com
198.91.42.24	avtproposal.com	https://whois.domaintools.com/avtproposal.com
198.91.42.26	bacaraemenus.com	https://whois.domaintools.com/bacaraemenus.com
198.91.42.26	bayviewcollection.international	https://whois.domaintools.com/bayviewcollection.international
198.91.42.26	bayviewhotels.international	https://whois.domaintools.com/bayviewhotels.international
198.91.42.24	benchmarkproposal.com	https://whois.domaintools.com/benchmarkproposal.com
198.91.42.25	bernarduslodgeeconcierge.com	https://whois.domaintools.com/bernarduslodgeeconcierge.com
198.91.42.26	bernssalongeremenus.com	https://whois.domaintools.com/bernssalongeremenus.com
198.91.42.3	bestwesternebrochure.com	https://whois.domaintools.com/bestwesternebrochure.com
198.91.42.26	bestwesternemenus.com	https://whois.domaintools.com/bestwesternemenus.com

198.91.42.27	bestwesterneplanner.com	https://whois.domaintools.com/bestwesterneplanner.com
198.91.42.1	bestwesternnews.com	https://whois.domaintools.com/bestwesternnews.com
198.91.42.26	beverlyheritagehotelemenus.com	https://whois.domaintools.com/beverlyheritagehotelemenus.com
198.91.42.26	beverlyhillshotelmenus.com	https://whois.domaintools.com/beverlyhillshotelmenus.com
198.91.42.24	biltmoreproposal.com	https://whois.domaintools.com/biltmoreproposal.com
198.91.42.26	boarsheadinnemenus.com	https://whois.domaintools.com/boarsheadinnemenus.com
198.91.42.8	bohemianhotelbiltmorevillage.com	https://whois.domaintools.com/bohemianhotelbiltmorevillage.com
198.91.42.26	bonnetcreekemenus.com	https://whois.domaintools.com/bonnetcreekemenus.com
198.91.42.23	bookmeeting.com	https://whois.domaintools.com/bookmeeting.com
198.91.42.25	borgataconcierge.com	https://whois.domaintools.com/borgataconcierge.com
198.91.42.164	brasstownvalleyconcierge.com	https://whois.domaintools.com/brasstownvalleyconcierge.com
198.91.42.26	broadmooremenus.com	https://whois.domaintools.com/broadmooremenus.com
198.91.42.24	broadmoorproposal.com	https://whois.domaintools.com/broadmoorproposal.com
198.91.42.43	brushcreekluxurycollection.com	https://whois.domaintools.com/brushcreekluxurycollection.com
198.91.42.43	brushcreekluxurycollections.com	https://whois.domaintools.com/brushcreekluxurycollections.com
198.91.42.26	buenavistaemenus.com	https://whois.domaintools.com/buenavistaemenus.com
198.91.42.56	bwiproposal.com	https://whois.domaintools.com/bwiproposal.com
198.91.42.24	cafeproposal.com	https://whois.domaintools.com/cafeproposal.com
198.91.42.8	casinoroyalehotel.com	https://whois.domaintools.com/casinoroyalehotel.com
198.91.42.1	cdcservices.com	https://whois.domaintools.com/cdcservices.com
198.91.42.24	celebrationproposal.com	https://whois.domaintools.com/celebrationproposal.com
198.91.42.2	cendyn-econcierge.com	https://whois.domaintools.com/cendyn-econcierge.com
198.91.42.56	cendynaccess.com	https://whois.domaintools.com/cendynaccess.com
198.91.42.3	cendynadvertising.com	https://whois.domaintools.com/cendynadvertising.com
198.91.42.43	cendyncommunity.com	https://whois.domaintools.com/cendyncommunity.com
198.91.42.24	cendynebrochure.com	https://whois.domaintools.com/cendynebrochure.com
198.91.42.1	cendynecard.com	https://whois.domaintools.com/cendynecard.com
198.91.42.20	cendyneconcierge.com	https://whois.domaintools.com/cendyneconcierge.com
198.91.42.56	cendyneproposal.com	https://whois.domaintools.com/cendyneproposal.com
198.91.42.3	cendynesalessuite.com	https://whois.domaintools.com/cendynesalessuite.com
198.91.42.3	cendynhotelqa.com	https://whois.domaintools.com/cendynhotelqa.com
198.91.42.36	cendynsource.com	https://whois.domaintools.com/cendynsource.com
198.91.42.3	cendynvoice.com	https://whois.domaintools.com/cendynvoice.com
198.91.42.26	chateaurestaurantemenus.com	https://whois.domaintools.com/chateaurestaurantemenus.com
198.91.42.24	cheecalodgeebrochure.com	https://whois.domaintools.com/cheecalodgeebrochure.com
198.91.42.158	choctawcasinoconcierge.com	https://whois.domaintools.com/choctawcasinoconcierge.com
198.91.42.2	chrco.ca	https://whois.domaintools.com/chrco.ca
198.91.42.210	chrco.com	https://whois.domaintools.com/chrco.com

198.91.42.156	client-qa-10.com	https://whois.domaintools.com/client-qa-10.com
198.91.42.236	clubproposal.com	https://whois.domaintools.com/clubproposal.com
198.91.42.43	cme-alcronhotel.com	https://whois.domaintools.com/cme-alcronhotel.com
198.91.42.43	cme-revolutionhotel.com	https://whois.domaintools.com/cme-revolutionhotel.com
198.91.42.43	cmte-hotellora.com	https://whois.domaintools.com/cmte-hotellora.com
198.91.42.43	cmte-lorahotel.com	https://whois.domaintools.com/cmte-lorahotel.com
198.91.42.43	cmte-villaroyalehotel.com	https://whois.domaintools.com/cmte-villaroyalehotel.com
198.91.42.43	cmte-woodlarkhotel.com	https://whois.domaintools.com/cmte-woodlarkhotel.com
198.91.42.24	coastproposal.com	https://whois.domaintools.com/coastproposal.com
198.91.42.20	conferenceplanningresources.biz	https://whois.domaintools.com/conferenceplanningresources.biz
198.91.42.20	conferenceplanningresources.info	https://whois.domaintools.com/conferenceplanningresources.info
198.91.42.20	conferenceplanningresources.net	https://whois.domaintools.com/conferenceplanningresources.net
198.91.42.20	conferenceplanningresources.org	https://whois.domaintools.com/conferenceplanningresources.org
198.91.42.26	connecticutconventioncenteremenus.com	https://whois.domaintools.com/connecticutconventioncenteremenus.com
198.91.42.26	conrademenus.com	https://whois.domaintools.com/conrademenus.com
198.91.42.136	conradmenus.com	https://whois.domaintools.com/conradmenus.com
198.91.42.5	coral-hospitality.com	https://whois.domaintools.com/coral-hospitality.com
198.91.42.5	coralbeachotelsandclubs.com	https://whois.domaintools.com/coralbeachotelsandclubs.com
198.91.42.5	coralcollection.com	https://whois.domaintools.com/coralcollection.com
198.91.42.5	coralhospitality.com	https://whois.domaintools.com/coralhospitality.com
198.91.42.9	corporatecup.org	https://whois.domaintools.com/corporatecup.org
198.91.42.5	courtyardmarriottpueblo.com	https://whois.domaintools.com/courtyardmarriottpueblo.com
198.91.42.24	coveproposal.com	https://whois.domaintools.com/coveproposal.com
198.91.42.210	crescenthotels.com	https://whois.domaintools.com/crescenthotels.com
198.91.42.1	crescentintranet.com	https://whois.domaintools.com/crescentintranet.com
198.91.42.26	crowneplazaemenus.com	https://whois.domaintools.com/crowneplazaemenus.com
198.91.42.56	crowneplazaproposal.com	https://whois.domaintools.com/crowneplazaproposal.com
198.91.42.26	crowneventsemenus.com	https://whois.domaintools.com/crowneventsemenus.com
198.91.42.43	cte-alcronhotel.com	https://whois.domaintools.com/cte-alcronhotel.com
198.91.42.43	cte-revolutionhotel.com	https://whois.domaintools.com/cte-revolutionhotel.com
198.91.42.26	curioemenus.com	https://whois.domaintools.com/curioemenus.com
198.91.42.43	cwresorts.com	https://whois.domaintools.com/cwresorts.com
198.91.42.24	davidsonproposal.com	https://whois.domaintools.com/davidsonproposal.com
198.91.42.8	delraysands.com	https://whois.domaintools.com/delraysands.com
198.91.42.209	delraysandsresort.com	https://whois.domaintools.com/delraysandsresort.com
198.91.42.24	destinationproposal.com	https://whois.domaintools.com/destinationproposal.com
198.91.42.24	disneyeproposal.com	https://whois.domaintools.com/disneyeproposal.com

198.91.42.24	dolceproposal.com	https://whois.domaintools.com/dolceproposal.com
198.91.42.26	doralgolfresortemenus.com	https://whois.domaintools.com/doralgolfresortemenus.com
198.91.42.24	dorchestercollectionproposal.com	https://whois.domaintools.com/dorchestercollectionproposal.com
198.91.42.26	doubletreemenus.com	https://whois.domaintools.com/doubletreemenus.com
198.91.42.24	doubletreeproposal.com	https://whois.domaintools.com/doubletreeproposal.com
198.91.42.26	drakehotelemenus.com	https://whois.domaintools.com/drakehotelemenus.com
198.91.42.24	dtebrochure.com	https://whois.domaintools.com/dtebrochure.com
198.91.42.20	e-confirmations.com	https://whois.domaintools.com/e-confirmations.com
198.91.42.25	eaglemountainhouseconcierge.com	https://whois.domaintools.com/eaglemountainhouseconcierge.com
198.91.42.20	eagleresortandspa.com	https://whois.domaintools.com/eagleresortandspa.com
198.91.42.20	eagleridgeinnresort.com	https://whois.domaintools.com/eagleridgeinnresort.com
198.91.42.20	eagleridgeresortonline.com	https://whois.domaintools.com/eagleridgeresortonline.com
198.91.42.26	eaglewoodresortemenus.com	https://whois.domaintools.com/eaglewoodresortemenus.com
198.91.42.25	eattacheservice.com	https://whois.domaintools.com/eattacheservice.com
198.91.42.26	ectcemenus.com	https://whois.domaintools.com/ectcemenus.com
198.91.42.30	elementemenus.com	https://whois.domaintools.com/elementemenus.com
198.91.42.56	elementproposal.com	https://whois.domaintools.com/elementproposal.com
198.91.42.43	email-hotelmodera.com	https://whois.domaintools.com/email-hotelmodera.com
198.91.42.43	email-montagehotels.com	https://whois.domaintools.com/email-montagehotels.com
198.91.42.43	email-pendryhotels.com	https://whois.domaintools.com/email-pendryhotels.com
198.91.42.43	email-rlhc.com	https://whois.domaintools.com/email-rlhc.com
198.91.42.43	email-sagehotelscollection.com	https://whois.domaintools.com/email-sagehotelscollection.com
198.91.42.26	embassysuitesemenus.com	https://whois.domaintools.com/embassysuitesemenus.com
198.91.42.26	embassysuiteshotelsemenus.com	https://whois.domaintools.com/embassysuiteshotelsemenus.com
198.91.42.136	embassysuitesmenus.com	https://whois.domaintools.com/embassysuitesmenus.com
198.91.42.201	emenusaccess.com	https://whois.domaintools.com/emenusaccess.com
198.91.42.43	encoreatreunion.com	https://whois.domaintools.com/encoreatreunion.com
198.91.42.43	encoreatreunion.info	https://whois.domaintools.com/encoreatreunion.info
198.91.42.19	enrichingthespiritatsandpearl.com	https://whois.domaintools.com/enrichingthespiritatsandpearl.com
198.91.42.81	eplanneraccess.com	https://whois.domaintools.com/eplanneraccess.com
198.91.42.56	eproposalaccess.com	https://whois.domaintools.com/eproposalaccess.com
198.91.42.3	eproposalsupport.com	https://whois.domaintools.com/eproposalsupport.com
198.91.42.163	essexhouseconcierge.com	https://whois.domaintools.com/essexhouseconcierge.com
198.91.42.24	eventeproposal.com	https://whois.domaintools.com/eventeproposal.com
198.91.42.25	exeterinnconcierge.com	https://whois.domaintools.com/exeterinnconcierge.com
198.91.42.43	experience-copamarina.com	https://whois.domaintools.com/experience-copamarina.com
198.91.42.43	experience-hoteljoaquin.com	https://whois.domaintools.com/experience-hoteljoaquin.com
198.91.42.43	experience-studyhotels.com	https://whois.domaintools.com/experience-studyhotels.com

198.91.42.43	experience-theedwinhotel.com	https://whois.domaintools.com/experience-theedwinhotel.com
198.91.42.43	experiencehotelerwin.com	https://whois.domaintools.com/experiencehotelerwin.com
198.91.42.43	experienceinnatperrycabin.com	https://whois.domaintools.com/experienceinnatperrycabin.com
198.91.42.43	explorebrushcreekranch.com	https://whois.domaintools.com/explorebrushcreekranch.com
198.91.42.43	explorebrushcreekranchcollection.com	https://whois.domaintools.com/explorebrushcreekranchcollection.com
198.91.42.43	explorefrenchcreeksportsmensclub.com	https://whois.domaintools.com/explorefrenchcreeksportsmensclub.com
198.91.42.43	exploremageehomestead.com	https://whois.domaintools.com/exploremageehomestead.com
198.91.42.26	fairmontemenus.com	https://whois.domaintools.com/fairmontemenus.com
198.91.42.24	fairmonthotelvancouverebrochure.com	https://whois.domaintools.com/fairmonthotelvancouverebrochure.com
198.91.42.26	fallsviewcasinoresortemenus.com	https://whois.domaintools.com/fallsviewcasinoresortemenus.com
198.91.42.30	fourpointsemenus.com	https://whois.domaintools.com/fourpointsemenus.com
198.91.42.56	fourpointsproposal.com	https://whois.domaintools.com/fourpointsproposal.com
198.91.42.26	fourseasonsemenus.com	https://whois.domaintools.com/fourseasonsemenus.com
198.91.42.136	fourseasonsmenus.com	https://whois.domaintools.com/fourseasonsmenus.com
198.91.42.20	galenaresort.com	https://whois.domaintools.com/galenaresort.com
198.91.42.77	getfinancebyhilton.com	https://whois.domaintools.com/getfinancebyhilton.com
198.91.42.78	getfinancebyhiltonstaging.com	https://whois.domaintools.com/getfinancebyhiltonstaging.com
198.91.42.26	glencovemansionemenus.com	https://whois.domaintools.com/glencovemansionemenus.com
198.91.42.1	globalgds.com	https://whois.domaintools.com/globalgds.com
198.91.42.1	goard.com	https://whois.domaintools.com/goard.com
198.91.42.43	gohotelvic.com	https://whois.domaintools.com/gohotelvic.com
198.91.42.20	golfgalena.com	https://whois.domaintools.com/golfgalena.com
198.91.42.8	grandbohemiangalleries.com	https://whois.domaintools.com/grandbohemiangalleries.com
198.91.42.24	grandbrochure.com	https://whois.domaintools.com/grandbrochure.com
198.91.42.19	grandlucayanatyourservice.com	https://whois.domaintools.com/grandlucayanatyourservice.com
198.91.42.8	grandthemehotels.com	https://whois.domaintools.com/grandthemehotels.com
198.91.42.3	gravesresidences.com	https://whois.domaintools.com/gravesresidences.com
198.91.42.43	greystonehotelscme.com	https://whois.domaintools.com/greystonehotelscme.com
198.91.42.43	greystonehotelscte.com	https://whois.domaintools.com/greystonehotelscte.com
198.91.42.5	groupmeetingsnyc.com	https://whois.domaintools.com/groupmeetingsnyc.com
198.91.42.5	groupsnyc.com	https://whois.domaintools.com/groupsnyc.com
198.91.42.24	gwrproposal.com	https://whois.domaintools.com/gwrproposal.com
198.91.42.26	hamiltonparkemenus.com	https://whois.domaintools.com/hamiltonparkemenus.com
198.91.42.26	hamptonhotelsemenus.com	https://whois.domaintools.com/hamptonhotelsemenus.com
198.91.42.26	hamptoninnemenus.com	https://whois.domaintools.com/hamptoninnemenus.com
198.91.42.24	hamptoninnproposal.com	https://whois.domaintools.com/hamptoninnproposal.com

198.91.42.24	hardrockcafesproposal.com	https://whois.domaintools.com/hardrockcafesproposal.com
198.91.42.20	hardrockebrochure.com	https://whois.domaintools.com/hardrockebrochure.com
198.91.42.24	hardrockproposal.com	https://whois.domaintools.com/hardrockproposal.com
198.91.42.3	hgimagnificentmileebrochure.com	https://whois.domaintools.com/hgimagnificentmileebrochure.com
198.91.42.189	hhotellosangeles.com	https://whois.domaintools.com/hhotellosangeles.com
198.91.42.211	hi-nyc.com	https://whois.domaintools.com/hi-nyc.com
198.91.42.20	hiltonebrochure.com	https://whois.domaintools.com/hiltonebrochure.com
198.91.42.26	hiltonemenus.com	https://whois.domaintools.com/hiltonemenus.com
198.91.42.26	hiltongardeninnemenus.com	https://whois.domaintools.com/hiltongardeninnemenus.com
198.91.42.136	hiltongardeninnmenus.com	https://whois.domaintools.com/hiltongardeninnmenus.com
198.91.42.24	hiltonproposal.com	https://whois.domaintools.com/hiltonproposal.com
198.91.42.26	hiltonwwemenus.com	https://whois.domaintools.com/hiltonwwemenus.com
198.91.42.26	holidayinnemenus.com	https://whois.domaintools.com/holidayinnemenus.com
198.91.42.24	holidayinnproposal.com	https://whois.domaintools.com/holidayinnproposal.com
198.91.42.5	holidaysatthedel.com	https://whois.domaintools.com/holidaysatthedel.com
198.91.42.26	homewoodsuitesemenus.com	https://whois.domaintools.com/homewoodsuitesemenus.com
198.91.42.25	hooterscasinohotelconcierge.com	https://whois.domaintools.com/hooterscasinohotelconcierge.com
198.91.42.194	hospitalityupgrade.com	https://whois.domaintools.com/hospitalityupgrade.com
198.91.42.26	hotelbelairemenus.com	https://whois.domaintools.com/hotelbelairemenus.com
198.91.42.26	hotelchicagodowntownemenus.com	https://whois.domaintools.com/hotelchicagodowntownemenus.com
198.91.42.24	hotelemployee.com	https://whois.domaintools.com/hotelemployee.com
198.91.42.26	hotelirvinemenus.com	https://whois.domaintools.com/hotelirvinemenus.com
198.91.42.58	hotelmadisonalumni.com	https://whois.domaintools.com/hotelmadisonalumni.com
198.91.42.43	hotelmadisonva.com	https://whois.domaintools.com/hotelmadisonva.com
198.91.42.26	hotelmonteleoneemenus.com	https://whois.domaintools.com/hotelmonteleoneemenus.com
198.91.42.26	hotelnobuibizabay.com	https://whois.domaintools.com/hotelnobuibizabay.com
198.91.42.1	hotelorigami.com	https://whois.domaintools.com/hotelorigami.com
198.91.42.140	hoteltrio.com	https://whois.domaintools.com/hoteltrio.com
198.91.42.141	hotelvicrewards.com	https://whois.domaintools.com/hotelvicrewards.com
198.91.42.162	hotelvikingeconcierge.com	https://whois.domaintools.com/hotelvikingeconcierge.com
198.91.42.24	houseofbluesproposal.com	https://whois.domaintools.com/houseofbluesproposal.com
198.91.42.43	huntleyexclusives.com	https://whois.domaintools.com/huntleyexclusives.com
198.91.42.43	huntleyexperience.com	https://whois.domaintools.com/huntleyexperience.com
198.91.42.26	huntvalleyinnemenus.com	https://whois.domaintools.com/huntvalleyinnemenus.com
198.91.42.167	hutchinsonshores.com	https://whois.domaintools.com/hutchinsonshores.com
198.91.42.2	hyatt.gr	https://whois.domaintools.com/hyatt.gr
198.91.42.2	hyattbrochure.com	https://whois.domaintools.com/hyattbrochure.com
198.91.42.151	hyattcatering.de	https://whois.domaintools.com/hyattcatering.de

198.91.42.154	hyattemenus.com	https://whois.domaintools.com/hyattemenus.com
198.91.42.3	hyattfortheholidays.com	https://whois.domaintools.com/hyattfortheholidays.com
198.91.42.135	hyattmenus.com	https://whois.domaintools.com/hyattmenus.com
198.91.42.24	hyattproposal.com	https://whois.domaintools.com/hyattproposal.com
198.91.42.198	iclocalrewards.com	https://whois.domaintools.com/iclocalrewards.com
198.91.42.24	icproposal.com	https://whois.domaintools.com/icproposal.com
198.91.42.26	ihgemenus.com	https://whois.domaintools.com/ihgemenus.com
198.91.42.26	indigoemenus.com	https://whois.domaintools.com/indigoemenus.com
198.91.42.43	info-hrhguadalajara.com	https://whois.domaintools.com/info-hrhguadalajara.com
198.91.42.43	info-hrhlondon.com	https://whois.domaintools.com/info-hrhlondon.com
198.91.42.43	innatperrycabinreservations.com	https://whois.domaintools.com/innatperrycabinreservations.com
198.91.42.43	islabellabeachresortfl.com	https://whois.domaintools.com/islabellabeachresortfl.com
198.91.42.24	jcresortsproposal.com	https://whois.domaintools.com/jcresortsproposal.com
198.91.42.24	jumeirahproposal.com	https://whois.domaintools.com/jumeirahproposal.com
198.91.42.207	jupiterbeachresort.com	https://whois.domaintools.com/jupiterbeachresort.com
198.91.42.56	kempinskiproposal.com	https://whois.domaintools.com/kempinskiproposal.com
198.91.42.25	kesslerconcierge.com	https://whois.domaintools.com/kesslerconcierge.com
198.91.42.24	kesslerproposal.com	https://whois.domaintools.com/kesslerproposal.com
198.91.42.24	kimptonebrochure.com	https://whois.domaintools.com/kimptonebrochure.com
198.91.42.56	kimptonproposal.com	https://whois.domaintools.com/kimptonproposal.com
198.91.42.25	kittitianhillexperience.com	https://whois.domaintools.com/kittitianhillexperience.com
198.91.42.24	kslproposal.com	https://whois.domaintools.com/kslproposal.com
198.91.42.26	kyotogardenemenus.com	https://whois.domaintools.com/kyotogardenemenus.com
198.91.42.26	kyotograndemenus.com	https://whois.domaintools.com/kyotograndemenus.com
198.91.42.197	lakeplacidlodge.com	https://whois.domaintools.com/lakeplacidlodge.com
198.91.42.24	langhamproposal.com	https://whois.domaintools.com/langhamproposal.com
198.91.42.26	lansingcenteremenus.com	https://whois.domaintools.com/lansingcenteremenus.com
198.91.42.24	laquintaproposal.com	https://whois.domaintools.com/laquintaproposal.com
198.91.42.8	lathamhotelphiladelphia.com	https://whois.domaintools.com/lathamhotelphiladelphia.com
198.91.42.3	latorrettaebrochure.com	https://whois.domaintools.com/latorrettaebrochure.com
198.91.42.26	latorrettalakeresortemenus.com	https://whois.domaintools.com/latorrettalakeresortemenus.com
198.91.42.26	lecrystalhotelemenus.com	https://whois.domaintools.com/lecrystalhotelemenus.com
198.91.42.30	lemeridienemenus.com	https://whois.domaintools.com/lemeridienemenus.com
198.91.42.56	lemeridienproposal.com	https://whois.domaintools.com/lemeridienproposal.com
198.91.42.26	lexingtonhotelsemenus.com	https://whois.domaintools.com/lexingtonhotelsemenus.com
198.91.42.1	lfcdevelopment.com	https://whois.domaintools.com/lfcdevelopment.com
198.91.42.200	lidobeachresort.com	https://whois.domaintools.com/lidobeachresort.com
198.91.42.24	limevenueproposal.com	https://whois.domaintools.com/limevenueproposal.com

198.91.42.24	livenationproposal.com	https://whois.domaintools.com/livenationproposal.com
198.91.42.26	loewsemenus.com	https://whois.domaintools.com/loewsemenus.com
198.91.42.203	longboatkeyclub.com	https://whois.domaintools.com/longboatkeyclub.com
198.91.42.215	longreachhouse.com	https://whois.domaintools.com/longreachhouse.com
198.91.42.134	lostvalleyranch.com	https://whois.domaintools.com/lostvalleyranch.com
198.91.42.26	lowesemenus.com	https://whois.domaintools.com/lowesemenus.com
198.91.42.30	luxurycollectionemenus.com	https://whois.domaintools.com/luxurycollectionemenus.com
198.91.42.56	luxurycollectionproposal.com	https://whois.domaintools.com/luxurycollectionproposal.com
198.91.42.3	lynnfinancialcenter.com	https://whois.domaintools.com/lynnfinancialcenter.com
198.91.42.1	madsearch.com	https://whois.domaintools.com/madsearch.com
198.91.42.43	makemyplaceyourplace.com	https://whois.domaintools.com/makemyplaceyourplace.com
198.91.42.24	mandarinorientalproposal.com	https://whois.domaintools.com/mandarinorientalproposal.com
198.91.42.24	mansionproposal.com	https://whois.domaintools.com/mansionproposal.com
198.91.42.43	margaritavilleres.com	https://whois.domaintools.com/margaritavilleres.com
198.91.42.26	marketingnobuhotelibizabay.com	https://whois.domaintools.com/marketingnobuhotelibizabay.com
198.91.42.24	marriottebrochure.com	https://whois.domaintools.com/marriottebrochure.com
198.91.42.1	marriottecard.com	https://whois.domaintools.com/marriottecard.com
198.91.42.5	marriottmn.com	https://whois.domaintools.com/marriottmn.com
198.91.42.24	marriottproposal.com	https://whois.domaintools.com/marriottproposal.com
198.91.42.26	meadowoodnapavalleyemenus.com	https://whois.domaintools.com/meadowoodnapavalleyemenus.com
198.91.42.26	mebymeliaemenus.com	https://whois.domaintools.com/mebymeliaemenus.com
198.91.42.14	media-client.com	https://whois.domaintools.com/media-client.com
198.91.42.8	meetinglouisville.com	https://whois.domaintools.com/meetinglouisville.com
198.91.42.43	mekongkingdoms.info	https://whois.domaintools.com/mekongkingdoms.info
198.91.42.181	menusaccess.com	https://whois.domaintools.com/menusaccess.com
198.91.42.43	mhm-news.com	https://whois.domaintools.com/mhm-news.com
198.91.42.1	millenniumebrochure.com	https://whois.domaintools.com/millenniumebrochure.com
198.91.42.43	minorhotels.info	https://whois.domaintools.com/minorhotels.info
198.91.42.205	miravalspamonarchbeach.com	https://whois.domaintools.com/miravalspamonarchbeach.com
198.91.42.43	montagereservations.com	https://whois.domaintools.com/montagereservations.com
198.91.42.3	mountainlodgeebrochure.com	https://whois.domaintools.com/mountainlodgeebrochure.com
198.91.42.216	mrccoconutgrove.com	https://whois.domaintools.com/mrccoconutgrove.com
198.91.42.216	mrchotels.com	https://whois.domaintools.com/mrchotels.com
198.91.42.216	mrcseaport.com	https://whois.domaintools.com/mrcseaport.com
198.91.42.25	myaffiniaconcierge.com	https://whois.domaintools.com/myaffiniaconcierge.com
198.91.42.179	mybreakersstay.com	https://whois.domaintools.com/mybreakersstay.com
198.91.42.25	mybroadmoorconcierge.com	https://whois.domaintools.com/mybroadmoorconcierge.com
198.91.42.43	myhotelvic.com	https://whois.domaintools.com/myhotelvic.com

198.91.42.19	myladeraexperience.com	https://whois.domaintools.com/myladeraexperience.com
198.91.42.43	mymiravalstay.com	https://whois.domaintools.com/mymiravalstay.com
198.91.42.43	myplacehotelsreservations.com	https://whois.domaintools.com/myplacehotelsreservations.com
198.91.42.43	myplacestayrewarded.com	https://whois.domaintools.com/myplacestayrewarded.com
198.91.42.161	myroundhillexperience.com	https://whois.domaintools.com/myroundhillexperience.com
198.91.42.20	myterracewedding.com	https://whois.domaintools.com/myterracewedding.com
198.91.42.43	naladhu.info	https://whois.domaintools.com/naladhu.info
198.91.42.26	newmarketemenusdemo.com	https://whois.domaintools.com/newmarketemenusdemo.com
198.91.42.43	news-belovedhotels.com	https://whois.domaintools.com/news-belovedhotels.com
198.91.42.43	news-excellenceresorts.com	https://whois.domaintools.com/news-excellenceresorts.com
198.91.42.43	news-finestresorts.com	https://whois.domaintools.com/news-finestresorts.com
198.91.42.43	news-theexcellencecollection.com	https://whois.domaintools.com/news-theexcellencecollection.com
198.91.42.43	newstunehotels.com	https://whois.domaintools.com/newstunehotels.com
198.91.42.43	niyama.info	https://whois.domaintools.com/niyama.info
198.91.42.157	noblehouseconcierge.com	https://whois.domaintools.com/noblehouseconcierge.com
198.91.42.24	noblehouseproposal.com	https://whois.domaintools.com/noblehouseproposal.com
198.91.42.172	nyloloyals.com	https://whois.domaintools.com/nyloloyals.com
198.91.42.172	nylomembers.com	https://whois.domaintools.com/nylomembers.com
198.91.42.43	oakshotels.info	https://whois.domaintools.com/oakshotels.info
198.91.42.43	oceansedgehotelkw.com	https://whois.domaintools.com/oceansedgehotelkw.com
198.91.42.43	omnihotels-cme.com	https://whois.domaintools.com/omnihotels-cme.com
198.91.42.43	omnihotels-cte.com	https://whois.domaintools.com/omnihotels-cte.com
198.91.42.26	oneoceanresortemenus.com	https://whois.domaintools.com/oneoceanresortemenus.com
198.91.42.193	opalcollection.com	https://whois.domaintools.com/opalcollection.com
198.91.42.57	opalgrand.com	https://whois.domaintools.com/opalgrand.com
198.91.42.38	ovationsmanagement.com	https://whois.domaintools.com/ovationsmanagement.com
198.91.42.38	ovationssolutions.com	https://whois.domaintools.com/ovationssolutions.com
198.91.42.2	ownkaanapali.com	https://whois.domaintools.com/ownkaanapali.com
198.91.42.24	palaceproposal.com	https://whois.domaintools.com/palaceproposal.com
198.91.42.43	palazzoversace-mail.ae	https://whois.domaintools.com/palazzoversace-mail.ae
198.91.42.26	panpacificseattleemenus.com	https://whois.domaintools.com/panpacificseattleemenus.com
198.91.42.26	parkvistagatlinburgemenus.com	https://whois.domaintools.com/parkvistagatlinburgemenus.com
198.91.42.26	peabodyorlandoemenus.com	https://whois.domaintools.com/peabodyorlandoemenus.com
198.91.42.24	pebblebeachproposal.com	https://whois.domaintools.com/pebblebeachproposal.com
198.91.42.26	pelicangrandbeachresortemenus.com	https://whois.domaintools.com/pelicangrandbeachresortemenus.com
198.91.42.43	pendryreservations.com	https://whois.domaintools.com/pendryreservations.com
198.91.42.26	peppermillemenus.com	https://whois.domaintools.com/peppermillemenus.com

198.91.42.3	pganationalebrochure.com	https://whois.domaintools.com/pganationalebrochure.com
198.91.42.26	pganationalemenus.com	https://whois.domaintools.com/pganationalemenus.com
198.91.42.43	platinumpinkclub.com	https://whois.domaintools.com/platinumpinkclub.com
198.91.42.24	projectionproposal.com	https://whois.domaintools.com/projectionproposal.com
198.91.42.56	proposalaccess.com	https://whois.domaintools.com/proposalaccess.com
198.91.42.55	proposalaccesssandbox.com	https://whois.domaintools.com/proposalaccesssandbox.com
198.91.42.26	radissonbluemenus.com	https://whois.domaintools.com/radissonbluemenus.com
198.91.42.26	radissonblumallofamericamenus.com	https://whois.domaintools.com/radissonblumallofamericamenus.com
198.91.42.26	radissonbluroyalhelsinkiemenus.com	https://whois.domaintools.com/radissonbluroyalhelsinkiemenus.com
198.91.42.26	radissonemenus.com	https://whois.domaintools.com/radissonemenus.com
198.91.42.24	radissonproposal.com	https://whois.domaintools.com/radissonproposal.com
198.91.42.24	ramadaebrochure.com	https://whois.domaintools.com/ramadaebrochure.com
198.91.42.26	redlionemenus.com	https://whois.domaintools.com/redlionemenus.com
198.91.42.3	regentpalmsebrochure.com	https://whois.domaintools.com/regentpalmsebrochure.com
198.91.42.48	relaxandenjoyclub.com	https://whois.domaintools.com/relaxandenjoyclub.com
198.91.42.24	renaissanceproposal.com	https://whois.domaintools.com/renaissanceproposal.com
198.91.42.43	res-hrhdesaru.com	https://whois.domaintools.com/res-hrhdesaru.com
198.91.42.43	res-hrhguadalajara.com	https://whois.domaintools.com/res-hrhguadalajara.com
198.91.42.43	res-hrhlondon.com	https://whois.domaintools.com/res-hrhlondon.com
198.91.42.43	reservations-copamarina.com	https://whois.domaintools.com/reservations-copamarina.com
198.91.42.43	reservations-hoteljoaquin.com	https://whois.domaintools.com/reservations-hoteljoaquin.com
198.91.42.43	reservations-hotelmodera.com	https://whois.domaintools.com/reservations-hotelmodera.com
198.91.42.43	reservations-sagehotelscollection.com	https://whois.domaintools.com/reservations-sagehotelscollection.com
198.91.42.1	resortecard.com	https://whois.domaintools.com/resortecard.com
198.91.42.133	revelationconsultancy.com	https://whois.domaintools.com/revelationconsultancy.com
198.91.42.24	reverehotelebrochure.com	https://whois.domaintools.com/reverehotelebrochure.com
198.91.42.160	rockstarhostconcierge.com	https://whois.domaintools.com/rockstarhostconcierge.com
198.91.42.1	roktekservices.com	https://whois.domaintools.com/roktekservices.com
198.91.42.24	rosenproposal.com	https://whois.domaintools.com/rosenproposal.com
198.91.42.56	rosewoodproposal.com	https://whois.domaintools.com/rosewoodproposal.com
198.91.42.172	roundhillselect.com	https://whois.domaintools.com/roundhillselect.com
198.91.42.43	rsvp-belovedhotels.com	https://whois.domaintools.com/rsvp-belovedhotels.com
198.91.42.43	rsvp-excellenceresorts.com	https://whois.domaintools.com/rsvp-excellenceresorts.com
198.91.42.43	rsvp-finestresorts.com	https://whois.domaintools.com/rsvp-finestresorts.com
198.91.42.43	rsvp-theexcellencecollection.com	https://whois.domaintools.com/rsvp-theexcellencecollection.com
198.91.42.186	saddlebrooktennis.com	https://whois.domaintools.com/saddlebrooktennis.com
198.91.42.159	sagamoreconcierge.com	https://whois.domaintools.com/sagamoreconcierge.com

198.91.42.43	sales-hrhdesaru.com	https://whois.domaintools.com/sales-hrhdesaru.com
198.91.42.188	samoset.com	https://whois.domaintools.com/samoset.com
198.91.42.188	samosetresort.com	https://whois.domaintools.com/samosetresort.com
198.91.42.24	sandiaproposal.com	https://whois.domaintools.com/sandiaproposal.com
198.91.42.26	sandiaresortandcasinoemenus.com	https://whois.domaintools.com/sandiaresortandcasinoemenus.com
198.91.42.25	sandiaresortexperience.com	https://whois.domaintools.com/sandiaresortexperience.com
198.91.42.24	sanibelproposal.com	https://whois.domaintools.com/sanibelproposal.com
198.91.42.20	santuitinncapecod.com	https://whois.domaintools.com/santuitinncapecod.com
198.91.42.3	seasidebrochure.com	https://whois.domaintools.com/seasidebrochure.com
198.91.42.9	secretharborbeachfrontresort.com	https://whois.domaintools.com/secretharborbeachfrontresort.com
198.91.42.9	secretharborbeachfrontresortusvi.com	https://whois.domaintools.com/secretharborbeachfrontresortusvi.com
198.91.42.9	secretharborbeachresortusvi.com	https://whois.domaintools.com/secretharborbeachresortusvi.com
198.91.42.9	secretharborusvi.com	https://whois.domaintools.com/secretharborusvi.com
198.91.42.9	secretharbourbeachfrontresortusvi.com	https://whois.domaintools.com/secretharbourbeachfrontresortusvi.com
198.91.42.9	secretharbourbeachresortusvi.com	https://whois.domaintools.com/secretharbourbeachresortusvi.com
198.91.42.9	secretharbourbeachresortvi.com	https://whois.domaintools.com/secretharbourbeachresortvi.com
198.91.42.9	secretharbourusvi.com	https://whois.domaintools.com/secretharbourusvi.com
198.91.42.5	sedona-resorts.com	https://whois.domaintools.com/sedona-resorts.com
198.91.42.26	sequelresortsemenus.com	https://whois.domaintools.com/sequelresortsemenus.com
198.91.42.26	shangrilasrasasentosaemenus.com	https://whois.domaintools.com/shangrilasrasasentosaemenus.com
198.91.42.30	sheratonemenus.com	https://whois.domaintools.com/sheratonemenus.com
198.91.42.56	sheratonproposal.com	https://whois.domaintools.com/sheratonproposal.com
198.91.42.24	shirehotelproposal.com	https://whois.domaintools.com/shirehotelproposal.com
198.91.42.26	sonestabayfrontemenus.com	https://whois.domaintools.com/sonestabayfrontemenus.com
198.91.42.26	southseasemenus.com	https://whois.domaintools.com/southseasemenus.com
198.91.42.26	springhillemenus.com	https://whois.domaintools.com/springhillemenus.com
198.91.42.29	standarddowntownlaconcierge.com	https://whois.domaintools.com/standarddowntownlaconcierge.com
198.91.42.29	standardeastvillagenycconcierge.com	https://whois.domaintools.com/standardeastvillagenycconcierge.com
198.91.42.29	standardhighlineconcierge.com	https://whois.domaintools.com/standardhighlineconcierge.com
198.91.42.29	standardhollywoodconcierge.com	https://whois.domaintools.com/standardhollywoodconcierge.com
198.91.42.29	standardmiamibeachconcierge.com	https://whois.domaintools.com/standardmiamibeachconcierge.com
198.91.42.30	starwoodemenus.com	https://whois.domaintools.com/starwoodemenus.com
198.91.42.23	starwoodproposalaccess.com	https://whois.domaintools.com/starwoodproposalaccess.com
198.91.42.20	statability.com	https://whois.domaintools.com/statability.com
198.91.42.26	statlerhotelemenus.com	https://whois.domaintools.com/statlerhotelemenus.com
198.91.42.43	stay-hotelerwin.com	https://whois.domaintools.com/stay-hotelerwin.com

198.91.42.43	stay-rlhc.com	https://whois.domaintools.com/stay-rlhc.com
198.91.42.43	stay-studyhotels.com	https://whois.domaintools.com/stay-studyhotels.com
198.91.42.43	stayatflemings-hotel.com	https://whois.domaintools.com/stayatflemings-hotel.com
198.91.42.43	stayatsavigny-hotel.com	https://whois.domaintools.com/stayatsavigny-hotel.com
198.91.42.43	staybrushcreekranch.com	https://whois.domaintools.com/staybrushcreekranch.com
198.91.42.43	staybrushcreekranchcollection.com	https://whois.domaintools.com/staybrushcreekranchcollection.com
198.91.42.43	stayfrenchcreeksportsmensclub.com	https://whois.domaintools.com/stayfrenchcreeksportsmensclub.com
198.91.42.8	staygaybaltimore.com	https://whois.domaintools.com/staygaybaltimore.com
198.91.42.43	staymageehomestead.com	https://whois.domaintools.com/staymageehomestead.com
198.91.42.43	staytunehotels.com	https://whois.domaintools.com/staytunehotels.com
198.91.42.26	steinlodgeemenus.com	https://whois.domaintools.com/steinlodgeemenus.com
198.91.42.20	stonedriftspa.com	https://whois.domaintools.com/stonedriftspa.com
198.91.42.26	stpaulmeetingcenteremenus.com	https://whois.domaintools.com/stpaulmeetingcenteremenus.com
198.91.42.30	stregisemenus.com	https://whois.domaintools.com/stregisemenus.com
198.91.42.56	stregisproposal.com	https://whois.domaintools.com/stregisproposal.com
198.91.42.26	stretisemenus.com	https://whois.domaintools.com/stretisemenus.com
198.91.42.26	sundyhouseemenus.com	https://whois.domaintools.com/sundyhouseemenus.com
198.91.42.26	suninternationalemenus.com	https://whois.domaintools.com/suninternationalemenus.com
198.91.42.176	sunsetkeycottages.com	https://whois.domaintools.com/sunsetkeycottages.com
198.91.42.24	swissotelproposal.com	https://whois.domaintools.com/swissotelproposal.com
198.91.42.26	swissotelsydneyemenus.com	https://whois.domaintools.com/swissotelsydneyemenus.com
198.91.42.24	tajproposal.com	https://whois.domaintools.com/tajproposal.com
198.91.42.20	terracehotelweddings.com	https://whois.domaintools.com/terracehotelweddings.com
198.91.42.26	thayerhotelatwestpointemenus.com	https://whois.domaintools.com/thayerhotelatwestpointemenus.com
198.91.42.25	thebenjaminconcierge.com	https://whois.domaintools.com/thebenjaminconcierge.com
198.91.42.1	thebluedolphins.com	https://whois.domaintools.com/thebluedolphins.com
198.91.42.26	thebreweryemenus.com	https://whois.domaintools.com/thebreweryemenus.com
198.91.42.166	thebrownpalaceconcierge.com	https://whois.domaintools.com/thebrownpalaceconcierge.com
198.91.42.26	thecharleshotelemenus.com	https://whois.domaintools.com/thecharleshotelemenus.com
198.91.42.26	thecheshireemenus.com	https://whois.domaintools.com/thecheshireemenus.com
198.91.42.43	thedominickhotelsoho.com	https://whois.domaintools.com/thedominickhotelsoho.com
198.91.42.182	theharborsidehotel.com	https://whois.domaintools.com/theharborsidehotel.com
198.91.42.26	thekingedwardhotelemenus.com	https://whois.domaintools.com/thekingedwardhotelemenus.com
198.91.42.43	theparchotelny.com	https://whois.domaintools.com/theparchotelny.com
198.91.42.1	thepurpledolphins.com	https://whois.domaintools.com/thepurpledolphins.com
198.91.42.43	theredburyhotelny.com	https://whois.domaintools.com/theredburyhotelny.com
198.91.42.196	thesagamore.biz	https://whois.domaintools.com/thesagamore.biz
198.91.42.196	thesagamore.com	https://whois.domaintools.com/thesagamore.com

198.91.42.196	thesagamore.net	https://whois.domaintools.com/thesagamore.net
198.91.42.196	thesagamore.org	https://whois.domaintools.com/thesagamore.org
198.91.42.8	thesuitesatbeavercreeklodge.com	https://whois.domaintools.com/thesuitesatbeavercreeklodge.com
198.91.42.183	theweststreethotel.com	https://whois.domaintools.com/theweststreethotel.com
198.91.42.43	tivolihotels.info	https://whois.domaintools.com/tivolihotels.info
198.91.42.26	trubyhiltonemenus.com	https://whois.domaintools.com/trubyhiltonemenus.com
198.91.42.26	trubyhiltoneplanner.com	https://whois.domaintools.com/trubyhiltoneplanner.com
198.91.42.136	trubyhiltonmenus.com	https://whois.domaintools.com/trubyhiltonmenus.com
198.91.42.24	trumpproposal.com	https://whois.domaintools.com/trumpproposal.com
198.91.42.43	turnberryisleinfo.com	https://whois.domaintools.com/turnberryisleinfo.com
198.91.42.43	turnberryislereservations.com	https://whois.domaintools.com/turnberryislereservations.com
198.91.42.173	universalhollywoodevents.com	https://whois.domaintools.com/universalhollywoodevents.com
198.91.42.24	universalproposal.com	https://whois.domaintools.com/universalproposal.com
198.91.42.26	universalstudioshollywoodemenus.com	https://whois.domaintools.com/universalstudioshollywoodemenus.com
198.91.42.26	universityofwashingtonemenus.com	https://whois.domaintools.com/universityofwashingtonemenus.com
198.91.42.8	ushgradventure.com	https://whois.domaintools.com/ushgradventure.com
198.91.42.56	vfcasinoproposal.com	https://whois.domaintools.com/vfcasinoproposal.com
198.91.42.43	visitflemings-hotel.com	https://whois.domaintools.com/visitflemings-hotel.com
198.91.42.43	visitmohonk.com	https://whois.domaintools.com/visitmohonk.com
198.91.42.43	visitsavigny-hotel.com	https://whois.domaintools.com/visitsavigny-hotel.com
198.91.42.26	waldorfastoriaemenus.com	https://whois.domaintools.com/waldorfastoriaemenus.com
198.91.42.30	westinemenus.com	https://whois.domaintools.com/westinemenus.com
198.91.42.3	westinlacanteraebrochure.com	https://whois.domaintools.com/westinlacanteraebrochure.com
198.91.42.56	westinproposal.com	https://whois.domaintools.com/westinproposal.com
198.91.42.3	westintysonsebrochure.com	https://whois.domaintools.com/westintysonsebrochure.com
198.91.42.26	westwardlookemenus.com	https://whois.domaintools.com/westwardlookemenus.com
198.91.42.3	wfortlauderdaleebrochure.com	https://whois.domaintools.com/wfortlauderdaleebrochure.com
198.91.42.30	whotelemenus.com	https://whois.domaintools.com/whotelemenus.com
198.91.42.56	whotelsproposal.com	https://whois.domaintools.com/whotelsproposal.com
198.91.42.1	wigwamebrochure.com	https://whois.domaintools.com/wigwamebrochure.com
198.91.42.25	windjammerexperience.com	https://whois.domaintools.com/windjammerexperience.com
198.91.42.144	winwestindetox.com	https://whois.domaintools.com/winwestindetox.com
198.91.42.24	wviequesweddingsebrochure.com	https://whois.domaintools.com/wviequesweddingsebrochure.com
198.91.42.43	wybostonlakesmail.com	https://whois.domaintools.com/wybostonlakesmail.com
198.91.42.26	wyndhamemenus.com	https://whois.domaintools.com/wyndhamemenus.com
198.91.42.24	wyndhamproposal.com	https://whois.domaintools.com/wyndhamproposal.com
198.91.42.24	wynnproposal.com	https://whois.domaintools.com/wynnproposal.com

198.91.42.5	yayagroves.com	https://whois.domaintools.com/yayagroves.com

DOMAINS HOSTED ON 63.251.151.0/24

IP Address	Domain	Whois Record URL
63.251.151.29	casaclaridgeconcierge.com	https://whois.domaintools.com/casaclaridgeconcierge.com
63.251.151.121	cendyn16.com	https://whois.domaintools.com/cendyn16.com
63.251.151.121	cendyn18.com	https://whois.domaintools.com/cendyn18.com
63.251.151.121	cendyn20.com	https://whois.domaintools.com/cendyn20.com
63.251.151.245	cendynproposal.com	https://whois.domaintools.com/cendynproposal.com
63.251.151.231	dolce-meetings.com	https://whois.domaintools.com/dolce-meetings.com
63.251.151.135	dolce-munich-ballhausforum.com	https://whois.domaintools.com/dolce-munich-ballhausforum.com
63.251.151.135	dolceballhausforum.com	https://whois.domaintools.com/dolceballhausforum.com
63.251.151.231	dolceconferencedestinations.com	https://whois.domaintools.com/dolceconferencedestinations.com
63.251.151.231	dolceconferencedestinations.net	https://whois.domaintools.com/dolceconferencedestinations.net
63.251.151.231	dolcegolf.es	https://whois.domaintools.com/dolcegolf.es
63.251.151.231	dolcehotel.de	https://whois.domaintools.com/dolcehotel.de
63.251.151.231	dolcehotel.es	https://whois.domaintools.com/dolcehotel.es
63.251.151.231	dolcehotelmanagement.com	https://whois.domaintools.com/dolcehotelmanagement.com
63.251.151.231	dolceinternational.net	https://whois.domaintools.com/dolceinternational.net
63.251.151.231	dolceinternationalonline.com	https://whois.domaintools.com/dolceinternationalonline.com
63.251.151.231	dolceinternationalonline.net	https://whois.domaintools.com/dolceinternationalonline.net
63.251.151.231	dolceintl.net	https://whois.domaintools.com/dolceintl.net
63.251.151.231	dolcemeeting.es	https://whois.domaintools.com/dolcemeeting.es
63.251.151.231	dolcemeetings.es	https://whois.domaintools.com/dolcemeetings.es
63.251.151.135	dolcemunich-unterschleissheim.com	https://whois.domaintools.com/dolcemunich-unterschleissheim.com
63.251.151.231	dolceonline.com	https://whois.domaintools.com/dolceonline.com
63.251.151.231	dolceonline.net	https://whois.domaintools.com/dolceonline.net
63.251.151.231	dolceresorts.es	https://whois.domaintools.com/dolceresorts.es
63.251.151.231	dolcespa.es	https://whois.domaintools.com/dolcespa.es
63.251.151.231	dolcevacation.es	https://whois.domaintools.com/dolcevacation.es
63.251.151.231	dolcevacation.it	https://whois.domaintools.com/dolcevacation.it
63.251.151.231	dolcevacations.es	https://whois.domaintools.com/dolcevacations.es
63.251.151.231	dolcewedding.es	https://whois.domaintools.com/dolcewedding.es
63.251.151.241	downtown-cc.com	https://whois.domaintools.com/downtown-cc.com

63.251.151.231	e-dolceconferencedestinations.com	https://whois.domaintools.com/e-dolceconferencedestinations.com
63.251.151.231	e-dolceconferencedestinations.net	https://whois.domaintools.com/e-dolceconferencedestinations.net
63.251.151.231	e-dolceinternational.com	https://whois.domaintools.com/e-dolceinternational.com
63.251.151.231	e-dolceinternational.net	https://whois.domaintools.com/e-dolceinternational.net
63.251.151.231	e-dolceintl.com	https://whois.domaintools.com/e-dolceintl.com
63.251.151.229	ecardemployee.com	https://whois.domaintools.com/ecardemployee.com
63.251.151.235	hotelcontessagroups.com	https://whois.domaintools.com/hotelcontessagroups.com
63.251.151.235	hotelcontessameetings.com	https://whois.domaintools.com/hotelcontessameetings.com
63.251.151.50	marriottemenus.com	https://whois.domaintools.com/marriottemenus.com
63.251.151.214	meetwithbedfordsprings.com	https://whois.domaintools.com/meetwithbedfordsprings.com
63.251.151.231	mydolceinternational.com	https://whois.domaintools.com/mydolceinternational.com
63.251.151.231	mydolceinternational.net	https://whois.domaintools.com/mydolceinternational.net
63.251.151.231	mydolceintl.com	https://whois.domaintools.com/mydolceintl.com
63.251.151.123	myproposal.com	https://whois.domaintools.com/myproposal.com
63.251.151.19	solvenhospitality.com	https://whois.domaintools.com/solvenhospitality.com
63.251.151.29	watercolorconcierge.com	https://whois.domaintools.com/watercolorconcierge.com

DOMAINS HOSTED ON 64.135.26.0/24

IP Address	Domain	Whois Record URL
64.135.26.49	acehotelreservations.com	https://whois.domaintools.com/acehotelreservations.com
64.135.26.65	amzak.com	https://whois.domaintools.com/amzak.com
64.135.26.5	arcaneo.com	https://whois.domaintools.com/arcaneo.com
64.135.26.46	bellemontfarm.com	https://whois.domaintools.com/bellemontfarm.com
64.135.26.48	c1awards.com	https://whois.domaintools.com/c1awards.com
64.135.26.3	cendyn-one.com	https://whois.domaintools.com/cendyn-one.com
64.135.26.49	cendyn17.com	https://whois.domaintools.com/cendyn17.com
64.135.26.5	cendynarcaneo.com	https://whois.domaintools.com/cendynarcaneo.com
64.135.26.49	cendynone.com	https://whois.domaintools.com/cendynone.com
64.135.26.5	cendynovations.org	https://whois.domaintools.com/cendynovations.org
64.135.26.15	client-qa.com	https://whois.domaintools.com/client-qa.com
64.135.26.3	clientqa.com	https://whois.domaintools.com/clientqa.com
64.135.26.49	contact-client.com	https://whois.domaintools.com/contact-client.com
64.135.26.49	contact-client2.com	https://whois.domaintools.com/contact-client2.com
64.135.26.56	embassysuiteslax.com	https://whois.domaintools.com/embassysuiteslax.com

64.135.26.49	esurvey-client.com	https://whois.domaintools.com/esurvey-client.com
64.135.26.3	halcyonhotelcherrycreek.com	https://whois.domaintools.com/halcyonhotelcherrycreek.com
64.135.26.14	hyattrsvp.com	https://whois.domaintools.com/hyattrsvp.com
64.135.26.50	kittitianhill.com	https://whois.domaintools.com/kittitianhill.com
64.135.26.52	laxembassy.com	https://whois.domaintools.com/laxembassy.com
64.135.26.56	laxresidenceinn.com	https://whois.domaintools.com/laxresidenceinn.com
64.135.26.56	losangelesresidenceinn.com	https://whois.domaintools.com/losangelesresidenceinn.com
64.135.26.38	lottenypalacemeetings.com	https://whois.domaintools.com/lottenypalacemeetings.com
64.135.26.56	marriottlax.com	https://whois.domaintools.com/marriottlax.com
64.135.26.59	muliabali.com	https://whois.domaintools.com/muliabali.com
64.135.26.59	muliaresort.com	https://whois.domaintools.com/muliaresort.com
64.135.26.59	muliaresortbali.com	https://whois.domaintools.com/muliaresortbali.com
64.135.26.59	muliavillabali.com	https://whois.domaintools.com/muliavillabali.com
64.135.26.59	muliavillasbali.com	https://whois.domaintools.com/muliavillasbali.com
64.135.26.5	ovationstechnologies.com	https://whois.domaintools.com/ovationstechnologies.com
64.135.26.66	paseocaribe.com	https://whois.domaintools.com/paseocaribe.com
64.135.26.49	reservations-client.com	https://whois.domaintools.com/reservations-client.com
64.135.26.56	residenceinnlax.com	https://whois.domaintools.com/residenceinnlax.com
64.135.26.57	saddlebrook.com	https://whois.domaintools.com/saddlebrook.com
64.135.26.58	saddlebrookprep.com	https://whois.domaintools.com/saddlebrookprep.com
64.135.26.59	themulia.com	https://whois.domaintools.com/themulia.com

DOMAINS HOSTED ON 64.95.241.0/34

IP Address	Domain	Whois Record URL
64.95.241.129	cendynhelp.com	https://whois.domaintools.com/cendynhelp.com
64.95.241.120	cendynhotelresort.com	https://whois.domaintools.com/cendynhotelresort.com
64.95.241.129	cendynresortqa.com	https://whois.domaintools.com/cendynresortqa.com
64.95.241.231	feeltheenergyathyatt.com	https://whois.domaintools.com/feeltheenergyathyatt.com
64.95.241.24	fourpointseplanner.com	https://whois.domaintools.com/fourpointseplanner.com
64.95.241.122	glbthyattthreeforfree.com	https://whois.domaintools.com/glbthyattthreeforfree.com
64.95.241.231	hssgrilling.com	https://whois.domaintools.com/hssgrilling.com
64.95.241.231	hyatt24hoursale.com	https://whois.domaintools.com/hyatt24hoursale.com
64.95.241.24	hyatteplanner.com	https://whois.domaintools.com/hyatteplanner.com
64.95.241.131	hyattfall08tv.com	https://whois.domaintools.com/hyattfall08tv.com
64.95.241.131	hyattfall2008.com	https://whois.domaintools.com/hyattfall2008.com
64.95.241.19	hyatthotdates.com	https://whois.domaintools.com/hyatthotdates.com

64.95.241.124	hyattsofsanantonio.com	https://whois.domaintools.com/hyattsofsanantonio.com
64.95.241.231	hybenefits.com	https://whois.domaintools.com/hybenefits.com
64.95.241.24	latorrettalakeresorteplanner.com	https://whois.domaintools.com/latorrettalakeresorteplanner.com
64.95.241.243	oceanahotelgroup.com	https://whois.domaintools.com/oceanahotelgroup.com
64.95.241.112	residenceinnfernandinabeach.com	https://whois.domaintools.com/residenceinnfernandinabeach.com
64.95.241.147	returntohyatt.com	https://whois.domaintools.com/returntohyatt.com
64.95.241.108	riverterraceinnebrochures.com	https://whois.domaintools.com/riverterraceinnebrochures.com
64.95.241.130	riviera-blackhawk.com	https://whois.domaintools.com/riviera-blackhawk.com
64.95.241.215	spalagunacliffs.com	https://whois.domaintools.com/spalagunacliffs.com

DOMAINS HOSTED ON 69.25.15.0/24

IP Address	Domain	Whois Record URL
69.25.15.114	1tierprocessing.com	https://whois.domaintools.com/1tierprocessing.com
69.25.15.101	4efi.com	https://whois.domaintools.com/4efi.com
69.25.15.100	4npa.com	https://whois.domaintools.com/4npa.com
69.25.15.104	aarmiami.com	https://whois.domaintools.com/aarmiami.com
69.25.15.112	affordableautorepairmiami.com	https://whois.domaintools.com/affordableautorepairmiami.com
69.25.15.113	eliteclient.capital	https://whois.domaintools.com/eliteclient.capital
69.25.15.117	eq.financial	https://whois.domaintools.com/eq.financial
69.25.15.107	equfi.com	https://whois.domaintools.com/equfi.com
69.25.15.20	fibercall.com	https://whois.domaintools.com/fibercall.com
69.25.15.20	i3adc.com	https://whois.domaintools.com/i3adc.com
69.25.15.20	i3computing.com	https://whois.domaintools.com/i3computing.com
69.25.15.20	i3medical.com	https://whois.domaintools.com/i3medical.com
69.25.15.20	i3servers.com	https://whois.domaintools.com/i3servers.com
69.25.15.20	i3soutions.com	https://whois.domaintools.com/i3soutions.com
69.25.15.20	innovativmed.com	https://whois.domaintools.com/innovativmed.com
69.25.15.13	kayecommunications.com	https://whois.domaintools.com/kayecommunications.com
69.25.15.111	nationalprocessingalliance.com	https://whois.domaintools.com/nationalprocessingalliance.com
69.25.15.166	palmbeachhistory.org	https://whois.domaintools.com/palmbeachhistory.org
69.25.15.166	pbhistory.com	https://whois.domaintools.com/pbhistory.com
69.25.15.166	pbhistory.org	https://whois.domaintools.com/pbhistory.org
69.25.15.102	sfeah.com	https://whois.domaintools.com/sfeah.com
69.25.15.122	stfrancisemergencyanimalhospital.com	https://whois.domaintools.com/stfrancisemergencyanimalhospital.com
69.25.15.103	wbaperformance.com	https://whois.domaintools.com/wbaperformance.com

69.25.15.123	wbapro.com	https://whois.domaintools.com/wbapro.com

APPENDIX B

DNS TESTING FOR EXTERNAL QUERY ACTIVITY (DNS FORGERY)

Ankura conducted a test that explored the idea that an outside party could push a DNS request query to Alfa-Bank's DNS servers. Additionally, we wanted to capture the traffic being generated from a test DNS server, to validate the activity associated with the DIG command being executed.

To synthesize the network environment CTAPT set up a Virtual Private Server (VPS), purchased from Linode. Using best practice, that VPS was setup and configured as a Ubuntu DNS server. A single Virtual Machine (VM) running Kali Linux was also part of the testing process. The VPS was designed to simulate the Alfa's DNS server. While the VM was to simulate an outside third party attempting to push DIG request through the VPS. For testing purposes, Ankura.com was the intended target for all DIG request. Wireshark was also running on both VPS and VM in order to capture and further analyze all traffic data.

CTAPT used a common python module called Scapy. Scapy is frequently used by penetration testers to craft custom packets in order to bypass restrictive firewalls and other security measures to gain access to targeted networks. Using Scapy we forged packets to manipulate our test server (mimicking Alfa-Bank's DNS server) to conduct DNS DIG requests for "Ankura.com." To generate the request, we set the nameserver we're querying, "50.116.57.58", the name we're querying, "Ankura.com", and the type of query, 255 for ANY records or "A" for A records. Then the sr() function sends the request and waits for a response. The commands used:

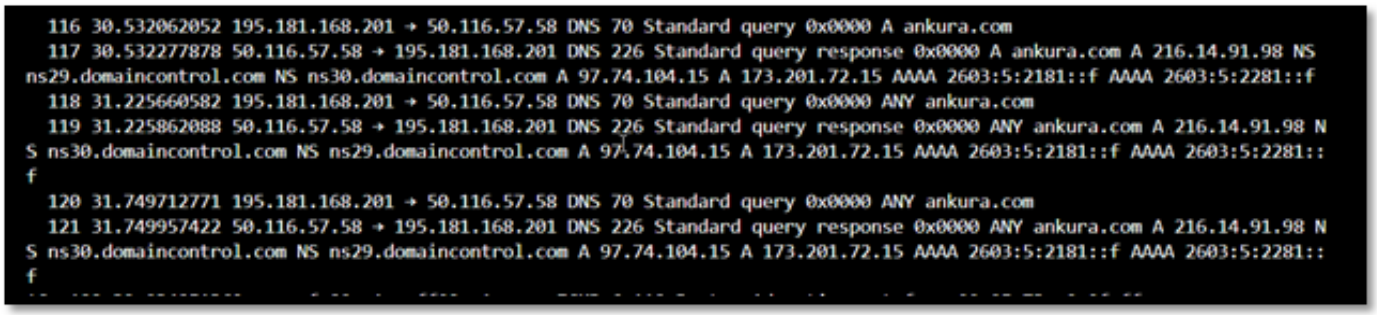
```
>>> any_dns=IP(dst="50.116.57.58")/UDP()/DNS(rd=1, qdcount=1, qd=DNSQR(qname="ankura.com", qtype=255))

>>> A_dns=IP(dst="50.116.57.58")/UDP()/DNS(rd=1, qd=DNSQR(qname="ankura.com",qtype="A"))

>>> sr(any_dns)

>>> sr(A_dns)
```

CTAPT testing confirms it is possible to execute an externally crafted request to a DNS server belonging to and entity like Alfa-Bank, and then that server responding to the crafted request, with a DNS query for the domain in the manipulated request (such as trump-email.com).


116 30.532062052 195.181.168.201 → 50.116.57.58 DNS 70 Standard query 0x0000 A ankura.com
117 30.532277878 50.116.57.58 → 195.181.168.201 DNS 226 Standard query response 0x0000 A ankura.com A 216.14.91.98 NS ns29.domaincontrol.com NS ns30.domaincontrol.com A 97.74.104.15 A 173.201.72.15 AAAA 2603:5:2181::f AAAA 2603:5:2281::f
118 31.225660582 195.181.168.201 → 50.116.57.58 DNS 70 Standard query 0x0000 ANY ankura.com
119 31.225862088 50.116.57.58 → 195.181.168.201 DNS 226 Standard query response 0x0000 ANY ankura.com A 216.14.91.98 NS ns30.domaincontrol.com NS ns29.domaincontrol.com A 97.74.104.15 A 173.201.72.15 AAAA 2603:5:2181::f AAAA 2603:5:2281::f
120 31.749712771 195.181.168.201 → 50.116.57.58 DNS 70 Standard query 0x0000 ANY ankura.com
121 31.749957422 50.116.57.58 → 195.181.168.201 DNS 226 Standard query response 0x0000 ANY ankura.com A 216.14.91.98 NS ns30.domaincontrol.com NS ns29.domaincontrol.com A 97.74.104.15 A 173.201.72.15 AAAA 2603:5:2181::f AAAA 2603:5:2281::f