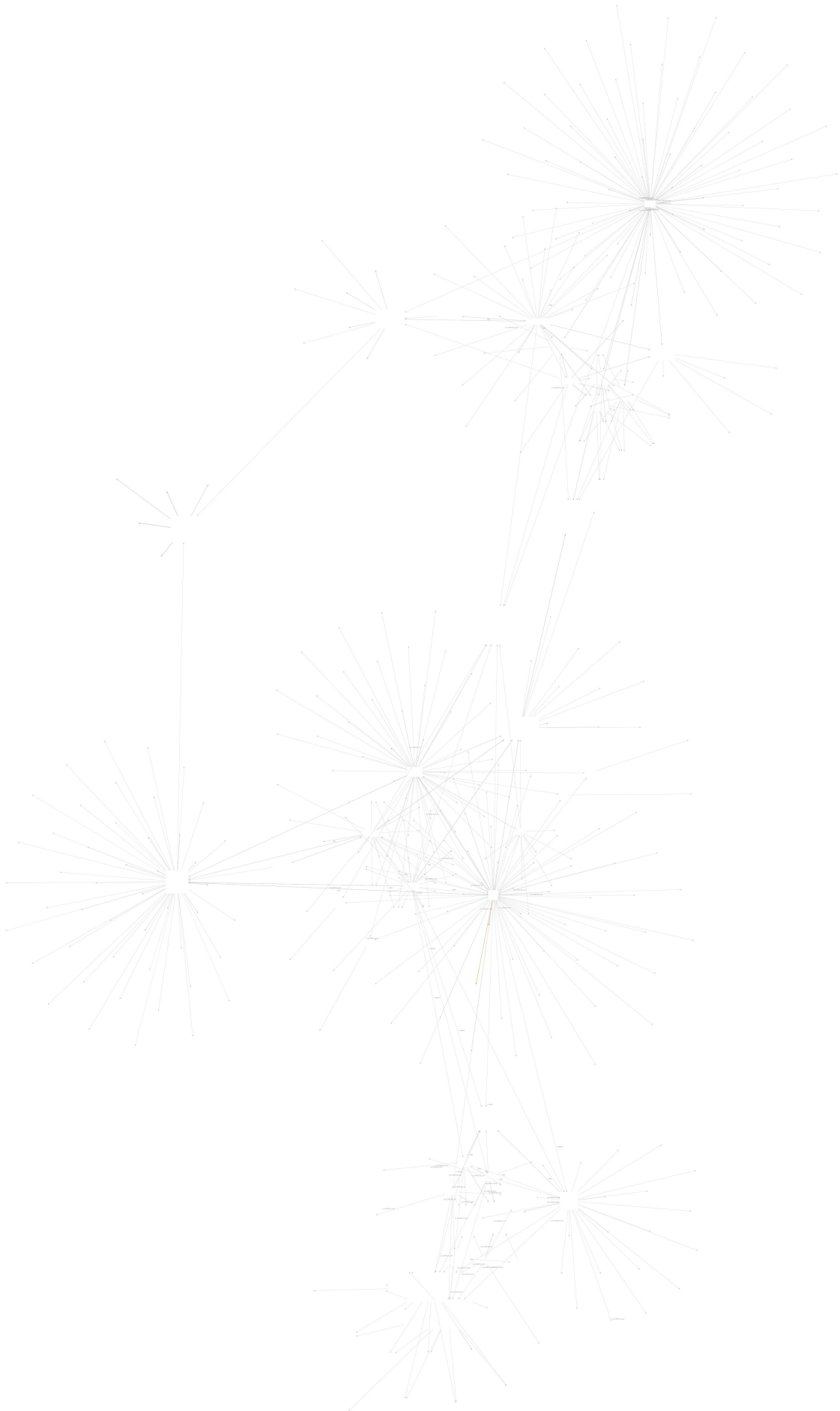


1. Top 10 Entities

Total number of entities	334
Total number of links	619

Ranked by Incoming Links

Rank	Type	Value	Incoming links
1	IPv4 Address	52.128.23.153	12
2	IPv4 Address	66.96.146.129	12
3	Domain	evil.com	11
4	Domain	evil.co	9
5	Location	United States	8
6	Shodan Tag	spf	8
7	IPv4 Address	52.86.133.10	7
8	SSL Certificate	*.evil.com	6
9	NS Record	ns2.uniregistrymarket.link	6
10	NS Record	ns1.uniregistrymarket.link	6

Ranked by Outgoing Links

Rank	Type	Value	Outgoing links
1	DNS Name	w3snoop.com	97
2	DNS Name	evil.com	85
3	DNS Name	www.evil.com	59
4	Domain	evil.com	58
5	DNS Name	apitwitter.com.w3snoop.com	36
6	DNS Name	apitwitter.evil.com	29
7	DNS Name	evil.co	27
8	DNS Name	apitwitter.com.evil.com	27
9	DNS Name	apitwitter.w3snoop.com	16
10	IPv4 Address	66.96.146.129	15

Ranked by Total Links

Rank	Type	Value	Total links
1	DNS Name	w3snoop.com	98
2	DNS Name	evil.com	87
3	Domain	evil.com	69
4	DNS Name	www.evil.com	63
5	DNS Name	apitwitter.com.w3snoop.com	37
6	DNS Name	evil.co	31
7	DNS Name	apitwitter.evil.com	30
8	DNS Name	apitwitter.com.evil.com	28
9	IPv4 Address	66.96.146.129	27
10	IPv4 Address	52.86.133.10	22

2. Entities by Type

A Records (20)	
apitwitter.com.evil.co	apitwitter.com.evil.com
apitwitter.com.w3snoop.com	apitwitter.evil.co
apitwitter.evil.com	apitwitter.w3snoop.com
com.evil.co	evil.co
evil.com	w3snoop.com
w3snoop.com	w3snoop.com
w3snoop.com	w3snoop.com
w3snoop.com	w3snoop.com
w3snoop.com	w3snoop.com
wildcard-in-use.apitwitter.evil.co	www.evil.com

Companies (6)	
Amazon Technologies Inc	Amazon Technologies Inc.
Domains By Proxy, LLC	EIG Network Operations
Endurance International Group	VeriSign

DNS Names (27)	
*.ac.uk.w3snoop.com	*.com.br.w3snoop.com
*.com.w3snoop.com	*.ee.w3snoop.com
*.evil.com	*.hr.w3snoop.com
*.hu.w3snoop.com	*.lt.w3snoop.com
*.lv.w3snoop.com	*.pk.w3snoop.com
*.pl.w3snoop.com	*.to.w3snoop.com
*.ua.w3snoop.com	apitwitter.com.evil.co
apitwitter.com.evil.com	apitwitter.com.w3snoop.com
apitwitter.evil.co	apitwitter.evil.com
apitwitter.w3snoop.com	cf-ez-middleton.w3snoop.com
com.evil.co	evil.co
evil.com	ns1.verio.com
w3snoop.com	wildcard-in-use.apitwitter.evil.co
www.evil.com	

Domains (59)	
ads.evil.com	apitwitter.com.evil.com
apitwitter.com.w3snoop.com	apitwitter.evil.co
apitwitter.evil.com	apitwitter.w3snoop.com
at.w3snoop.com	au.evil.com
bbcswahili.co.uk	box.evil.co
brandsight-whois.com	c2.evil.com
cc.w3snoop.com	chowchilla.com
co.w3snoop.com	com.evil.co
com.evil.com	com.w3snoop.com
comune.evil.co	cookiegrabber.evil.com
cz.w3snoop.com	dom.evil.co

eg.evil.com	evil.co
evil.com	fi.w3snoop.com
ggoel.co.uk	google.evil.com
hr.w3snoop.com	imap.evil.co
imap1.evil.co	imap2.evil.co
in.w3snoop.com	ir.w3snoop.com
jp.w3snoop.com	jumpershorseline.co.uk
komikaze.com	leedsbradford.co.uk
mailrelay.evil.co	mal.evil.com
mx.evil.co	mx.evil.com
mybham.co.uk	newbi.com
pimpmywebpage.com	po.evil.co
poczta.evil.co	pop3.evil.co
remotehost.evil.com	ro.w3snoop.com
some.evil.com	su.w3snoop.com
tajtour.co.uk	trly.com
villain.evil.com	volumized.com
w3snoop.com	ws.w3snoop.com
www.evil.com	

Email Addresses (28)

abuse@godaddy.com	abuse@web.com
alice@evil.com	amzn-noc-contact@amazon.com
attacker@evil.com	aws-routing-poc@amazon.com
aws-rpki-routing-poc@amazon.com	collect@evil.com
crart@evil.com	devil@evil.com
devilteachme@evil.com	domain.operations@web.com
eig-abuse@endurance.com	eig-net-team@endurance.com
eig-noc@endurance.com	evil@unspeakable-evil.com
hacker@evil.com	info@crackevil.com
info@mid-evil.com	jc9aq8n264m@networksolutionsprivateregistration.com
n69pg4637nj@networksolutionsprivateregistration.com	script@evil.com
site@evil.com	slaytanic@evil.com
talk2us@lesserevil.com	vil@unspeakable-evil.com
w3snoop.com@domainsbyproxy.com	zen@evil.com

IPv4 Addresses (29)

15.188.66.177	18.156.95.187
18.159.80.129	18.232.245.187
192.220.74.179	209.204.174.29
3.126.196.163	3.127.76.126
3.128.0.0	3.224.0.0
3.234.104.255	3.239.255.255
3.255.255.255	35.175.60.16
35.181.159.169	45.56.91.58
50.16.0.0	50.16.49.81
50.17.255.255	50.19.255.255
52.128.23.153	52.47.187.175
52.60.126.229	52.86.133.10

66.96.146.129	69.172.201.153
72.52.4.119	91.195.240.126
99.79.175.42	

LittleSis Organizations (1)

Verisign Inc. PAC

LittleSis Public Companys (1)

VeriSign, Inc.

Locations (9)

Ashburn, Virginia (United States)	Burlington
FL	Jacksonville, US
Seattle	Tempe, US
US	United States
WA	

MX Records (4)

localhost	mx.evil.com
mx.zoho.com	mx2.zoho.com

NS Records (8)

indri.ezoicns.com	ns1.uniregistrymarket.link
ns1.verio.com	ns2.uniregistrymarket.link
ns2.verio.com	saola.ezoicns.com
sheep.ezoicns.com	skunk.ezoicns.com

Peering DB Organizations (1)

VeriSign

People (6)

GoDaddy.com, LLC	NETWORK SOLUTIONS, LLC.
OrgNOCName	OrgName
OrgTechName	StateProv

Phone Numbers (7)

+1 206 266 4064	+1 480 624 2505
+1 480 624 2598	+1 570 708 8780
+1 800 333 7680	+1 877 659 6181
+1 877 722 8662	

Phrases (4)

google-site-verification=Z_UJlgtJtBjgdgQoxs4nDCo72fuLeSdHXHq8huCgmn	google-site-verification=Z_UJlgtJtBjgdgQoxs4nDCo72fuLeSdHXHq8huCgmnw
v=spf1 -all	v=spf1 ip4:66.96.128.0/18 ?all

SSL Certificates (26)

*.bizland.com	*.evil.com
*.evil.com	*.evil.com
*.evil.com	*.evil.com
*.evil.com	*.evil.com
*.evil.com	*.evil.com
*.evil.com	*.evil.com
*.evil.com	w3snoop.com
w3snoop.com	w3snoop.com
w3snoop.com	w3snoop.com
w3snoop.com	w3snoop.com
w3snoop.com	w3snoop.com
w3snoop.com	w3snoop.com
w3snoop.com	w3snoop.com

Shodan Tags (1)

spf

Snapshots (21)

1996 Dec 29: http://www.evil.com:80/	1997 Feb 04: http://www.evil.com:80/
1997 Oct 14: http://www.evil.com:80/	1998 Dec 05: http://www.evil.com:80/
1998 Dec 12: http://www.evil.com:80/	1999 Feb 02: http://www.evil.com:80/
1999 Feb 03: http://evil.com:80/	1999 Jan 25: http://evil.com:80/
1999 Jan 25: http://www.evil.com:80/	2000 Apr 07: http://www.evil.com:80/
2000 Feb 29: http://www.evil.com:80/	2000 Jun 21: http://www.evil.com:80/
2000 Jun 21: http://www.evil.com:80/	2000 Jun 21: http://www.evil.com:80/
2000 Mar 03: http://www.evil.com:80/	2000 Mar 04: http://www.evil.com:80/
2000 May 11: http://www.evil.com:80/	2000 Oct 17: http://www.evil.com:80/
2000 Oct 18: http://www.evil.com:80/	2000 Oct 18: http://www.evil.com:80/
2000 Oct 19: http://www.evil.com:80/	

VirusTotal Categorys (4)

Entertainment	entertainment
hobbies	information technology

VirusTotal Comments (2)

Evil.com is reco...	I Mean Makes sen...

VirusTotal Files (45)

01217b1a3f83a64c45533f31f51b12fb56e60b89b079a641e8cdf3e868a612ad	06-gotor-action.pdf
15-bro-x32.exe	15-bro-x32[1].exe
25c55cd1571c3bab3a1db71f26d7b20c4c4f0ae46374f0db251c2febaf0cd9e6	4646-apk.apk
9038431d73550aedf97d341faef1025c.virus	BlackBelt Privacy PostFF57 10.2021.10.1.exe
MalwareDropper.pdf.exe	Release NDD NFS-e Core_6103_26290.exe
SMServer_x32_Setup.exe	SMServer_x32_Setup.exe
Speed Booster [Android].xlsx	StackOverflowData.csv

VpnSetup.exe	VpnSetup.exe
Zalando-Rechnung-234541.pdf .exe	all_data.tar
appke.exe	b37bea1d85faf990730dff11fbfc5c71c9ac4c3a472c77c6ecf9b41b675c908b~
b99e813023393fd166ed3d053c41fdb987d74d2dec3fd4e4e4535105d605e0f2	bbagrfmp.exe
binded_server.exe	check-client.phar
code-editor-master.tar	d8307ef63337fa211962ef4cebdacb240ffd079fdccad3ba2a4e3d1c05553d39
ddd7d622dc5517e202383bc7d02fb333ceac8b6f4b9c4bceef96a302b732297b	deccab.exe
degrees-of-lewdity-rus.tar	dropper.exe
ebcd1eb0db969353c12284a3c36f958ff9ab6a9a1a113ea8a89cad0cefbf10f3	evilback.exe.bin
explorer.exe	gibmtbpf.exe
ib_logfile2 - Copy	minilab_3-1.exe
notevil.exe	notevil_50M.exe
places.sqlite	pnuqpywn.exe
prefs-2.js	svowuweo.exe
web hacking tutorial.doc	yfighhxl.exe
Солодушкин_С_И_Разработка_программных_комплексов_на_языке_JavaScript.pdf	

WHOIS Records (15)

apitwitter.com.w3snoop.com	evil.co
evil.co	evil.co
evil.com	evil.com
evil.com	evil.com
w3snoop.com	w3snoop.com
w3snoop.com	www.evil.com
www.evil.com	www.evil.com
www.evil.com	

Websites (4)

apitwitter.com.evil.com	apitwitter.com.w3snoop.com
evil.com	www.apitwitter.evil.co

X509 Certificate (4)

x509-certificate--1ce7e13b-39f8-5d85-94ab-7567aadfe9d9	x509-certificate--87052faa-ce0b-55a0-b253-95e2150038fc
x509-certificate--e72c2a81-44d5-5c56-b9fb-9cc476194843	x509-certificate--f2d07fae-c770-5241-b074-1ad8137ce391

maltego.PeeringDBNetworks (2)

VeriSign Global Registry Services	Verisign

3. Entity Details

DNS Name

maltego.DNSName

w3snoop.com

Weight	0
DNS Name	w3snoop.com
Context	apitwitter.com.w3snoop.co

Incoming (1)		
	DNS Name	apitwitter.com.w3snoop.com
Outgoing (97)		
	A Record	w3snoop.com
	A Record	w3snoop.com
	A Record	w3snoop.com
	A Record	w3snoop.com
	A Record	w3snoop.com
	A Record	w3snoop.com
	A Record	w3snoop.com
	A Record	w3snoop.com
	A Record	w3snoop.com
	A Record	w3snoop.com
	DNS Name	*.ac.uk.w3snoop.com
	DNS Name	*.ac.uk.w3snoop.com
	DNS Name	*.com.br.w3snoop.com
	DNS Name	*.com.br.w3snoop.com
	DNS Name	*.com.w3snoop.com
	DNS Name	*.ee.w3snoop.com
	DNS Name	*.ee.w3snoop.com
	DNS Name	*.hr.w3snoop.com
	DNS Name	*.hr.w3snoop.com
	DNS Name	*.hu.w3snoop.com
	DNS Name	*.hu.w3snoop.com
	DNS Name	*.lt.w3snoop.com
	DNS Name	*.lt.w3snoop.com
	DNS Name	*.lv.w3snoop.com
	DNS Name	*.lv.w3snoop.com
	DNS Name	*.pk.w3snoop.com
	DNS Name	*.pk.w3snoop.com
	DNS Name	*.pl.w3snoop.com
	DNS Name	*.to.w3snoop.com
	DNS Name	*.to.w3snoop.com
	DNS Name	*.ua.w3snoop.com
	DNS Name	*.ua.w3snoop.com
	DNS Name	cf-ez-middleton.w3snoop.com
	DNS Name	cf-ez-middleton.w3snoop.com
	Domain	apitwitter.w3snoop.com
	Domain	at.w3snoop.com
	Domain	cc.w3snoop.com
	Domain	co.w3snoop.com
	Domain	cz.w3snoop.com
	Domain	fi.w3snoop.com
	Domain	hr.w3snoop.com
	Domain	in.w3snoop.com
	Domain	ir.w3snoop.com
	Domain	jp.w3snoop.com
	Domain	ro.w3snoop.com
	Domain	su.w3snoop.com
	Domain	w3snoop.com

IPv4 Address	15.188.66.177
IPv4 Address	18.156.95.187
IPv4 Address	18.232.245.187
IPv4 Address	18.232.245.187
IPv4 Address	3.126.196.163
IPv4 Address	3.127.76.126
IPv4 Address	3.234.104.255
IPv4 Address	3.234.104.255
IPv4 Address	35.175.60.16
IPv4 Address	35.175.60.16
IPv4 Address	35.181.159.169
IPv4 Address	50.16.49.81
IPv4 Address	50.16.49.81
IPv4 Address	52.47.187.175
IPv4 Address	52.60.126.229
IPv4 Address	52.86.133.10
IPv4 Address	52.86.133.10
IPv4 Address	99.79.175.42
MX Record	mx.zoho.com
MX Record	mx2.zoho.com
NS Record	indri.ezoicns.com
NS Record	saola.ezoicns.com
NS Record	saola.ezoicns.com
NS Record	sheep.ezoicns.com
NS Record	skunk.ezoicns.com
Phrase	google-site-verification=Z_UJlgtJtBjgdgQoxs4nDCo72fuLeSdHXHq8huCgmn
Phrase	google-site-verification=Z_UJlgtJtBjgdgQoxs4nDCo72fuLeSdHXHq8huCgmnw
SSL Certificate	w3snoop.com
SSL Certificate	w3snoop.com
SSL Certificate	w3snoop.com
SSL Certificate	w3snoop.com
SSL Certificate	w3snoop.com
SSL Certificate	w3snoop.com
SSL Certificate	w3snoop.com
SSL Certificate	w3snoop.com
SSL Certificate	w3snoop.com
SSL Certificate	w3snoop.com
SSL Certificate	w3snoop.com
SSL Certificate	w3snoop.com
SSL Certificate	w3snoop.com
SSL Certificate	w3snoop.com
Shodan Tag	spf
VirusTotal Category	information technology
VirusTotal File	4646-apk.apk
VirusTotal File	Speed Booster [Android].xlsx
VirusTotal File	deccab.exe
VirusTotal File	places.sqlite
VirusTotal File	prefs-2.js
WHOIS Record	w3snoop.com

WHOIS Record	w3snoop.com
WHOIS Record	w3snoop.com

DNS Name

maltego.DNSName

evil.com

Weight	0
DNS Name	evil.com
Context	apitwitter.evil.co

Incoming (2)	
DNS Name	apitwitter.com.evil.com
DNS Name	apitwitter.evil.com
Outgoing (85)	
A Record	evil.com
A Record	evil.com
DNS Name	*.evil.com
DNS Name	*.evil.com
DNS Name	apitwitter.evil.co
DNS Name	evil.co
DNS Name	ns1.verio.com
DNS Name	www.evil.com
DNS Name	www.evil.com
Domain	ads.evil.com
Domain	apitwitter.evil.com
Domain	au.evil.com
Domain	cookiegrabber.evil.com
Domain	eg.evil.com
Domain	evil.co
Domain	evil.com
Domain	evil.com
Domain	evil.com
Domain	google.evil.com
Domain	mal.evil.com
Domain	mx.evil.com
Domain	remotehost.evil.com
Domain	some.evil.com
Domain	villain.evil.com
Domain	www.evil.com
IPv4 Address	192.220.74.179
IPv4 Address	209.204.174.29
IPv4 Address	45.56.91.58
IPv4 Address	66.96.146.129
IPv4 Address	66.96.146.129
IPv4 Address	66.96.146.129
MX Record	mx.evil.com
MX Record	mx.evil.com
NS Record	ns1.verio.com
NS Record	ns1.verio.com
NS Record	ns2.verio.com
NS Record	ns2.verio.com
Phrase	v=spf1 ip4:66.96.128.0/18 ?all
Phrase	v=spf1 ip4:66.96.128.0/18 ?all
SSL Certificate	*.evil.com
SSL Certificate	*.evil.com
SSL Certificate	*.evil.com
SSL Certificate	*.evil.com
SSL Certificate	*.evil.com
SSL Certificate	*.evil.com
SSL Certificate	*.evil.com

SSL Certificate	*.evil.com
SSL Certificate	*.evil.com
SSL Certificate	*.evil.com
SSL Certificate	*.evil.com
SSL Certificate	*.evil.com
SSL Certificate	*.evil.com
Shodan Tag	spf
VirusTotal Category	Entertainment
VirusTotal Comment	Evil.com is reco...
VirusTotal Comment	I Mean Makes sen...
VirusTotal File	06-gotor-action.pdf
VirusTotal File	15-bro-x32.exe
VirusTotal File	15-bro-x32[1].exe
VirusTotal File	9038431d73550aedf97d341faef1025c.virus
VirusTotal File	BlackBelt Privacy PostFF57 10.2021.10.1.exe
VirusTotal File	Release NDD NFS-e Core_6103_26290.exe
VirusTotal File	SMServer_x32_Setup.exe
VirusTotal File	SMServer_x32_Setup.exe
VirusTotal File	VpnSetup.exe
VirusTotal File	VpnSetup.exe
VirusTotal File	b37bea1d85faf990730dff11fbfc5c71c9ac4c3a472c77c6ecf9b41b675c908b~
VirusTotal File	bbagrfmp.exe
VirusTotal File	binded_server.exe
VirusTotal File	ddd7d622dc5517e202383bc7d02fb333ceac8b6f4b9c4bceef96a302b732297b
VirusTotal File	dropper.exe
VirusTotal File	ebcd1eb0db969353c12284a3c36f958ff9ab6a9a1a113ea8a89cad0cefbf10f3
VirusTotal File	evilback.exe.bin
VirusTotal File	gibmtbpf.exe
VirusTotal File	notevil.exe
VirusTotal File	notevil_50M.exe
VirusTotal File	pnuqpywn.exe
VirusTotal File	svowuweo.exe
VirusTotal File	yfighhxl.exe
VirusTotal File	Солодушкин_С_И_Разработка_программных_комплексов_на_языке_JavaScript.pdf
WHOIS Record	evil.com
WHOIS Record	evil.com
WHOIS Record	evil.com
WHOIS Record	evil.com
Website	evil.com

Domain

maltego.Domain

evil.com

Weight	6
Domain Name	evil.com
WHOIS Info	Creation Date: 1995-04-10T04:00:00Z DNSSEC: unsigned Domain Name: EVIL.COM Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited Name Server: NS1.VERIO.COM Name Server: NS2.VERIO.COM Registrar Abuse Contact Email: abuse@web.com Registrar Abuse Contact Phone: +1.8003337680 Registrar IANA ID: 2 Registrar URL: http://networksolutions.com Registrar WHOIS Server: whois.networksolutions.com Registrar: Network Solutions, LLC Registry Domain ID: 1040763_DOMAIN_COM-VRSN Registry Expiry Date: 2023-04-11T04:00:00Z Updated Date: 2019-12-17T16:17:59Z
Context	evil.co

VirusTotal Domain Summary

VirusTotal Reputation	-1
Tags	
Popularity Ranking	
Majestic	
415577	
Statvoo	
581630	
Alexa	
581630	
Cisco Umbrella	
922584	

VirusTotal Analysis Summary

Aggregate Result	harmless - 78 / 87

VirusTotal Analysis Stats

Analysis Type	Number of Analysis
Confirmed Timeout	0
Failure	0
Harmless	78
Malicious	0
Suspicious	0
Timeout	0
Type Unsupported	0
Undetected	9
Total	**87**

View on VirusTotal

GUI Url: https://www.virustotal.com/gui/domain/evil.com

Categories

Engines	Category
alphaMountain.ai	Entertainment

Community Votes

Total votes cast: 1

Harmless: 0/1
Malicious: 1/1

Incoming (11)	
DNS Name	apitwitter.com.evil.com
DNS Name	apitwitter.com.evil.com
DNS Name	apitwitter.evil.com
DNS Name	apitwitter.evil.com
DNS Name	apitwitter.evil.com
DNS Name	evil.com
DNS Name	evil.com
DNS Name	evil.com
DNS Name	www.evil.com
DNS Name	www.evil.com
Website	apitwitter.com.evil.com
Outgoing (58)	
Company	VeriSign
Email Address	abuse@web.com
Email Address	abuse@web.com
Email Address	alice@evil.com
Email Address	attacker@evil.com
Email Address	collect@evil.com
Email Address	crart@evil.com
Email Address	devil@evil.com
Email Address	devilteachme@evil.com
Email Address	domain.operations@web.com
Email Address	domain.operations@web.com
Email Address	evil@unspeakable-evil.com
Email Address	hacker@evil.com
Email Address	info@crackevil.com
Email Address	info@mid-evil.com
Email Address	jc9aq8n264m@networksolutionsprivateregistration.com
Email Address	jc9aq8n264m@networksolutionsprivateregistration.com
Email Address	n69pg4637nj@networksolutionsprivateregistration.com
Email Address	n69pg4637nj@networksolutionsprivateregistration.com
Email Address	script@evil.com
Email Address	site@evil.com
Email Address	slaytanic@evil.com
Email Address	talk2us@lesserevil.com
Email Address	vil@unspeakable-evil.com
Email Address	zen@evil.com
Location	FL
Location	Jacksonville, US
Person	NETWORK SOLUTIONS, LLC.
Phone Number	+1 570 708 8780
Phone Number	+1 570 708 8780
Phone Number	+1 800 333 7680
Phone Number	+1 800 333 7680
Phone Number	+1 877 722 8662
Phone Number	+1 877 722 8662
Snapshot	1996 Dec 29: http://www.evil.com:80/
Snapshot	1997 Feb 04: http://www.evil.com:80/
Snapshot	1997 Oct 14: http://www.evil.com:80/

Snapshot	1998 Dec 05: http://www.evil.com:80/
Snapshot	1998 Dec 12: http://www.evil.com:80/
Snapshot	1999 Feb 02: http://www.evil.com:80/
Snapshot	1999 Feb 03: http://evil.com:80/
Snapshot	1999 Jan 25: http://evil.com:80/
Snapshot	1999 Jan 25: http://www.evil.com:80/
Snapshot	2000 Apr 07: http://www.evil.com:80/
Snapshot	2000 Feb 29: http://www.evil.com:80/
Snapshot	2000 Feb 29: http://www.evil.com:80/
Snapshot	2000 Jun 21: http://www.evil.com:80/
Snapshot	2000 Jun 21: http://www.evil.com:80/
Snapshot	2000 Jun 21: http://www.evil.com:80/
Snapshot	2000 Mar 03: http://www.evil.com:80/
Snapshot	2000 Mar 03: http://www.evil.com:80/
Snapshot	2000 Mar 04: http://www.evil.com:80/
Snapshot	2000 Mar 04: http://www.evil.com:80/
Snapshot	2000 May 11: http://www.evil.com:80/
Snapshot	2000 Oct 17: http://www.evil.com:80/
Snapshot	2000 Oct 18: http://www.evil.com:80/
Snapshot	2000 Oct 18: http://www.evil.com:80/
Snapshot	2000 Oct 19: http://www.evil.com:80/

DNS Name

maltego.DNSName

www.evil.com

Weight	0
DNS Name	www.evil.com

Incoming (4)	
DNS Name	evil.com
DNS Name	evil.com
Website	evil.com
Website	evil.com
Outgoing (59)	
A Record	www.evil.com
A Record	www.evil.com
Domain	ads.evil.com
Domain	apitwitter.evil.com
Domain	au.evil.com
Domain	c2.evil.com
Domain	cookiegrabber.evil.com
Domain	eg.evil.com
Domain	evil.com
Domain	evil.com
Domain	google.evil.com
Domain	mal.evil.com
Domain	mx.evil.com
Domain	remotehost.evil.com
Domain	some.evil.com
Domain	villain.evil.com
Domain	www.evil.com
IPv4 Address	192.220.74.179
IPv4 Address	209.204.174.29
IPv4 Address	66.96.146.129
IPv4 Address	66.96.146.129
MX Record	mx.evil.com
SSL Certificate	*.evil.com
SSL Certificate	*.evil.com
SSL Certificate	*.evil.com
SSL Certificate	*.evil.com
SSL Certificate	*.evil.com
SSL Certificate	*.evil.com
SSL Certificate	*.evil.com
SSL Certificate	*.evil.com
SSL Certificate	*.evil.com
SSL Certificate	*.evil.com
SSL Certificate	*.evil.com
SSL Certificate	*.evil.com
SSL Certificate	*.evil.com
Shodan Tag	spf
VirusTotal Category	entertainment
VirusTotal Category	hobbies
VirusTotal File	01217b1a3f83a64c45533f31f51b12fb56e60b89b079a641e8cdf3e868a612ad
VirusTotal File	25c55cd1571c3bab3a1db71f26d7b20c4c4f0ae46374f0db251c2febaf0cd9e6
VirusTotal File	MalwareDropper.pdf.exe
VirusTotal File	StackOverflowData.csv

VirusTotal File	Zalando-Rechnung-234541.pdf .exe
VirusTotal File	all_data.tar
VirusTotal File	appke.exe
VirusTotal File	b99e813023393fd166ed3d053c41fdb987d74d2dec3fd4e4e4535105d605e0f2
VirusTotal File	check-client.phar
VirusTotal File	code-editor-master.tar
VirusTotal File	d8307ef63337fa211962ef4cebdacb240ffd079fdccad3ba2a4e3d1c05553d39
VirusTotal File	degrees-of-lewdity-rus.tar
VirusTotal File	explorer.exe
VirusTotal File	explorer.exe
VirusTotal File	ib_logfile2 - Copy
VirusTotal File	minilab_3-1.exe
VirusTotal File	web hacking tutorial.doc
WHOIS Record	www.evil.com
WHOIS Record	www.evil.com
WHOIS Record	www.evil.com
WHOIS Record	www.evil.com

DNS Name

maltego.DNSName

apitwitter.com.w3snoop.com

Weight	10
DNS Name	apitwitter.com.w3snoop.com
DNSDB JSON Output	{"count": 3, "time_first": 1520301970, "time_last": 1520301971, "rrname": "apitwitter.com.w3snoop.com.", "rrtype": "CNAME", "bailiwick": "w3snoop.com.", "rdata": "w3snoop.com."}

DNSDB JSON Output

{"count": 2, "time_first": 1555029159, "time_last": 1555029159, "rrname": "apitwitter.com.w3snoop.com.", "rrtype": "A", "bailiwick": "w3snoop.com.", "rdata": "18.195.122.112"}

DNSDB JSON Output

{"count": 2, "time_first": 1558494374, "time_last": 1558494374, "rrname": "apitwitter.com.w3snoop.com.", "rrtype": "A", "bailiwick": "w3snoop.com.", "rdata": "18.197.0.7"}

DNSDB JSON Output

{"count": 18, "time_first": 1454605804, "time_last": 1512134580, "rrname": "apitwitter.com.w3snoop.com.", "rrtype": "A", "bailiwick": "w3snoop.com.", "rdata": "173.199.149.76"}

DNSDB JSON Output

{"count": 3, "time_first": 1520301970, "time_last": 1520301971, "rrname": "apitwitter.com.w3snoop.com.", "rrtype": "CNAME", "bailiwick": "w3snoop.com.", "rdata": "w3snoop.com."}

Incoming (1)	
Website	apitwitter.com.w3snoop.com
Outgoing (36)	
A Record	apitwitter.com.w3snoop.com
DNS Name	apitwitter.w3snoop.com
DNS Name	w3snoop.com
Domain	apitwitter.com.w3snoop.com
Domain	at.w3snoop.com
Domain	cc.w3snoop.com
Domain	co.w3snoop.com
Domain	com.w3snoop.com
Domain	cz.w3snoop.com
Domain	fi.w3snoop.com
Domain	hr.w3snoop.com
Domain	in.w3snoop.com
Domain	ir.w3snoop.com
Domain	jp.w3snoop.com
Domain	ro.w3snoop.com
Domain	su.w3snoop.com
Domain	w3snoop.com
Domain	w3snoop.com
Domain	ws.w3snoop.com
IPv4 Address	18.159.80.129
IPv4 Address	18.232.245.187
IPv4 Address	18.232.245.187
IPv4 Address	3.127.76.126
IPv4 Address	3.234.104.255
IPv4 Address	3.234.104.255
IPv4 Address	35.175.60.16
IPv4 Address	35.175.60.16
IPv4 Address	50.16.49.81
IPv4 Address	50.16.49.81
IPv4 Address	52.86.133.10
IPv4 Address	52.86.133.10
SSL Certificate	w3snoop.com
SSL Certificate	w3snoop.com
Shodan Tag	spf
WHOIS Record	apitwitter.com.w3snoop.com
Website	apitwitter.com.w3snoop.com

DNS Name

maltego.DNSName

evil.co

Weight	0
DNS Name	evil.co
Context	apitwitter.evil.c

Incoming (4)	
DNS Name	apitwitter.com.evil.co
DNS Name	apitwitter.evil.com
DNS Name	com.evil.co
DNS Name	evil.com
Outgoing (27)	
A Record	evil.co
Domain	box.evil.co
Domain	com.evil.co
Domain	comune.evil.co
Domain	dom.evil.co
Domain	evil.co
Domain	evil.co
Domain	imap.evil.co
Domain	imap1.evil.co
Domain	imap2.evil.co
Domain	mailrelay.evil.co
Domain	mx.evil.co
Domain	po.evil.co
Domain	poczta.evil.co
Domain	pop3.evil.co
IPv4 Address	52.128.23.153
IPv4 Address	52.128.23.153
IPv4 Address	69.172.201.153
IPv4 Address	72.52.4.119
IPv4 Address	91.195.240.126
MX Record	localhost
NS Record	ns1.uniregistrymarket.link
NS Record	ns2.uniregistrymarket.link
Phrase	v=spf1 -all
WHOIS Record	evil.co
WHOIS Record	evil.co
WHOIS Record	evil.co

DNS Name

maltego.DNSName

apitwitter.evil.com

Weight	0
DNS Name	apitwitter.evil.com
Context	apitwitter.evil.co

Incoming (1)	
DNS Name	apitwitter.com.evil.com

Outgoing (29)	
A Record	apitwitter.evil.com
DNS Name	apitwitter.com.evil.co
DNS Name	com.evil.co
DNS Name	evil.co
DNS Name	evil.com
Domain	ads.evil.com
Domain	apitwitter.evil.com
Domain	au.evil.com
Domain	c2.evil.com
Domain	cookiegrabber.evil.com
Domain	eg.evil.com
Domain	evil.co
Domain	evil.com
Domain	evil.com
Domain	evil.com
Domain	google.evil.com
Domain	mal.evil.com
Domain	mx.evil.com
Domain	remotehost.evil.com
Domain	some.evil.com
Domain	villain.evil.com
Domain	www.evil.com
IPv4 Address	66.96.146.129
IPv4 Address	66.96.146.129
IPv4 Address	66.96.146.129
MX Record	mx.evil.com
SSL Certificate	*.evil.com
SSL Certificate	*.evil.com
Shodan Tag	spf

DNS Name

maltego.DNSName

apitwitter.com.evil.com

Weight	3
DNS Name	apitwitter.com.evil.com
DNSDB JSON Output	{"count": 3, "time_first": 1614290179, "time_last": 1622789802, "rrname": "apitwitter.com.evil.com.", "rrtype": "A", "bailiwick": "evil.com.", "rdata": "66.96.146.129"}

DNSDB JSON Output

{"count": 3, "time_first": 1614290179, "time_last": 1622789802, "rrname": "apitwitter.com.evil.com.", "rrtype": "A", "bailiwick": "evil.com.", "rdata": "66.96.146.129"}

Incoming (1)		
	Website	apitwitter.com.evil.com
Outgoing (27)		
	A Record	apitwitter.com.evil.com
	DNS Name	apitwitter.evil.com
	DNS Name	evil.com
	Domain	ads.evil.com
	Domain	apitwitter.com.evil.com
	Domain	apitwitter.evil.com
	Domain	au.evil.com
	Domain	com.evil.com
	Domain	cookiegrabber.evil.com
	Domain	eg.evil.com
	Domain	evil.com
	Domain	evil.com
	Domain	google.evil.com
	Domain	mal.evil.com
	Domain	mx.evil.com
	Domain	remotehost.evil.com
	Domain	some.evil.com
	Domain	villain.evil.com
	Domain	www.evil.com
	IPv4 Address	66.96.146.129
	IPv4 Address	66.96.146.129
	IPv4 Address	66.96.146.129
	MX Record	mx.evil.com
	SSL Certificate	*.bizland.com
	SSL Certificate	*.bizland.com
	Shodan Tag	spf
	Website	apitwitter.com.evil.com

IPv4 Address

maltego.IPv4Address

66.96.146.129

Weight	12
IP Address	66.96.146.129
Internal	false
Date Resolved	2021-10-11T07:09:49Z
Resolver	VirusTotal

IP whois

```
#
# ARIN WHOIS data and services are subject to the Terms of Use
# available at: https://www.arin.net/resources/registry/whois/tou/
#
# If you see inaccuracies in the results, please report at
# https://www.arin.net/resources/registry/whois/inaccuracy_reporting/
#
# Copyright 1997-2021, American Registry for Internet Numbers, Ltd.
#


#
# Query terms are ambiguous.  The query is assumed to be:
#     "n 66.96.146.129"
#
# Use "?" to get help.
#

NetRange:       66.96.128.0 - 66.96.191.255
CIDR:           66.96.128.0/18
NetName:        BIZLAND-FC01
NetHandle:      NET-66-96-128-0-1
Parent:         NET66 (NET-66-0-0-0-0)
NetType:        Direct Allocation
OriginAS:
Organization:   The Endurance International Group, Inc. (EIG-12)
RegDate:        2001-04-03
Updated:        2012-03-02
Comment:        ADDRESSES WITHIN THIS BLOCK ARE NON-PORTABLE
Ref:            https://rdap.arin.net/registry/ip/66.96.128.0


OrgName:        The Endurance International Group, Inc.
OrgId:          EIG-12
Address:        10 Corporate Drive
Address:        Suite 300
City:           Burlington
StateProv:      MA
PostalCode:     01803
Country:        US
RegDate:        2005-02-07
Updated:        2019-11-08
Ref:            https://rdap.arin.net/registry/entity/EIG-12


OrgAbuseHandle: EIGAB-ARIN
OrgAbuseName:   eig-abuse
OrgAbusePhone:  +1-877-659-6181
OrgAbuseEmail:  eig-abuse@endurance.com
OrgAbuseRef:    https://rdap.arin.net/registry/entity/EIGAB-ARIN

OrgNOCHandle: ENO74-ARIN
OrgNOCName:   EIG Network Operations
OrgNOCPhone:  +1-877-659-6181
OrgNOCEmail:  eig-net-team@endurance.com
OrgNOCRef:    https://rdap.arin.net/registry/entity/ENO74-ARIN

OrgTechHandle: ENO74-ARIN
OrgTechName:   EIG Network Operations
OrgTechPhone:  +1-877-659-6181
OrgTechEmail:  eig-net-team@endurance.com
OrgTechRef:    https://rdap.arin.net/registry/entity/ENO74-ARIN


#
# ARIN WHOIS data and services are subject to the Terms of Use
# available at: https://www.arin.net/resources/registry/whois/tou/
#
# If you see inaccuracies in the results, please report at
# https://www.arin.net/resources/registry/whois/inaccuracy_reporting/
#
# Copyright 1997-2021, American Registry for Internet Numbers, Ltd.
#
```

Incoming (12)	
DNS Name	apitwitter.com.evil.com
DNS Name	apitwitter.com.evil.com
DNS Name	apitwitter.com.evil.com
DNS Name	apitwitter.evil.com
DNS Name	apitwitter.evil.com
DNS Name	apitwitter.evil.com
DNS Name	evil.com
DNS Name	evil.com
DNS Name	evil.com
DNS Name	www.evil.com
DNS Name	www.evil.com
Website	evil.com
Outgoing (15)	
Company	EIG Network Operations
Company	Endurance International Group
Email Address	eig-abuse@endurance.com
Email Address	eig-abuse@endurance.com
Email Address	eig-net-team@endurance.com
Email Address	eig-noc@endurance.com
Location	Burlington
Location	United States
Location	United States
Location	United States
Person	OrgNOCName
Person	OrgName
Person	OrgTechName
Person	StateProv
Phone Number	+1 877 659 6181

IPv4 Address

maltego.IPv4Address

52.86.133.10

Weight	25
IP Address	52.86.133.10
Internal	false
Date Resolved	2021-10-11T07:09:57Z
Resolver	VirusTotal

IP whois

```
#
# ARIN WHOIS data and services are subject to the Terms of Use
# available at: https://www.arin.net/resources/registry/whois/tou/
#
# If you see inaccuracies in the results, please report at
# https://www.arin.net/resources/registry/whois/inaccuracy_reporting/
#
# Copyright 1997-2021, American Registry for Internet Numbers, Ltd.
#


#
# Query terms are ambiguous.  The query is assumed to be:
#     "n 52.86.133.10"
#
# Use "?" to get help.
#

NetRange:       52.84.0.0 - 52.95.255.255
CIDR:           52.88.0.0/13, 52.84.0.0/14
NetName:        AT-88-Z
NetHandle:      NET-52-84-0-0-1
Parent:         NET52 (NET-52-0-0-0-0)
NetType:        Direct Allocation
OriginAS:       AS16509, AS14618
Organization:   Amazon Technologies Inc. (AT-88-Z)
RegDate:        1991-12-19
Updated:        2018-02-27
Ref:            https://rdap.arin.net/registry/ip/52.84.0.0


OrgName:        Amazon Technologies Inc.
OrgId:          AT-88-Z
Address:        410 Terry Ave N.
City:           Seattle
StateProv:      WA
PostalCode:     98109
Country:        US
RegDate:        2011-12-08
Updated:        2021-07-28
Comment:        All abuse reports MUST include:
Comment:        * src IP
Comment:        * dest IP (your IP)
Comment:        * dest port
Comment:        * Accurate date/timestamp and timezone of activity
Comment:        * Intensity/frequency (short log extracts)
Comment:        * Your contact details (phone and email) Without these we will
be unable to identify the correct owner of the IP address at that point in time.
Ref:            https://rdap.arin.net/registry/entity/AT-88-Z


OrgRoutingHandle: IPROU3-ARIN
OrgRoutingName:   IP Routing
OrgRoutingPhone:  +1-206-266-4064
OrgRoutingEmail:  aws-routing-poc@amazon.com
OrgRoutingRef:    https://rdap.arin.net/registry/entity/IPROU3-ARIN

OrgRoutingHandle: ARMP-ARIN
OrgRoutingName:   AWS RPKI Management POC
OrgRoutingPhone:  +1-206-266-4064
OrgRoutingEmail:  aws-rpki-routing-poc@amazon.com
OrgRoutingRef:    https://rdap.arin.net/registry/entity/ARMP-ARIN

OrgTechHandle: ANO24-ARIN
OrgTechName:   Amazon EC2 Network Operations
OrgTechPhone:  +1-206-266-4064
OrgTechEmail:  amzn-noc-contact@amazon.com
OrgTechRef:    https://rdap.arin.net/registry/entity/ANO24-ARIN

OrgNOCHandle: AANO1-ARIN
OrgNOCName:   Amazon AWS Network Operations
OrgNOCPhone:  +1-206-266-4064
OrgNOCEmail:  amzn-noc-contact@amazon.com
OrgNOCRef:    https://rdap.arin.net/registry/entity/AANO1-ARIN

OrgAbuseHandle: AEA8-ARIN
```

OrgAbuseHandle: AEA8-ARIN
OrgAbuseName: Amazon EC2 Abuse
OrgAbusePhone: +1-206-266-4064
OrgAbuseEmail: abuse@amazonaws.com
OrgAbuseRef: https://rdap.arin.net/registry/entity/AEA8-ARIN

#
ARIN WHOIS data and services are subject to the Terms of Use
available at: https://www.arin.net/resources/registry/whois/tou/
#
If you see inaccuracies in the results, please report at
https://www.arin.net/resources/registry/whois/inaccuracy_reporting/
#
Copyright 1997-2021, American Registry for Internet Numbers, Ltd.
#

Incoming (7)	
DNS Name	apitwitter.com.w3snoop.com
DNS Name	apitwitter.com.w3snoop.com
DNS Name	apitwitter.w3snoop.com
DNS Name	apitwitter.w3snoop.com
DNS Name	apitwitter.w3snoop.com
DNS Name	w3snoop.com
DNS Name	w3snoop.com

Outgoing (15)	
Company	Amazon Technologies Inc
Company	Amazon Technologies Inc.
Email Address	amzn-noc-contact@amazon.com
Email Address	amzn-noc-contact@amazon.com
Email Address	aws-routing-poc@amazon.com
Email Address	aws-routing-poc@amazon.com
Email Address	aws-rpki-routing-poc@amazon.com
Email Address	aws-rpki-routing-poc@amazon.com
Location	Ashburn, Virginia (United States)
Location	Seattle
Location	US
Location	United States
Location	WA
Person	StateProv
Phone Number	+1 206 266 4064

IPv4 Address

maltego.IPv4Address

35.175.60.16

Weight	50
IP Address	35.175.60.16
Internal	false
Date Resolved	2020-05-01T14:36:21Z
Resolver	VirusTotal

IP whois

```
#
# ARIN WHOIS data and services are subject to the Terms of Use
# available at: https://www.arin.net/resources/registry/whois/tou/
#
# If you see inaccuracies in the results, please report at
# https://www.arin.net/resources/registry/whois/inaccuracy_reporting/
#
# Copyright 1997-2021, American Registry for Internet Numbers, Ltd.
#


#
# Query terms are ambiguous.  The query is assumed to be:
#     "n 35.175.60.16"
#
# Use "?" to get help.
#

NetRange:       35.152.0.0 - 35.183.255.255
CIDR:           35.176.0.0/13, 35.160.0.0/12, 35.152.0.0/13
NetName:        AT-88-Z
NetHandle:      NET-35-152-0-0-1
Parent:         NET35 (NET-35-0-0-0-0)
NetType:        Direct Allocation
OriginAS:
Organization:   Amazon Technologies Inc. (AT-88-Z)
RegDate:        2016-08-09
Updated:        2016-08-09
Ref:            https://rdap.arin.net/registry/ip/35.152.0.0



OrgName:        Amazon Technologies Inc.
OrgId:          AT-88-Z
Address:        410 Terry Ave N.
City:           Seattle
StateProv:      WA
PostalCode:     98109
Country:        US
RegDate:        2011-12-08
Updated:        2021-07-28
Comment:        All abuse reports MUST include:
Comment:        * src IP
Comment:        * dest IP (your IP)
Comment:        * dest port
Comment:        * Accurate date/timestamp and timezone of activity
Comment:        * Intensity/frequency (short log extracts)
Comment:        * Your contact details (phone and email) Without these we will
be unable to identify the correct owner of the IP address at that point in time.
Ref:            https://rdap.arin.net/registry/entity/AT-88-Z


OrgTechHandle: ANO24-ARIN
OrgTechName:   Amazon EC2 Network Operations
OrgTechPhone:  +1-206-266-4064
OrgTechEmail:  amzn-noc-contact@amazon.com
OrgTechRef:    https://rdap.arin.net/registry/entity/ANO24-ARIN

OrgAbuseHandle: AEA8-ARIN
OrgAbuseName:   Amazon EC2 Abuse
OrgAbusePhone:  +1-206-266-4064
OrgAbuseEmail:  abuse@amazonaws.com
OrgAbuseRef:    https://rdap.arin.net/registry/entity/AEA8-ARIN

OrgRoutingHandle: ARMP-ARIN
OrgRoutingName:   AWS RPKI Management POC
OrgRoutingPhone:  +1-206-266-4064
OrgRoutingEmail:  aws-rpki-routing-poc@amazon.com
OrgRoutingRef:    https://rdap.arin.net/registry/entity/ARMP-ARIN

OrgNOCHandle: AANO1-ARIN
OrgNOCName:   Amazon AWS Network Operations
OrgNOCPhone:  +1-206-266-4064
OrgNOCEmail:  amzn-noc-contact@amazon.com
OrgNOCRef:    https://rdap.arin.net/registry/entity/AANO1-ARIN

OrgRoutingHandle: IPROU3-ARIN
```

OrgRoutingHandle: IPROU3-ARIN
OrgRoutingName: IP Routing
OrgRoutingPhone: +1-206-266-4064
OrgRoutingEmail: aws-routing-poc@amazon.com
OrgRoutingRef: https://rdap.arin.net/registry/entity/IPROU3-ARIN

#
ARIN WHOIS data and services are subject to the Terms of Use
available at: https://www.arin.net/resources/registry/whois/tou/
#
If you see inaccuracies in the results, please report at
https://www.arin.net/resources/registry/whois/inaccuracy_reporting/
#
Copyright 1997-2021, American Registry for Internet Numbers, Ltd.
#

Incoming (6)	
DNS Name	apitwitter.com.w3snoop.com
DNS Name	apitwitter.com.w3snoop.com
DNS Name	apitwitter.w3snoop.com
DNS Name	apitwitter.w3snoop.com
DNS Name	w3snoop.com
DNS Name	w3snoop.com
Outgoing (15)	
Company	Amazon Technologies Inc
Company	Amazon Technologies Inc.
Email Address	amzn-noc-contact@amazon.com
Email Address	amzn-noc-contact@amazon.com
Email Address	aws-routing-poc@amazon.com
Email Address	aws-routing-poc@amazon.com
Email Address	aws-rpki-routing-poc@amazon.com
Email Address	aws-rpki-routing-poc@amazon.com
Location	Ashburn, Virginia (United States)
Location	Seattle
Location	US
Location	United States
Location	WA
Person	StateProv
Phone Number	+1 206 266 4064

IPv4 Address

maltego.IPv4Address

18.232.245.187

Weight	50
IP Address	18.232.245.187
Internal	false
Date Resolved	2020-05-01T14:36:21Z
Resolver	VirusTotal

IP whois

```
#
# ARIN WHOIS data and services are subject to the Terms of Use
# available at: https://www.arin.net/resources/registry/whois/tou/
#
# If you see inaccuracies in the results, please report at
# https://www.arin.net/resources/registry/whois/inaccuracy_reporting/
#
# Copyright 1997-2021, American Registry for Internet Numbers, Ltd.
#


#
# Query terms are ambiguous.  The query is assumed to be:
#     "n 18.232.245.187"
#
# Use "?" to get help.
#

NetRange:       18.32.0.0 - 18.255.255.255
CIDR:           18.32.0.0/11, 18.128.0.0/9, 18.64.0.0/10
NetName:        AT-88-Z
NetHandle:      NET-18-32-0-0-1
Parent:         NET18 (NET-18-0-0-0-0)
NetType:        Direct Allocation
OriginAS:
Organization:   Amazon Technologies Inc. (AT-88-Z)
RegDate:        2019-10-07
Updated:        2021-02-10
Ref:            https://rdap.arin.net/registry/ip/18.32.0.0


OrgName:        Amazon Technologies Inc.
OrgId:          AT-88-Z
Address:        410 Terry Ave N.
City:           Seattle
StateProv:      WA
PostalCode:     98109
Country:        US
RegDate:        2011-12-08
Updated:        2021-07-28
Comment:        All abuse reports MUST include:
Comment:        * src IP
Comment:        * dest IP (your IP)
Comment:        * dest port
Comment:        * Accurate date/timestamp and timezone of activity
Comment:        * Intensity/frequency (short log extracts)
Comment:        * Your contact details (phone and email) Without these we will
be unable to identify the correct owner of the IP address at that point in time.
Ref:            https://rdap.arin.net/registry/entity/AT-88-Z


OrgRoutingHandle: IPROU3-ARIN
OrgRoutingName:   IP Routing
OrgRoutingPhone:  +1-206-266-4064
OrgRoutingEmail:  aws-routing-poc@amazon.com
OrgRoutingRef:    https://rdap.arin.net/registry/entity/IPROU3-ARIN

OrgRoutingHandle: ARMP-ARIN
OrgRoutingName:   AWS RPKI Management POC
OrgRoutingPhone:  +1-206-266-4064
OrgRoutingEmail:  aws-rpki-routing-poc@amazon.com
OrgRoutingRef:    https://rdap.arin.net/registry/entity/ARMP-ARIN

OrgAbuseHandle: AEA8-ARIN
OrgAbuseName:   Amazon EC2 Abuse
OrgAbusePhone:  +1-206-266-4064
OrgAbuseEmail:  abuse@amazonaws.com
OrgAbuseRef:    https://rdap.arin.net/registry/entity/AEA8-ARIN

OrgNOCHandle: AANO1-ARIN
OrgNOCName:   Amazon AWS Network Operations
OrgNOCPhone:  +1-206-266-4064
OrgNOCEmail:  amzn-noc-contact@amazon.com
OrgNOCRef:    https://rdap.arin.net/registry/entity/AANO1-ARIN

OrgTechHandle: ANO24-ARIN
```

	OrgTechHandle: ANO24-ARIN OrgTechName: Amazon EC2 Network Operations OrgTechPhone: +1-206-266-4064 OrgTechEmail: amzn-noc-contact@amazon.com OrgTechRef: https://rdap.arin.net/registry/entity/ANO24-ARIN # # ARIN WHOIS data and services are subject to the Terms of Use # available at: https://www.arin.net/resources/registry/whois/tou/ # # If you see inaccuracies in the results, please report at # https://www.arin.net/resources/registry/whois/inaccuracy_reporting/ # # Copyright 1997-2021, American Registry for Internet Numbers, Ltd. #

Incoming (6)		
	DNS Name	apitwitter.com.w3snoop.com
	DNS Name	apitwitter.com.w3snoop.com
	DNS Name	apitwitter.w3snoop.com
	DNS Name	apitwitter.w3snoop.com
	DNS Name	w3snoop.com
	DNS Name	w3snoop.com
Outgoing (15)		
	Company	Amazon Technologies Inc
	Company	Amazon Technologies Inc.
@	Email Address	amzn-noc-contact@amazon.com
@	Email Address	amzn-noc-contact@amazon.com
@	Email Address	aws-routing-poc@amazon.com
@	Email Address	aws-routing-poc@amazon.com
@	Email Address	aws-rpki-routing-poc@amazon.com
@	Email Address	aws-rpki-routing-poc@amazon.com
	Location	Ashburn, Virginia (United States)
	Location	Seattle
	Location	US
	Location	United States
	Location	WA
	Person	StateProv
	Phone Number	+1 206 266 4064

NS Record

maltego.NSRecord

ns2.uniregistrymarket.link

Weight	50
NS Record	ns2.uniregistrymarket.link
Time To Live	3600
Type	NS

Incoming (6)	
DNS Name	apitwitter.com.evil.co
DNS Name	apitwitter.evil.co
DNS Name	com.evil.co
DNS Name	evil.co
DNS Name	wildcard-in-use.apitwitter.evil.co
Domain	apitwitter.evil.co
Outgoing (12)	
Domain	bbcswahili.co.uk
Domain	brandsight-whois.com
Domain	chowchilla.com
Domain	ggoel.co.uk
Domain	jumpershorseline.co.uk
Domain	leedsbradford.co.uk
Domain	mybham.co.uk
Domain	newbi.com
Domain	pimpmywebpage.com
Domain	tajtour.co.uk
Domain	trly.com
Domain	volumized.com

NS Record

maltego.NSRecord

ns1.uniregistrymarket.link

Weight	50
NS Record	ns1.uniregistrymarket.link
Refresh	10800
Time To Live	3600
Type	NS
Expire	604800
Minimum	86400
Serial	1555555555
Rname	hostmaster.hostingnet.com
Retry	3600

Incoming (6)	
DNS Name	apitwitter.com.evil.co
DNS Name	apitwitter.evil.co
DNS Name	com.evil.co
DNS Name	evil.co
DNS Name	wildcard-in-use.apitwitter.evil.co
Domain	apitwitter.evil.co
Outgoing (12)	
Domain	bbcswahili.co.uk
Domain	chowchilla.com
Domain	ggoel.co.uk
Domain	jumpershorseline.co.uk
Domain	komikaze.com
Domain	leedsbradford.co.uk
Domain	mybham.co.uk
Domain	newbi.com
Domain	pimpmywebpage.com
Domain	tajtour.co.uk
Domain	trly.com
Domain	volumized.com

DNS Name

maltego.DNSName

apitwitter.w3snoop.com

Weight	0
DNS Name	apitwitter.w3snoop.com
Context	apitwitter.com.w3snoop.co

Incoming (1)	
DNS Name	apitwitter.com.w3snoop.com
Outgoing (16)	
A Record	apitwitter.w3snoop.com
Domain	w3snoop.com
IPv4 Address	18.232.245.187
IPv4 Address	18.232.245.187
IPv4 Address	3.234.104.255
IPv4 Address	3.234.104.255
IPv4 Address	35.175.60.16
IPv4 Address	35.175.60.16
IPv4 Address	50.16.49.81
IPv4 Address	50.16.49.81
IPv4 Address	52.86.133.10
IPv4 Address	52.86.133.10
IPv4 Address	52.86.133.10
SSL Certificate	w3snoop.com
SSL Certificate	w3snoop.com
Shodan Tag	spf

Domain

maltego.Domain

w3snoop.com

Weight	6
Domain Name	w3snoop.com
WHOIS Info	Admin City: Tempe Admin Country: US Admin Email: c9b5a1cf1d0c3764s@domainsbyproxy.com Admin Organization: Domains By Proxy, LLC Admin Postal Code: 85284 Admin State/Province: Arizona Creation Date: 2011-06-05T21:04:22Z Creation Date: 2011-06-06T02:04:22Z DNSSEC: unsigned Domain Name: W3SNOOP.COM Domain Status: clientDeleteProhibited http://www.icann.org/epp#clientDeleteProhibited Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited Domain Status: clientRenewProhibited http://www.icann.org/epp#clientRenewProhibited Domain Status: clientRenewProhibited https://icann.org/epp#clientRenewProhibited Domain Status: clientTransferProhibited http://www.icann.org/epp#clientTransferProhibited Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Domain Status: clientUpdateProhibited http://www.icann.org/epp#clientUpdateProhibited Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited Name Server: INDRI.EZOICNS.COM Name Server: SAOLA.EZOICNS.COM Registrant City: a7319ae5e6c95df5 Registrant Country: US Registrant Email: c9b5a1cf1d0c3764s@domainsbyproxy.com Registrant Fax Ext: 3432650ec337c945 Registrant Fax: 9fad764be0c7e95d Registrant Name: 80315b2e6ac1a801 Registrant Organization: b46a98a26fe2fd9f Registrant Phone Ext: 3432650ec337c945 Registrant Phone: d5f66d3a005b000d Registrant Postal Code: 052e5bd148f904f9 Registrant State/Province: 30bdd2917a604c83 Registrant Street: 037792fd5a6fe619 Registrant Street: d733533b6a6c0c21 Registrar Abuse Contact Email: abuse@godaddy.com Registrar Abuse Contact Phone: +1.4806242505 Registrar Abuse Contact Phone: 480-624-2505 Registrar IANA ID: 146 Registrar Registration Expiration Date: 2023-06-05T21:04:22Z Registrar URL: http://www.godaddy.com Registrar WHOIS Server: whois.godaddy.com Registrar: GoDaddy.com, LLC Registry Admin ID: Not Available From Registry Registry Domain ID: 1660071767_DOMAIN_COM-VRSN Registry Expiry Date: 2023-06-06T02:04:22Z Registry Registrant ID: Not Available From Registry Registry Tech ID: Not Available From Registry Tech City: Tempe Tech Country: US Tech Email: c9b5a1cf1d0c3764s@domainsbyproxy.com Tech Organization: Domains By Proxy, LLC Tech Postal Code: 85284 Tech State/Province: Arizona Updated Date: 2020-02-09T21:49:40Z Updated Date: 2020-02-10T04:49:41Z
Context	apitwitter.com.w3snoop.co

VirusTotal Domain Summary	
VirusTotal Reputation	0
Tags	
Popularity Ranking	
Majestic	
195855	
Statvoo	
54046	
Alexa	
69309	
Cisco Umbrella	
271981	
Quantcast	
32079	

VirusTotal Analysis Summary	
Aggregate Result	harmless - 78 / 87

VirusTotal Analysis Stats	
Analysis Type	Number of Analysis
Confirmed Timeout	0
Failure	0
Harmless	78
Malicious	0
Suspicious	0
Timeout	0
Type Unsupported	0
Undetected	9
Total	**87**

View on VirusTotal

GUI Url: https://www.virustotal.com/gui/domain/w3snoop.com

Categories	
Engines	Category
Forcepoint ThreatSeeker	information technology
Sophos	information technology

Community Votes

Total votes cast: 0

Incoming (5)		
	DNS Name	apitwitter.com.w3snoop.com
	DNS Name	apitwitter.com.w3snoop.com
	DNS Name	apitwitter.w3snoop.com
	DNS Name	w3snoop.com
	Website	apitwitter.com.w3snoop.com
Outgoing (12)		
	Company	Domains By Proxy, LLC
	Company	VeriSign
@	Email Address	abuse@godaddy.com
@	Email Address	abuse@godaddy.com
@	Email Address	w3snoop.com@domainsbyproxy.com
@	Email Address	w3snoop.com@domainsbyproxy.com
	Location	Tempe, US
	Person	GoDaddy.com, LLC
	Phone Number	+1 480 624 2505
	Phone Number	+1 480 624 2505
	Phone Number	+1 480 624 2598
	Phone Number	+1 480 624 2598

Website

maltego.Website

evil.com

Weight	100
Website	evil.com
SSL Enabled	false
Ports	[80]
SSL Ports	443

Info

View Website

Incoming (1)		
	DNS Name	evil.com
Outgoing (14)		
	A Record	evil.com
	DNS Name	*.evil.com
	DNS Name	*.evil.com
	DNS Name	ns1.verio.com
	DNS Name	www.evil.com
	DNS Name	www.evil.com
	IPv4 Address	209.204.174.29
	IPv4 Address	45.56.91.58
	IPv4 Address	66.96.146.129
	MX Record	mx.evil.com
	NS Record	ns1.verio.com
	NS Record	ns2.verio.com
	Phrase	v=spf1 ip4:66.96.128.0/18 ?all
	Shodan Tag	spf

IPv4 Address

maltego.IPv4Address

3.234.104.255

Weight	50
IP Address	3.234.104.255
Internal	false
Date Resolved	2020-05-01T14:36:21Z
Resolver	VirusTotal
IP whois	# # ARIN WHOIS data and services are subject to the Terms of Use # available at: https://www.arin.net/resources/registry/whois/tou/ # # If you see inaccuracies in the results, please report at # https://www.arin.net/resources/registry/whois/inaccuracy_reporting/ # # Copyright 1997-2021, American Registry for Internet Numbers, Ltd. # # # # Query terms are ambiguous. The query is assumed to be: # "n 3.234.104.255" # # Use "?" to get help. # Amazon Technologies Inc. AT-88-Z (NET-3-128-0-0-1) 3.128.0.0 - 3.255.255.255 Amazon Data Services NoVa AMAZON-IAD (NET-3-224-0-0-1) 3.224.0.0 - 3.239.255.255 # # ARIN WHOIS data and services are subject to the Terms of Use # available at: https://www.arin.net/resources/registry/whois/tou/ # # If you see inaccuracies in the results, please report at # https://www.arin.net/resources/registry/whois/inaccuracy_reporting/ # # Copyright 1997-2021, American Registry for Internet Numbers, Ltd. #

Info

Relevance:	0.433512
Count:	1

Incoming (6)

DNS Name	apitwitter.com.w3snoop.com
DNS Name	apitwitter.com.w3snoop.com
DNS Name	apitwitter.w3snoop.com
DNS Name	apitwitter.w3snoop.com
DNS Name	w3snoop.com
DNS Name	w3snoop.com

Outgoing (7)

Company	Amazon Technologies Inc
IPv4 Address	3.128.0.0
IPv4 Address	3.224.0.0
IPv4 Address	3.239.255.255
IPv4 Address	3.255.255.255
Location	Ashburn, Virginia (United States)
Location	United States

DNS Name

maltego.DNSName

apitwitter.com.evil.co

Weight	0
DNS Name	apitwitter.com.evil.co
Context	apitwitter.com.evil.c

Incoming (1)

DNS Name	apitwitter.evil.com

Outgoing (11)

A Record	apitwitter.com.evil.co
DNS Name	com.evil.co
DNS Name	evil.co
Domain	com.evil.co
Domain	evil.co
IPv4 Address	52.128.23.153
IPv4 Address	52.128.23.153
MX Record	localhost
NS Record	ns1.uniregistrymarket.link
NS Record	ns2.uniregistrymarket.link
Phrase	v=spf1 -all

DNS Name

maltego.DNSName

com.evil.co

Weight	0
DNS Name	com.evil.co
Context	com.evil.c

Incoming (2)

DNS Name	apitwitter.com.evil.co
DNS Name	apitwitter.evil.com

Outgoing (10)

A Record	com.evil.co
DNS Name	evil.co
Domain	evil.co
Domain	evil.co
IPv4 Address	52.128.23.153
IPv4 Address	52.128.23.153
MX Record	localhost
NS Record	ns1.uniregistrymarket.link
NS Record	ns2.uniregistrymarket.link
Phrase	v=spf1 -all

IPv4 Address

maltego.IPv4Address

52.128.23.153

Weight	25
IP Address	52.128.23.153
Internal	false
Date Resolved	2021-10-11T07:09:58Z
Resolver	VirusTotal

Incoming (12)

DNS Name	apitwitter.com.evil.co
DNS Name	apitwitter.com.evil.co
DNS Name	apitwitter.evil.co
DNS Name	apitwitter.evil.co
DNS Name	com.evil.co
DNS Name	com.evil.co
DNS Name	evil.co
DNS Name	evil.co
DNS Name	wildcard-in-use.apitwitter.evil.co
DNS Name	wildcard-in-use.apitwitter.evil.co
DNS Name	wildcard-in-use.apitwitter.evil.co
Website	www.apitwitter.evil.co

DNS Name

maltego.DNSName

apitwitter.evil.co

Weight	0
DNS Name	apitwitter.evil.co
Context	apitwitter.evil.c

Incoming (1)

DNS Name	evil.com

Outgoing (10)

A Record	apitwitter.evil.co
Domain	apitwitter.evil.co
Domain	evil.co
Domain	evil.co
IPv4 Address	52.128.23.153
IPv4 Address	52.128.23.153
MX Record	localhost
NS Record	ns1.uniregistrymarket.link
NS Record	ns2.uniregistrymarket.link
Phrase	v=spf1 -all

DNS Name

maltego.DNSName

wildcard-in-use.apitwitter.evil.co

Weight	100
DNS Name	wildcard-in-use.apitwitter.evil.co

Incoming (2)

Domain	apitwitter.evil.co
Domain	apitwitter.evil.co

Outgoing (9)

A Record	wildcard-in-use.apitwitter.evil.co
Domain	apitwitter.evil.co
IPv4 Address	52.128.23.153
IPv4 Address	52.128.23.153
IPv4 Address	52.128.23.153
MX Record	localhost
NS Record	ns1.uniregistrymarket.link
NS Record	ns2.uniregistrymarket.link
Phrase	v=spf1 -all

IPv4 Address

maltego.IPv4Address

50.16.49.81

Weight	50
IP Address	50.16.49.81
Internal	false
Date Resolved	2020-05-01T14:36:21Z
Resolver	VirusTotal
IP whois	# # ARIN WHOIS data and services are subject to the Terms of Use # available at: https://www.arin.net/resources/registry/whois/tou/ # # If you see inaccuracies in the results, please report at # https://www.arin.net/resources/registry/whois/inaccuracy_reporting/ # # Copyright 1997-2021, American Registry for Internet Numbers, Ltd. # # # # Query terms are ambiguous. The query is assumed to be: # "n 50.16.49.81" # # Use "?" to get help. # Amazon.com, Inc. AMAZON-EC2-8 (NET-50-16-0-0-1) 50.16.0.0 - 50.19.255.255 Amazon Data Services NoVa AMAZON-IAD (NET-50-16-0-0-2) 50.16.0.0 - 50.17.255.255 # # ARIN WHOIS data and services are subject to the Terms of Use # available at: https://www.arin.net/resources/registry/whois/tou/ # # If you see inaccuracies in the results, please report at # https://www.arin.net/resources/registry/whois/inaccuracy_reporting/ # # Copyright 1997-2021, American Registry for Internet Numbers, Ltd. #

Info

Relevance:	0.437367
Count:	1

Incoming (6)

DNS Name	apitwitter.com.w3snoop.com
DNS Name	apitwitter.com.w3snoop.com
DNS Name	apitwitter.w3snoop.com
DNS Name	apitwitter.w3snoop.com
DNS Name	w3snoop.com
DNS Name	w3snoop.com

Outgoing (5)

IPv4 Address	50.16.0.0
IPv4 Address	50.17.255.255
IPv4 Address	50.19.255.255
Location	Ashburn, Virginia (United States)
Location	United States

Company

maltego.Company

VeriSign

Weight	52
Name	VeriSign

Info

Relevance:	0.497591
Count:	7

Info

Relevance:	0.558786
Count:	7

Incoming (2)

Domain	evil.com
Domain	w3snoop.com

Outgoing (8)

LittleSis Organization	Verisign Inc. PAC
LittleSis Public Company	VeriSign, Inc.
Peering DB Organization	VeriSign
Peering DB Organization	VeriSign
PeeringDB Network	VeriSign Global Registry Services
PeeringDB Network	VeriSign Global Registry Services
PeeringDB Network	Verisign
PeeringDB Network	Verisign

Domain

maltego.Domain

evil.co

Weight	6
Domain Name	evil.co
WHOIS Info	Admin City: REDACTED FOR PRIVACY Admin Country: REDACTED FOR PRIVACY Admin Organization: REDACTED FOR PRIVACY Admin Postal Code: REDACTED FOR PRIVACY Admin State/Province: REDACTED FOR PRIVACY Creation Date: 2019-10-05T17:00:14Z DNSSEC: unsigned Domain Name: evil.co Domain Status: clientDeleteProhibited http://www.icann.org/epp#clientDeleteProhibited Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited Domain Status: clientRenewProhibited http://www.icann.org/epp#clientRenewProhibited Domain Status: clientRenewProhibited https://icann.org/epp#clientRenewProhibited Domain Status: clientTransferProhibited http://www.icann.org/epp#clientTransferProhibited Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Domain Status: clientUpdateProhibited http://www.icann.org/epp#clientUpdateProhibited Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited Name Server: NS1.UNIREGISTRYMARKET.LINK Name Server: NS2.UNIREGISTRYMARKET.LINK Name Server: ns1.uniregistrymarket.link Name Server: ns2.uniregistrymarket.link Registrant City: 1f8f4166599d23ee Registrant Country: US Registrant Email: 44f8172ee385b60bs@ Registrant Email: f651612a2f356ad3s@ Registrant Fax Ext: 1f8f4166599d23ee Registrant Fax: 1f8f4166599d23ee Registrant Name: 1f8f4166599d23ee Registrant Organization: 3432650ec337c945 Registrant Phone Ext: 1f8f4166599d23ee Registrant Phone: 1f8f4166599d23ee Registrant Postal Code: 1f8f4166599d23ee Registrant State/Province: c5117919ef41a795 Registrant Street: 1f8f4166599d23ee Registrar Abuse Contact Email: abuse@godaddy.com Registrar Abuse Contact Phone: +1.4806242505 Registrar IANA ID: 146 Registrar Registration Expiration Date: 2022-10-05T17:00:14Z Registrar URL: http://www.godaddy.com Registrar URL: whois.godaddy.com Registrar WHOIS Server: whois.godaddy.com Registrar: GoDaddy.com, LLC Registry Admin ID: REDACTED FOR PRIVACY Registry Domain ID: D8A750721BA904C4A90CFDA260DBE314E-NSR Registry Expiry Date: 2022-10-05T17:00:14Z Registry Registrant ID: REDACTED FOR PRIVACY Registry Tech ID: REDACTED FOR PRIVACY Tech City: REDACTED FOR PRIVACY Tech Country: REDACTED FOR PRIVACY Tech Organization: REDACTED FOR PRIVACY Tech Postal Code: REDACTED FOR PRIVACY Tech State/Province: REDACTED FOR PRIVACY Updated Date: 2021-06-17T12:14:42Z Updated Date: 2021-06-22T19:14:40Z
Context	apitwitter.evil.c

VirusTotal Domain Summary	
VirusTotal Reputation	0
Tags	
Popularity Ranking	
Statvoo	
390893	
Alexa	
390893	

VirusTotal Analysis Summary	
Aggregate Result	harmless - 76 / 87

VirusTotal Analysis Stats	
Analysis Type	Number of Analysis
Confirmed Timeout	0
Failure	0
Harmless	76
Malicious	0
Suspicious	0
Timeout	0
Type Unsupported	0
Undetected	11
Total	**87**

View on VirusTotal

GUI Url: https://www.virustotal.com/gui/domain/evil.co

Community Votes

Total votes cast: 0

Incoming (9)		
	DNS Name	apitwitter.com.evil.co
	DNS Name	apitwitter.evil.co
	DNS Name	apitwitter.evil.co
	DNS Name	apitwitter.evil.com
	DNS Name	com.evil.co
	DNS Name	com.evil.co
	DNS Name	evil.co
	DNS Name	evil.co
	DNS Name	evil.com

Domain

maltego.Domain

apitwitter.evil.co

Weight	50
Domain Name	apitwitter.evil.co
WHOIS Info	Admin City: REDACTED FOR PRIVACY Admin Country: REDACTED FOR PRIVACY Admin Organization: REDACTED FOR PRIVACY Admin Postal Code: REDACTED FOR PRIVACY Admin State/Province: REDACTED FOR PRIVACY Creation Date: 2019-10-05T17:00:14Z DNSSEC: unsigned Domain Name: evil.co Domain Status: clientDeleteProhibited http://www.icann.org/epp#clientDeleteProhibited Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited Domain Status: clientRenewProhibited http://www.icann.org/epp#clientRenewProhibited Domain Status: clientRenewProhibited https://icann.org/epp#clientRenewProhibited Domain Status: clientTransferProhibited http://www.icann.org/epp#clientTransferProhibited Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Domain Status: clientUpdateProhibited http://www.icann.org/epp#clientUpdateProhibited Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited Name Server: NS1.UNIREGISTRYMARKET.LINK Name Server: NS2.UNIREGISTRYMARKET.LINK Name Server: ns1.uniregistrymarket.link Name Server: ns2.uniregistrymarket.link Registrant City: 1f8f4166599d23ee Registrant Country: US Registrant Email: 44f8172ee385b60bs@ Registrant Email: f651612a2f356ad3s@ Registrant Fax Ext: 1f8f4166599d23ee Registrant Fax: 1f8f4166599d23ee Registrant Name: 1f8f4166599d23ee Registrant Organization: 3432650ec337c945 Registrant Phone Ext: 1f8f4166599d23ee Registrant Phone: 1f8f4166599d23ee Registrant Postal Code: 1f8f4166599d23ee Registrant State/Province: c5117919ef41a795 Registrant Street: 1f8f4166599d23ee Registrar Abuse Contact Email: abuse@godaddy.com Registrar Abuse Contact Phone: +1.4806242505 Registrar IANA ID: 146 Registrar Registration Expiration Date: 2022-10-05T17:00:14Z Registrar URL: http://www.godaddy.com Registrar URL: whois.godaddy.com Registrar WHOIS Server: whois.godaddy.com Registrar: GoDaddy.com, LLC Registry Admin ID: REDACTED FOR PRIVACY Registry Domain ID: D8A750721BA904C4A90CFDA260DBE314E-NSR Registry Expiry Date: 2022-10-05T17:00:14Z Registry Registrant ID: REDACTED FOR PRIVACY Registry Tech ID: REDACTED FOR PRIVACY Tech City: REDACTED FOR PRIVACY Tech Country: REDACTED FOR PRIVACY Tech Organization: REDACTED FOR PRIVACY Tech Postal Code: REDACTED FOR PRIVACY Tech State/Province: REDACTED FOR PRIVACY Updated Date: 2021-06-17T12:14:42Z Updated Date: 2021-06-22T19:14:40Z

VirusTotal Domain Summary

VirusTotal Reputation	0
Tags	

VirusTotal Analysis Summary

Aggregate Result	harmless - 86 / 86

VirusTotal Analysis Stats

Analysis Type	Number of Analysis
Confirmed Timeout	0
Failure	0
Harmless	86
Malicious	0
Suspicious	0
Timeout	0
Type Unsupported	0
Undetected	0
Total	**86**

View on VirusTotal

GUI Url: https://www.virustotal.com/gui/domain/apitwitter.evil.co

Community Votes

Total votes cast: 0

Incoming (2)

DNS Name	apitwitter.evil.co
DNS Name	wildcard-in-use.apitwitter.evil.co

Outgoing (6)

DNS Name	wildcard-in-use.apitwitter.evil.co
DNS Name	wildcard-in-use.apitwitter.evil.co
MX Record	localhost
NS Record	ns1.uniregistrymarket.link
NS Record	ns2.uniregistrymarket.link
Website	www.apitwitter.evil.co

Location

maltego.Location

United States

Weight	86
Name	United States
Country	United States
City	
Street Address	
Area	
Area Code	
Country Code	US
Longitude	0.0
Latitude	0.0
Continent	North America
Timezone	America/Chicago
Postal code	

Info

Information retrieved from the Maxmind GeoLite2 DB.
Available Here.

Info

Relevance:	0.46569
Count:	2

Incoming (8)

IPv4 Address	18.232.245.187
IPv4 Address	3.234.104.255
IPv4 Address	35.175.60.16
IPv4 Address	50.16.49.81
IPv4 Address	52.86.133.10
IPv4 Address	66.96.146.129
IPv4 Address	66.96.146.129
IPv4 Address	66.96.146.129

Shodan Tag

maltego.shodan.Tag

spf

Weight	0
Text	spf

Incoming (8)

DNS Name	apitwitter.com.evil.com
DNS Name	apitwitter.com.w3snoop.com
DNS Name	apitwitter.evil.com
DNS Name	apitwitter.w3snoop.com
DNS Name	evil.com
DNS Name	w3snoop.com
DNS Name	www.evil.com
Website	evil.com

SSL Certificate

maltego.X509Certificate

*.evil.com

Weight	0
Subject	*.evil.com
Issuer	R3
Subject DN	
Issuer DN	
SKI	daad26d1d9c7901537e84a12886ef8ddc37132e5
AKI	
Serial	420ec82f5bb8df074c6094d73cc1d57dd17
SAN	[*.evil.com, evil.com]
Usage	
Issuance ID	
Valid From	Tue Oct 05 00:00:00 GMT 2021
Valid Until	Mon Jan 03 00:00:00 GMT 2022
Country	
Organization	

Incoming (6)

DNS Name	apitwitter.evil.com
DNS Name	apitwitter.evil.com
DNS Name	evil.com
DNS Name	evil.com
DNS Name	www.evil.com
DNS Name	www.evil.com

MX Record

maltego.MXRecord

localhost

Weight	50
MX Record	localhost
Priority	0
Time To Live	3600
Type	MX
Priority	1

Incoming (6)

DNS Name	apitwitter.com.evil.co
DNS Name	apitwitter.evil.co
DNS Name	com.evil.co
DNS Name	evil.co
DNS Name	wildcard-in-use.apitwitter.evil.co
Domain	apitwitter.evil.co

Email Address

maltego.EmailAddress

aws-routing-poc@amazon.com

Weight	100
Email Address	aws-routing-poc@amazon.com

Incoming (6)

IPv4 Address	18.232.245.187
IPv4 Address	18.232.245.187
IPv4 Address	35.175.60.16
IPv4 Address	35.175.60.16
IPv4 Address	52.86.133.10
IPv4 Address	52.86.133.10

Email Address

maltego.EmailAddress

aws-rpki-routing-poc@amazon.com

Weight	100
Email Address	aws-rpki-routing-poc@amazon.com

Incoming (6)

IPv4 Address	18.232.245.187
IPv4 Address	18.232.245.187
IPv4 Address	35.175.60.16
IPv4 Address	35.175.60.16
IPv4 Address	52.86.133.10
IPv4 Address	52.86.133.10

Email Address

maltego.EmailAddress

amzn-noc-contact@amazon.com

Weight	100
Email Address	amzn-noc-contact@amazon.com

Incoming (6)

IPv4 Address	18.232.245.187
IPv4 Address	18.232.245.187
IPv4 Address	35.175.60.16
IPv4 Address	35.175.60.16
IPv4 Address	52.86.133.10
IPv4 Address	52.86.133.10

MX Record

maltego.MXRecord

mx.evil.com

Weight	0
MX Record	mx.evil.com
Priority	0
Time To Live	3600
Type	MX
Record Last Seen	2021-09-29T05:55:26.564296+00:00
Priority	30
DNS Record Type	MX

Incoming (6)

DNS Name	apitwitter.com.evil.com
DNS Name	apitwitter.evil.com
DNS Name	evil.com
DNS Name	evil.com
DNS Name	www.evil.com
Website	evil.com

Location

maltego.Location

Ashburn, Virginia (United States)

Weight	100
Name	Ashburn, Virginia (United States)
Country	
City	
Street Address	
Area	Virginia
Area Code	VA
Country Code	US
Longitude	-77.4728
Latitude	39.0481
Continent	North America
Timezone	America/New_York
Postal code	20149

Info

Information retrieved from the Maxmind GeoLite2 DB.
Available Here.

Incoming (5)

IPv4 Address	18.232.245.187
IPv4 Address	3.234.104.255
IPv4 Address	35.175.60.16
IPv4 Address	50.16.49.81
IPv4 Address	52.86.133.10

Phrase

maltego.Phrase

v=spf1 -all

Weight	0
Text	v=spf1 -all
Time To Live	3600
Type	TXT

Incoming (5)

DNS Name	apitwitter.com.evil.co
DNS Name	apitwitter.evil.co
DNS Name	com.evil.co
DNS Name	evil.co
DNS Name	wildcard-in-use.apitwitter.evil.co

Domain

maltego.Domain

villain.evil.com

Weight	0
Domain Name	villain.evil.com
WHOIS Info	Creation Date: 1995-04-10T04:00:00Z DNSSEC: unsigned Domain Name: EVIL.COM Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited Name Server: NS1.VERIO.COM Name Server: NS2.VERIO.COM Registrar Abuse Contact Email: abuse@web.com Registrar Abuse Contact Phone: +1.8003337680 Registrar IANA ID: 2 Registrar URL: http://networksolutions.com Registrar WHOIS Server: whois.networksolutions.com Registrar: Network Solutions, LLC Registry Domain ID: 1040763_DOMAIN_COM-VRSN Registry Expiry Date: 2023-04-11T04:00:00Z Updated Date: 2019-12-17T16:17:59Z

VirusTotal Domain Summary

VirusTotal Reputation	0
Tags	

VirusTotal Analysis Summary

Aggregate Result	harmless - 86 / 86

VirusTotal Analysis Stats

Analysis Type	Number of Analysis
Confirmed Timeout	0
Failure	0
Harmless	86
Malicious	0
Suspicious	0
Timeout	0
Type Unsupported	0
Undetected	0
Total	**86**

View on VirusTotal

GUI Url: https://www.virustotal.com/gui/domain/villain.evil.com

Community Votes

Total votes cast: 0

Incoming (4)

DNS Name	apitwitter.com.evil.com
DNS Name	apitwitter.evil.com
DNS Name	evil.com
DNS Name	www.evil.com

Domain

maltego.Domain

some.evil.com

Weight	0
Domain Name	some.evil.com
WHOIS Info	Creation Date: 1995-04-10T04:00:00Z DNSSEC: unsigned Domain Name: EVIL.COM Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited Name Server: NS1.VERIO.COM Name Server: NS2.VERIO.COM Registrar Abuse Contact Email: abuse@web.com Registrar Abuse Contact Phone: +1.8003337680 Registrar IANA ID: 2 Registrar URL: http://networksolutions.com Registrar WHOIS Server: whois.networksolutions.com Registrar: Network Solutions, LLC Registry Domain ID: 1040763_DOMAIN_COM-VRSN Registry Expiry Date: 2023-04-11T04:00:00Z Updated Date: 2019-12-17T16:17:59Z

VirusTotal Domain Summary	
VirusTotal Reputation	0
Tags	

VirusTotal Analysis Summary	
Aggregate Result	harmless - 86 / 86

VirusTotal Analysis Stats	
Analysis Type	Number of Analysis
Confirmed Timeout	0
Failure	0
Harmless	86
Malicious	0
Suspicious	0
Timeout	0
Type Unsupported	0
Undetected	0
Total	**86**

View on VirusTotal

GUI Url: https://www.virustotal.com/gui/domain/some.evil.com

Community Votes

Total votes cast: 0

Incoming (4)

DNS Name	apitwitter.com.evil.com
DNS Name	apitwitter.evil.com
DNS Name	evil.com
DNS Name	www.evil.com

Domain

maltego.Domain

eg.evil.com

Weight	0
Domain Name	eg.evil.com
WHOIS Info	Creation Date: 1995-04-10T04:00:00Z DNSSEC: unsigned Domain Name: EVIL.COM Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited Name Server: NS1.VERIO.COM Name Server: NS2.VERIO.COM Registrar Abuse Contact Email: abuse@web.com Registrar Abuse Contact Phone: +1.8003337680 Registrar IANA ID: 2 Registrar URL: http://networksolutions.com Registrar WHOIS Server: whois.networksolutions.com Registrar: Network Solutions, LLC Registry Domain ID: 1040763_DOMAIN_COM-VRSN Registry Expiry Date: 2023-04-11T04:00:00Z Updated Date: 2019-12-17T16:17:59Z

VirusTotal Domain Summary

VirusTotal Reputation	0
Tags	

VirusTotal Analysis Summary

Aggregate Result	harmless - 86 / 86

VirusTotal Analysis Stats

Analysis Type	Number of Analysis
Confirmed Timeout	0
Failure	0
Harmless	86
Malicious	0
Suspicious	0
Timeout	0
Type Unsupported	0
Undetected	0
Total	**86**

View on VirusTotal

GUI Url: https://www.virustotal.com/gui/domain/eg.evil.com

Community Votes

Total votes cast: 0

Incoming (4)		
	DNS Name	apitwitter.com.evil.com
	DNS Name	apitwitter.evil.com
	DNS Name	evil.com
	DNS Name	www.evil.com

Domain

maltego.Domain

au.evil.com

Weight	0
Domain Name	au.evil.com
WHOIS Info	Creation Date: 1995-04-10T04:00:00Z DNSSEC: unsigned Domain Name: EVIL.COM Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited Name Server: NS1.VERIO.COM Name Server: NS2.VERIO.COM Registrar Abuse Contact Email: abuse@web.com Registrar Abuse Contact Phone: +1.8003337680 Registrar IANA ID: 2 Registrar URL: http://networksolutions.com Registrar WHOIS Server: whois.networksolutions.com Registrar: Network Solutions, LLC Registry Domain ID: 1040763_DOMAIN_COM-VRSN Registry Expiry Date: 2023-04-11T04:00:00Z Updated Date: 2019-12-17T16:17:59Z

VirusTotal Domain Summary	
VirusTotal Reputation	0
Tags	

VirusTotal Analysis Summary	
Aggregate Result	harmless - 86 / 86

VirusTotal Analysis Stats

Analysis Type	Number of Analysis
Confirmed Timeout	0
Failure	0
Harmless	86
Malicious	0
Suspicious	0
Timeout	0
Type Unsupported	0
Undetected	0
Total	**86**

View on VirusTotal

GUI Url: https://www.virustotal.com/gui/domain/au.evil.com

Community Votes

Total votes cast: 0

Incoming (4)

DNS Name	apitwitter.com.evil.com
DNS Name	apitwitter.evil.com
DNS Name	evil.com
DNS Name	www.evil.com

Domain

maltego.Domain

mal.evil.com

Weight	0
Domain Name	mal.evil.com
WHOIS Info	Creation Date: 1995-04-10T04:00:00Z DNSSEC: unsigned Domain Name: EVIL.COM Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited Name Server: NS1.VERIO.COM Name Server: NS2.VERIO.COM Registrar Abuse Contact Email: abuse@web.com Registrar Abuse Contact Phone: +1.8003337680 Registrar IANA ID: 2 Registrar URL: http://networksolutions.com Registrar WHOIS Server: whois.networksolutions.com Registrar: Network Solutions, LLC Registry Domain ID: 1040763_DOMAIN_COM-VRSN Registry Expiry Date: 2023-04-11T04:00:00Z Updated Date: 2019-12-17T16:17:59Z

VirusTotal Domain Summary	
VirusTotal Reputation	0
Tags	

VirusTotal Analysis Summary	
Aggregate Result	harmless - 78 / 87

VirusTotal Analysis Stats	
Analysis Type	Number of Analysis
Confirmed Timeout	0
Failure	0
Harmless	78
Malicious	0
Suspicious	0
Timeout	0
Type Unsupported	0
Undetected	9
Total	**87**

View on VirusTotal

GUI Url: https://www.virustotal.com/gui/domain/mal.evil.com

Categories	
Engines	Category
Forcepoint ThreatSeeker	entertainment
BitDefender	hobbies

Community Votes

Total votes cast: 0

Incoming (4)

DNS Name	apitwitter.com.evil.com
DNS Name	apitwitter.evil.com
DNS Name	evil.com
DNS Name	www.evil.com

Domain

maltego.Domain

remotehost.evil.com

Weight	0
Domain Name	remotehost.evil.com
WHOIS Info	Creation Date: 1995-04-10T04:00:00Z DNSSEC: unsigned Domain Name: EVIL.COM Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited Name Server: NS1.VERIO.COM Name Server: NS2.VERIO.COM Registrar Abuse Contact Email: abuse@web.com Registrar Abuse Contact Phone: +1.8003337680 Registrar IANA ID: 2 Registrar URL: http://networksolutions.com Registrar WHOIS Server: whois.networksolutions.com Registrar: Network Solutions, LLC Registry Domain ID: 1040763_DOMAIN_COM-VRSN Registry Expiry Date: 2023-04-11T04:00:00Z Updated Date: 2019-12-17T16:17:59Z

VirusTotal Domain Summary

VirusTotal Reputation	0
Tags	

VirusTotal Analysis Summary

Aggregate Result	harmless - 86 / 86

VirusTotal Analysis Stats

Analysis Type	Number of Analysis
Confirmed Timeout	0
Failure	0
Harmless	86
Malicious	0
Suspicious	0
Timeout	0
Type Unsupported	0
Undetected	0
Total	**86**

View on VirusTotal

GUI Url: https://www.virustotal.com/gui/domain/remotehost.evil.com

Community Votes

Total votes cast: 0

Incoming (4)		
	DNS Name	apitwitter.com.evil.com
	DNS Name	apitwitter.evil.com
	DNS Name	evil.com
	DNS Name	www.evil.com

Domain

maltego.Domain

cookiegrabber.evil.com

Weight	0
Domain Name	cookiegrabber.evil.com
WHOIS Info	Creation Date: 1995-04-10T04:00:00Z DNSSEC: unsigned Domain Name: EVIL.COM Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited Name Server: NS1.VERIO.COM Name Server: NS2.VERIO.COM Registrar Abuse Contact Email: abuse@web.com Registrar Abuse Contact Phone: +1.8003337680 Registrar IANA ID: 2 Registrar URL: http://networksolutions.com Registrar WHOIS Server: whois.networksolutions.com Registrar: Network Solutions, LLC Registry Domain ID: 1040763_DOMAIN_COM-VRSN Registry Expiry Date: 2023-04-11T04:00:00Z Updated Date: 2019-12-17T16:17:59Z

VirusTotal Domain Summary	
VirusTotal Reputation	0
Tags	

VirusTotal Analysis Summary	
Aggregate Result	harmless - 86 / 86

VirusTotal Analysis Stats

Analysis Type	Number of Analysis
Confirmed Timeout	0
Failure	0
Harmless	86
Malicious	0
Suspicious	0
Timeout	0
Type Unsupported	0
Undetected	0
Total	**86**

View on VirusTotal

GUI Url: https://www.virustotal.com/gui/domain/cookiegrabber.evil.com

Community Votes

Total votes cast: 0

Incoming (4)

DNS Name	apitwitter.com.evil.com
DNS Name	apitwitter.evil.com
DNS Name	evil.com
DNS Name	www.evil.com

Domain

maltego.Domain

google.evil.com

Weight	0
Domain Name	google.evil.com
WHOIS Info	Creation Date: 1995-04-10T04:00:00Z DNSSEC: unsigned Domain Name: EVIL.COM Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited Name Server: NS1.VERIO.COM Name Server: NS2.VERIO.COM Registrar Abuse Contact Email: abuse@web.com Registrar Abuse Contact Phone: +1.8003337680 Registrar IANA ID: 2 Registrar URL: http://networksolutions.com Registrar WHOIS Server: whois.networksolutions.com Registrar: Network Solutions, LLC Registry Domain ID: 1040763_DOMAIN_COM-VRSN Registry Expiry Date: 2023-04-11T04:00:00Z Updated Date: 2019-12-17T16:17:59Z

VirusTotal Domain Summary	
VirusTotal Reputation	0
Tags	

VirusTotal Analysis Summary	
Aggregate Result	harmless - 86 / 86

VirusTotal Analysis Stats	
Analysis Type	Number of Analysis
Confirmed Timeout	0
Failure	0
Harmless	86
Malicious	0
Suspicious	0
Timeout	0
Type Unsupported	0
Undetected	0
Total	**86**

View on VirusTotal

GUI Url: https://www.virustotal.com/gui/domain/google.evil.com

Community Votes

Total votes cast: 0

Incoming (4)

DNS Name	apitwitter.com.evil.com
DNS Name	apitwitter.evil.com
DNS Name	evil.com
DNS Name	www.evil.com

Domain

maltego.Domain

mx.evil.com

Weight	0
Domain Name	mx.evil.com
WHOIS Info	Creation Date: 1995-04-10T04:00:00Z DNSSEC: unsigned Domain Name: EVIL.COM Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited Name Server: NS1.VERIO.COM Name Server: NS2.VERIO.COM Registrar Abuse Contact Email: abuse@web.com Registrar Abuse Contact Phone: +1.8003337680 Registrar IANA ID: 2 Registrar URL: http://networksolutions.com Registrar WHOIS Server: whois.networksolutions.com Registrar: Network Solutions, LLC Registry Domain ID: 1040763_DOMAIN_COM-VRSN Registry Expiry Date: 2023-04-11T04:00:00Z Updated Date: 2019-12-17T16:17:59Z

VirusTotal Domain Summary

VirusTotal Reputation	0
Tags	

VirusTotal Analysis Summary

Aggregate Result	harmless - 86 / 86

VirusTotal Analysis Stats

Analysis Type	Number of Analysis
Confirmed Timeout	0
Failure	0
Harmless	86
Malicious	0
Suspicious	0
Timeout	0
Type Unsupported	0
Undetected	0
Total	**86**

View on VirusTotal

GUI Url: https://www.virustotal.com/gui/domain/mx.evil.com

Categories	
Engines	Category
Forcepoint ThreatSeeker	entertainment
BitDefender	hobbies

Community Votes

Total votes cast: 0

Incoming (4)

DNS Name	apitwitter.com.evil.com
DNS Name	apitwitter.evil.com
DNS Name	evil.com
DNS Name	www.evil.com

Domain

maltego.Domain

ads.evil.com

Weight	0
Domain Name	ads.evil.com
WHOIS Info	Creation Date: 1995-04-10T04:00:00Z DNSSEC: unsigned Domain Name: EVIL.COM Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited Name Server: NS1.VERIO.COM Name Server: NS2.VERIO.COM Registrar Abuse Contact Email: abuse@web.com Registrar Abuse Contact Phone: +1.8003337680 Registrar IANA ID: 2 Registrar URL: http://networksolutions.com Registrar WHOIS Server: whois.networksolutions.com Registrar: Network Solutions, LLC Registry Domain ID: 1040763_DOMAIN_COM-VRSN Registry Expiry Date: 2023-04-11T04:00:00Z Updated Date: 2019-12-17T16:17:59Z

VirusTotal Domain Summary	
VirusTotal Reputation	0
Tags	

VirusTotal Analysis Summary	
Aggregate Result	harmless - 86 / 86

VirusTotal Analysis Stats

Analysis Type	Number of Analysis
Confirmed Timeout	0
Failure	0
Harmless	86
Malicious	0
Suspicious	0
Timeout	0
Type Unsupported	0
Undetected	0
Total	**86**

View on VirusTotal

GUI Url: https://www.virustotal.com/gui/domain/ads.evil.com

Community Votes

Total votes cast: 0

Incoming (4)

DNS Name	apitwitter.com.evil.com
DNS Name	apitwitter.evil.com
DNS Name	evil.com
DNS Name	www.evil.com

SSL Certificate

maltego.X509Certificate

w3snoop.com

Weight	0
Subject	w3snoop.com
Issuer	R3
Subject DN	
Issuer DN	
SKI	88940c697316b7d636b0fe43ea253f6f2629698b
AKI	
Serial	3a6e3164ab720f39ce7d4888aafbfc6f5a7
SAN	[*.w3snoop.com, w3snoop.com]
Usage	
Issuance ID	
Valid From	Mon Sep 27 00:00:00 GMT 2021
Valid Until	Sun Dec 26 00:00:00 GMT 2021
Country	
Organization	

Incoming (4)	
DNS Name	apitwitter.w3snoop.com
DNS Name	apitwitter.w3snoop.com
DNS Name	w3snoop.com
DNS Name	w3snoop.com

DNS Name

maltego.DNSName

*.evil.com

Weight	0
DNS Name	*.evil.com

Incoming (4)	
DNS Name	evil.com
DNS Name	evil.com
Website	evil.com
Website	evil.com

Person

maltego.Person

StateProv

Weight	39
Full Name	StateProv
First Names	
Surname	

Info	
Relevance:	0.399039
Count:	1

Info	
Relevance:	0.399193
Count:	1

Info	
Relevance:	0.390749
Count:	1

Incoming (4)	
IPv4 Address	18.232.245.187
IPv4 Address	35.175.60.16
IPv4 Address	52.86.133.10
IPv4 Address	66.96.146.129

Company

maltego.Company

Amazon Technologies Inc

Weight	61
Name	Amazon Technologies Inc

Info

Relevance:	0.633604
Count:	1

Info

Relevance:	0.635188
Count:	1

Info

Relevance:	0.488291
Count:	1

Incoming (4)

IPv4 Address	18.232.245.187
IPv4 Address	3.234.104.255
IPv4 Address	35.175.60.16
IPv4 Address	52.86.133.10

Domain

maltego.Domain

www.evil.com

Weight	0
Domain Name	www.evil.com
WHOIS Info	Creation Date: 1995-04-10T04:00:00Z DNSSEC: unsigned Domain Name: EVIL.COM Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited Name Server: NS1.VERIO.COM Name Server: NS2.VERIO.COM Registrar Abuse Contact Email: abuse@web.com Registrar Abuse Contact Phone: +1.8003337680 Registrar IANA ID: 2 Registrar URL: http://networksolutions.com Registrar WHOIS Server: whois.networksolutions.com Registrar: Network Solutions, LLC Registry Domain ID: 1040763_DOMAIN_COM-VRSN Registry Expiry Date: 2023-04-11T04:00:00Z Updated Date: 2019-12-17T16:17:59Z

VirusTotal Domain Summary	
VirusTotal Reputation	0
Tags	
Popularity Ranking	
Cisco Umbrella	
588683	

VirusTotal Analysis Summary	
Aggregate Result	harmless - 77 / 87

VirusTotal Analysis Stats	
Analysis Type	Number of Analysis
Confirmed Timeout	0
Failure	0
Harmless	77
Malicious	1
Suspicious	0
Timeout	0
Type Unsupported	0
Undetected	9
Total	**87**

View on VirusTotal

GUI Url: https://www.virustotal.com/gui/domain/www.evil.com

Categories	
Engines	Category
Forcepoint ThreatSeeker	entertainment
BitDefender	hobbies

Community Votes

Total votes cast: 0

Incoming (4)		
	DNS Name	apitwitter.com.evil.com
	DNS Name	apitwitter.evil.com
	DNS Name	evil.com
	DNS Name	www.evil.com

Domain

maltego.Domain

apitwitter.evil.com

Weight	0
Domain Name	apitwitter.evil.com
WHOIS Info	Creation Date: 1995-04-10T04:00:00Z DNSSEC: unsigned Domain Name: EVIL.COM Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited Name Server: NS1.VERIO.COM Name Server: NS2.VERIO.COM Registrar Abuse Contact Email: abuse@web.com Registrar Abuse Contact Phone: +1.8003337680 Registrar IANA ID: 2 Registrar URL: http://networksolutions.com Registrar WHOIS Server: whois.networksolutions.com Registrar: Network Solutions, LLC Registry Domain ID: 1040763_DOMAIN_COM-VRSN Registry Expiry Date: 2023-04-11T04:00:00Z Updated Date: 2019-12-17T16:17:59Z

VirusTotal Domain Summary

VirusTotal Reputation	0
Tags	

VirusTotal Analysis Summary

Aggregate Result	harmless - 86 / 86

VirusTotal Analysis Stats

Analysis Type	Number of Analysis
Confirmed Timeout	0
Failure	0
Harmless	86
Malicious	0
Suspicious	0
Timeout	0
Type Unsupported	0
Undetected	0
Total	**86**

View on VirusTotal

GUI Url: https://www.virustotal.com/gui/domain/apitwitter.evil.com

Community Votes	
Total votes cast: 0	
Incoming (4)	
DNS Name	apitwitter.com.evil.com
DNS Name	apitwitter.evil.com
DNS Name	evil.com
DNS Name	www.evil.com

Website

maltego.Website

apitwitter.com.evil.com

Weight	100
Website	apitwitter.com.evil.com
SSL Enabled	false
Ports	[80]
SSL Ports	443

Info

View Website

Incoming (1)	
DNS Name	apitwitter.com.evil.com
Outgoing (2)	
DNS Name	apitwitter.com.evil.com
Domain	evil.com

Website

maltego.Website

apitwitter.com.w3snoop.com

Weight	100
Website	apitwitter.com.w3snoop.com
SSL Enabled	false
Ports	[80]
SSL Ports	443

Info

View Website

Incoming (1)	
DNS Name	apitwitter.com.w3snoop.com
Outgoing (2)	
DNS Name	apitwitter.com.w3snoop.com
Domain	w3snoop.com

SSL Certificate

maltego.X509Certificate

*.evil.com

Weight	0
Subject	*.evil.com
Issuer	R3
Subject DN	
Issuer DN	
SKI	daad26d1d9c7901537e84a12886ef8ddc37132e5
AKI	
Serial	4e7eefa66e979c3d6ddafbdc4dc9df0eb95
SAN	[*.evil.com, evil.com]
Usage	
Issuance ID	
Valid From	Fri Aug 06 00:00:00 GMT 2021
Valid Until	Thu Nov 04 00:00:00 GMT 2021
Country	
Organization	

Incoming (2)

DNS Name	evil.com
DNS Name	www.evil.com

Outgoing (1)

STIX2 X509 Certificate	x509-certificate--e72c2a81-44d5-5c56-b9fb-9cc476194843

SSL Certificate

maltego.X509Certificate

*.evil.com

Weight	0
Subject	*.evil.com
Issuer	Let's Encrypt Authority X3
Subject DN	
Issuer DN	
SKI	daad26d1d9c7901537e84a12886ef8ddc37132e5
AKI	
Serial	3cf1a21b5354a66ac415c5041bad6394456
SAN	[*.evil.com, evil.com]
Usage	
Issuance ID	
Valid From	Mon Jul 20 00:00:00 GMT 2020
Valid Until	Sun Oct 18 00:00:00 GMT 2020
Country	
Organization	

Incoming (2)		
	DNS Name	evil.com
	DNS Name	www.evil.com
Outgoing (1)		
	STIX2 X509 Certificate	x509-certificate--f2d07fae-c770-5241-b074-1ad8137ce391

SSL Certificate

maltego.X509Certificate

*.evil.com

Weight	0
Subject	*.evil.com
Issuer	R3
Subject DN	
Issuer DN	
SKI	daad26d1d9c7901537e84a12886ef8ddc37132e5
AKI	
Serial	4271acbc2e3b0e9d85a50d383cf03f22d22
SAN	[*.evil.com, evil.com]
Usage	
Issuance ID	
Valid From	Wed Jan 27 00:00:00 GMT 2021
Valid Until	Tue Apr 27 00:00:00 GMT 2021
Country	
Organization	

Incoming (2)		
	DNS Name	evil.com
	DNS Name	www.evil.com
Outgoing (1)		
	STIX2 X509 Certificate	x509-certificate--1ce7e13b-39f8-5d85-94ab-7567aadfe9d9

SSL Certificate

maltego.X509Certificate

*.evil.com

Weight	0
Subject	*.evil.com
Issuer	R3
Subject DN	
Issuer DN	
SKI	daad26d1d9c7901537e84a12886ef8ddc37132e5
AKI	
Serial	4425cf6c15690ba3f7635882e17b14c4e94
SAN	[*.evil.com, evil.com]
Usage	
Issuance ID	
Valid From	Mon Mar 29 00:00:00 GMT 2021
Valid Until	Sun Jun 27 00:00:00 GMT 2021
Country	
Organization	

Incoming (2)

DNS Name	evil.com
DNS Name	www.evil.com

Outgoing (1)

STIX2 X509 Certificate	x509-certificate--87052faa-ce0b-55a0-b253-95e2150038fc

NS Record

maltego.NSRecord

ns1.verio.com

Weight	0
NS Record	ns1.verio.com
Time To Live	3600
Refresh	10800
Type	SOA
Expire	604800
Minimum	3600
Serial	2016111729
Shodan Last Update	2021-09-29T05:55:26.556056+00:00
Rname	dnsadmin.verio.com
Retry	3600

Incoming (3)

DNS Name	evil.com
DNS Name	evil.com
Website	evil.com

A Record

maltego.ARecord

evil.com

Weight	0
IPv4 Address	66.96.146.129
Time to Live (TTL)	0
DNS Name	evil.com
Time To Live	3600
Type	A
Shodan Last Update	2021-09-29T05:55:26.572472+00:00

Incoming (3)

DNS Name	evil.com
DNS Name	evil.com
Website	evil.com

Phrase

maltego.Phrase

v=spf1 ip4:66.96.128.0/18 ?all

Weight	0
Text	v=spf1 ip4:66.96.128.0/18 ?all
Record Last Seen	2021-09-29T05:55:26.559229+00:00
Time To Live	3600
DNS Record Type	TXT
Type	TXT

Incoming (3)

DNS Name	evil.com
DNS Name	evil.com
Website	evil.com

NS Record

maltego.NSRecord

ns2.verio.com

Weight	0
NS Record	ns2.verio.com
Time To Live	3600
Type	NS
Shodan Last Update	2021-09-29T05:55:26.551568+00:00

Incoming (3)

DNS Name	evil.com
DNS Name	evil.com
Website	evil.com

IPv4 Address

maltego.IPv4Address

209.204.174.29

Weight	0
IP Address	209.204.174.29
Internal	false

Incoming (3)

DNS Name	evil.com
DNS Name	www.evil.com
Website	evil.com

Location

maltego.Location

WA

Weight	38
Name	WA
Country	
City	
Street Address	
Area	
Area Code	
Country Code	
Longitude	0.0
Latitude	0.0

Info

Relevance:	0.382308
Count:	1

Info

Relevance:	0.382497
Count:	1

Incoming (3)

IPv4 Address	18.232.245.187
IPv4 Address	35.175.60.16
IPv4 Address	52.86.133.10

Location

maltego.Location

Seattle

Weight	42
Name	Seattle
Country	
City	
Street Address	
Area	
Area Code	
Country Code	
Longitude	0.0
Latitude	0.0

Info

Relevance:	0.42257
Count:	1

Info

Relevance:	0.422749
Count:	1

Incoming (3)

IPv4 Address	18.232.245.187
IPv4 Address	35.175.60.16
IPv4 Address	52.86.133.10

Phone Number

maltego.PhoneNumber

+1 206 266 4064

Weight	100
Phone Number	+1 206 266 4064
Country Code	
City Code	
Area Code	
Last Digits	

Incoming (3)

IPv4 Address	18.232.245.187
IPv4 Address	35.175.60.16
IPv4 Address	52.86.133.10

Location

maltego.Location

US

Weight	48
Name	US
Country	
City	
Street Address	
Area	
Area Code	
Country Code	
Longitude	0.0
Latitude	0.0

Info

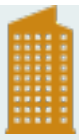
Relevance:	0.488257
Count:	2

Info

Relevance:	0.488456
Count:	2

Incoming (3)

IPv4 Address	18.232.245.187
IPv4 Address	35.175.60.16
IPv4 Address	52.86.133.10



Company

maltego.Company

Amazon Technologies Inc.

Weight	62
Name	Amazon Technologies Inc.

Info

Relevance:	0.620121
Count:	1

Info

Relevance:	0.621579
Count:	1

Incoming (3)

IPv4 Address	18.232.245.187
IPv4 Address	35.175.60.16
IPv4 Address	52.86.133.10

Website

maltego.Website

www.apitwitter.evil.co

Weight	100
Website	www.apitwitter.evil.co
SSL Enabled	false
Ports	[80]

Incoming (1)

Domain	apitwitter.evil.co

Outgoing (1)

IPv4 Address	52.128.23.153

Email Address

maltego.EmailAddress

w3snoop.com@domainsbyproxy.com

Weight	100
Email Address	w3snoop.com@domainsbyproxy.com

Incoming (2)

Domain	w3snoop.com
Domain	w3snoop.com

Email Address

maltego.EmailAddress

abuse@godaddy.com

Weight	100
Email Address	abuse@godaddy.com

Incoming (2)

Domain	w3snoop.com
Domain	w3snoop.com

Phone Number

maltego.PhoneNumber

+1 877 722 8662

Weight	100
Phone Number	+1 877 722 8662
Country Code	
City Code	
Area Code	
Last Digits	

Incoming (2)	
Domain	evil.com
Domain	evil.com

Phone Number

maltego.PhoneNumber

+1 570 708 8780

Weight	100
Phone Number	+1 570 708 8780
Country Code	
City Code	
Area Code	
Last Digits	

Incoming (2)	
Domain	evil.com
Domain	evil.com

Phone Number

maltego.PhoneNumber

+1 800 333 7680

Weight	100
Phone Number	+1 800 333 7680
Country Code	
City Code	
Area Code	
Last Digits	

Incoming (2)	
Domain	evil.com
Domain	evil.com

Domain

maltego.Domain

tajtour.co.uk

Weight	100
Domain Name	tajtour.co.uk
WHOIS Info	

Incoming (2)	
NS Record	ns1.uniregistrymarket.link
NS Record	ns2.uniregistrymarket.link

Domain

maltego.Domain

pimpmywebpage.com

Weight	100
Domain Name	pimpmywebpage.com
WHOIS Info	

Incoming (2)

NS Record	ns1.uniregistrymarket.link
NS Record	ns2.uniregistrymarket.link

Email Address

maltego.EmailAddress

domain.operations@web.com

Weight	100
Email Address	domain.operations@web.com

Incoming (2)

Domain	evil.com
Domain	evil.com

Email Address

maltego.EmailAddress

jc9aq8n264m@networksolutionsprivateregistration.com

Weight	100
Email Address	jc9aq8n264m@networksolutionsprivateregistration.com

Incoming (2)

Domain	evil.com
Domain	evil.com

VirusTotal File

maltego.virustotal.File

explorer.exe

Weight	0
MeaningfulName	explorer.exe
File Id	d3800e689103863112909a6487b87cc51d780dbda819ef23f6fd2f6d48121210
Names	explorer.exe
File Type	PEEXE
File Type Description	Win32 EXE
MD5	c2475c328d53e219e42eafbb45bce18c
SHA-1	1761cd9ceb9bb3802558339f267bd9c234786027
SHA-256	d3800e689103863112909a6487b87cc51d780dbda819ef23f6fd2f6d48121210
Vhash	016056655d15756210b02002300a46z161d013zf2za0030e039z
Authentihash	f8c684ac5761846f9de21405388e84a5606a5c858964703adcdafcf121f1f44a
SSDEEP	49152:7w80cTsjkWa/5MJXQOF3UCFgALAUDc0qbcJnM:08sjkKJgE31B8Rbcn
Magic	PE32 executable for MS Windows (GUI) Intel 80386 32-bit
File Size	1895936
Tags	peexe, direct-cpu-clock-access, detect-debug-environment, long-sleeps, runtime-modules
Capability Tags	
Downloadable	null
Creation Date	2016-01-21T20:55:37Z
First Submission Date	2016-01-21T21:41:33Z
Last Submission Date	2016-02-04T14:00:30Z
Last Analysis Date	2021-07-07T03:29Z
Total Votes - Harmless	0
Total Votes - Malicious	0
Submissions	3
Reputation	0

View on VirusTotal

GUI Url:
https://www.virustotal.com/gui/file/d3800e689103863112909a6487b87cc51d780dbda819ef23f6fd2f6d48121210

File Summary

Names	explorer.exe
File Type	peexe
File Type Description	Win32 EXE
Tags	peexe, direct-cpu-clock-access, detect-debug-environment, long-sleeps, runtime-modules
Times Submitted	3

TrID - file type identification tool	
File Type	Probability %
Windows Control Panel Item (generic)	85.7
Win64 Executable (generic)	4.5
Win32 Dynamic Link Library (generic)	2.8
Win16 NE executable (generic)	2.1
Win32 Executable (generic)	1.9

VirusTotal Analysis Summary	
Aggregate Result	malicious - 42 / 74

VirusTotal Analysis Stats	
Analysis Type	Number of Analysis
Confirmed Timeout	0
Failure	0
Harmless	0
Malicious	42
Suspicious	0
Timeout	0
Type Unsupported	5
Undetected	27
Total	**74**

Community Votes

Total votes cast: 0

Incoming (2)

DNS Name	www.evil.com
DNS Name	www.evil.com

Email Address

maltego.EmailAddress

n69pg4637nj@networksolutionsprivateregistration.com

Weight	100
Email Address	n69pg4637nj@networksolutionsprivateregistration.com

Incoming (2)

Domain	evil.com
Domain	evil.com

Email Address

maltego.EmailAddress

abuse@web.com

Weight	100
Email Address	abuse@web.com

Incoming (2)

Domain	evil.com
Domain	evil.com

Domain

maltego.Domain

volumized.com

Weight	100
Domain Name	volumized.com
WHOIS Info	

Incoming (2)

NS Record	ns1.uniregistrymarket.link
NS Record	ns2.uniregistrymarket.link

Domain

maltego.Domain

newbi.com

Weight	100
Domain Name	newbi.com
WHOIS Info	

Incoming (2)

NS Record	ns1.uniregistrymarket.link
NS Record	ns2.uniregistrymarket.link

Domain

maltego.Domain

bbcswahili.co.uk

Weight	100
Domain Name	bbcswahili.co.uk
WHOIS Info	

Incoming (2)

NS Record	ns1.uniregistrymarket.link
NS Record	ns2.uniregistrymarket.link

Domain

maltego.Domain

ggoel.co.uk

Weight	100
Domain Name	ggoel.co.uk
WHOIS Info	

Incoming (2)

NS Record	ns1.uniregistrymarket.link
NS Record	ns2.uniregistrymarket.link

Domain

maltego.Domain

jumpershorseline.co.uk

Weight	100
Domain Name	jumpershorseline.co.uk
WHOIS Info	

Incoming (2)

NS Record	ns1.uniregistrymarket.link
NS Record	ns2.uniregistrymarket.link

Domain

maltego.Domain

leedsbradford.co.uk

Weight	100
Domain Name	leedsbradford.co.uk
WHOIS Info	

Incoming (2)

NS Record	ns1.uniregistrymarket.link
NS Record	ns2.uniregistrymarket.link

Domain

maltego.Domain

mybham.co.uk

Weight	100
Domain Name	mybham.co.uk
WHOIS Info	

Incoming (2)

NS Record	ns1.uniregistrymarket.link
NS Record	ns2.uniregistrymarket.link

Domain

maltego.Domain

chowchilla.com

Weight	100
Domain Name	chowchilla.com
WHOIS Info	

Incoming (2)

NS Record	ns1.uniregistrymarket.link
NS Record	ns2.uniregistrymarket.link

Domain

maltego.Domain

trly.com

Weight	100
Domain Name	trly.com
WHOIS Info	

Incoming (2)

NS Record	ns1.uniregistrymarket.link
NS Record	ns2.uniregistrymarket.link

SSL Certificate

maltego.X509Certificate

*.evil.com

Weight	0
Subject	*.evil.com
Issuer	Let's Encrypt Authority X3
Subject DN	
Issuer DN	
SKI	daad26d1d9c7901537e84a12886ef8ddc37132e5
AKI	
Serial	4d85160cb2985067bf4de4e95b88110a9f5
SAN	[*.evil.com, evil.com]
Usage	
Issuance ID	
Valid From	Tue Nov 17 00:00:00 GMT 2020
Valid Until	Mon Feb 15 00:00:00 GMT 2021
Country	
Organization	

Incoming (2)

DNS Name	evil.com
DNS Name	www.evil.com

SSL Certificate

maltego.X509Certificate

*.evil.com

Weight	0
Subject	*.evil.com
Issuer	Let's Encrypt Authority X3
Subject DN	
Issuer DN	
SKI	daad26d1d9c7901537e84a12886ef8ddc37132e5
AKI	
Serial	430d943b638186b5dbd2b63522bf012bc7e
SAN	[*.evil.com, evil.com]
Usage	
Issuance ID	
Valid From	Fri Sep 18 00:00:00 GMT 2020
Valid Until	Thu Dec 17 00:00:00 GMT 2020
Country	
Organization	

Incoming (2)

DNS Name	evil.com
DNS Name	www.evil.com

SSL Certificate

maltego.X509Certificate

*.evil.com

Weight	0
Subject	*.evil.com
Issuer	Let's Encrypt Authority X3
Subject DN	
Issuer DN	
SKI	daad26d1d9c7901537e84a12886ef8ddc37132e5
AKI	
Serial	45cab7ae987d1b8a5bc809cafdda80e2022
SAN	[*.evil.com, evil.com]
Usage	
Issuance ID	
Valid From	Wed May 20 00:00:00 GMT 2020
Valid Until	Tue Aug 18 00:00:00 GMT 2020
Country	
Organization	

Incoming (2)

DNS Name	evil.com
DNS Name	www.evil.com

SSL Certificate

maltego.X509Certificate

*.evil.com

Weight	0
Subject	*.evil.com
Issuer	R3
Subject DN	
Issuer DN	
SKI	daad26d1d9c7901537e84a12886ef8ddc37132e5
AKI	
Serial	4231e61d5a0929e7c28bbd9c9534979cee2
SAN	[*.evil.com, evil.com]
Usage	
Issuance ID	
Valid From	Sun May 30 00:00:00 GMT 2021
Valid Until	Sat Aug 28 00:00:00 GMT 2021
Country	
Organization	

Incoming (2)

DNS Name	evil.com
DNS Name	www.evil.com

SSL Certificate

maltego.X509Certificate

*.evil.com

Weight	0
Subject	*.evil.com
Issuer	Let's Encrypt Authority X3
Subject DN	
Issuer DN	
SKI	daad26d1d9c7901537e84a12886ef8ddc37132e5
AKI	
Serial	3e24d02ef5befc3664d60bf87b7831375b9
SAN	[*.evil.com, evil.com]
Usage	
Issuance ID	
Valid From	Sat Mar 21 00:00:00 GMT 2020
Valid Until	Fri Jun 19 00:00:00 GMT 2020
Country	
Organization	

Incoming (2)

DNS Name	evil.com
DNS Name	www.evil.com

SSL Certificate

maltego.X509Certificate

*.evil.com

Weight	0
Subject	*.evil.com
Issuer	Let's Encrypt Authority X3
Subject DN	
Issuer DN	
SKI	daad26d1d9c7901537e84a12886ef8ddc37132e5
AKI	
Serial	3b1e1a9cd50790c8d75b430f927acd06d3a
SAN	[*.evil.com, evil.com]
Usage	
Issuance ID	
Valid From	Wed Nov 20 00:00:00 GMT 2019
Valid Until	Tue Feb 18 00:00:00 GMT 2020
Country	
Organization	

Incoming (2)

DNS Name	evil.com
DNS Name	www.evil.com

SSL Certificate

maltego.X509Certificate

*.evil.com

Weight	0
Subject	*.evil.com
Issuer	Let's Encrypt Authority X3
Subject DN	
Issuer DN	
SKI	daad26d1d9c7901537e84a12886ef8ddc37132e5
AKI	
Serial	3d2a49992f66f2aec8f164c03701d6e56fb
SAN	[*.evil.com, evil.com]
Usage	
Issuance ID	
Valid From	Mon Jan 20 00:00:00 GMT 2020
Valid Until	Sun Apr 19 00:00:00 GMT 2020
Country	
Organization	

Incoming (2)

DNS Name	evil.com
DNS Name	www.evil.com

SSL Certificate

maltego.X509Certificate

w3snoop.com

Weight	0
Subject	w3snoop.com
Issuer	Let's Encrypt Authority X3
Subject DN	
Issuer DN	
SKI	2a553be787a81957f51f9555078139d59b28e3fc
AKI	
Serial	33cef15d62eb0cf8720c596134ceba66e49
SAN	[*.ac.in.w3snoop.com, *.ac.uk.w3snoop.com, *.ae.w3snoop.com, *.at.w3snoop.com, *.az.w3snoop.com, *.be.w3snoop.com, *.bg.w3snoop.com, *.biz.w3snoop.com, *.by.w3snoop.com, *.ca.w3snoop.com, *.cc.w3snoop.com, *.ch.w3snoop.com, *.cl.w3snoop.com, *.cn.w3snoop.com, *.co.id.w3snoop.com, *.co.il.w3snoop.com, *.co.in.w3snoop.com, *.co.jp.w3snoop.com, *.co.kr.w3snoop.com, *.co.nz.w3snoop.com, *.co.uk.w3snoop.com, *.co.w3snoop.com, *.co.za.w3snoop.com, *.com.ar.w3snoop.com, *.com.au.w3snoop.com, *.com.br.w3snoop.com, *.com.cn.w3snoop.com, *.com.co.w3snoop.com, *.com.hk.w3snoop.com, *.com.mx.w3snoop.com, *.com.my.w3snoop.com, *.com.pk.w3snoop.com, *.com.pl.w3snoop.com, *.com.sg.w3snoop.com, *.com.tr.w3snoop.com, *.com.tw.w3snoop.com, *.com.ua.w3snoop.com, *.com.vn.w3snoop.com, *.com.w3snoop.com, *.cz.w3snoop.com, *.de.w3snoop.com, *.dk.w3snoop.com, *.edu.w3snoop.com, *.ee.w3snoop.com, *.es.w3snoop.com, *.eu.w3snoop.com, *.fi.w3snoop.com, *.fm.w3snoop.com, *.fr.w3snoop.com, *.gov.cn.w3snoop.com, *.gov.w3snoop.com, *.gr.w3snoop.com, *.hk.w3snoop.com, *.hr.w3snoop.com, *.hu.w3snoop.com, *.ie.w3snoop.com, *.in.w3snoop.com, *.info.w3snoop.com, *.io.w3snoop.com, *.ir.w3snoop.com, *.it.w3snoop.com, *.jp.w3snoop.com, *.kz.w3snoop.com, *.lt.w3snoop.com, *.lv.w3snoop.com, *.md.w3snoop.com, *.me.w3snoop.com, *.mobi.w3snoop.com, *.mx.w3snoop.com, *.name.w3snoop.com, *.ne.jp.w3snoop.com, *.net.au.w3snoop.com, *.net.w3snoop.com, *.nl.w3snoop.com, *.no.w3snoop.com, *.nu.w3snoop.com, *.or.jp.w3snoop.com, *.org.au.w3snoop.com, *.org.br.w3snoop.com, *.org.uk.w3snoop.com, *.org.w3snoop.com, *.pk.w3snoop.com, *.pl.w3snoop.com, *.pt.w3snoop.com, *.ro.w3snoop.com, *.rs.w3snoop.com, *.ru.w3snoop.com, *.se.w3snoop.com, *.si.w3snoop.com, *.sk.w3snoop.com, *.su.w3snoop.com, *.tk.w3snoop.com, *.to.w3snoop.com, *.tv.w3snoop.com, *.ua.w3snoop.com, *.us.w3snoop.com, *.vn.w3snoop.com, *.w3snoop.com, *.ws.w3snoop.com, w3snoop.com]
Usage	
Issuance ID	
Valid From	Wed Aug 19 00:00:00 GMT 2020
Valid Until	Tue Nov 17 00:00:00 GMT 2020
Country	
Organization	

Incoming (2)

DNS Name	apitwitter.com.w3snoop.com
DNS Name	apitwitter.com.w3snoop.com

PeeringDB Network

maltego.PeeringDBNetwork

VeriSign Global Registry Services

Weight	100
maltego.PeeringDBNetwork	VeriSign Global Registry Services
ID	9897
Organization ID	1124
Org	
Name	VeriSign Global Registry Services
Also known as	
Website	http://www.verisign.com/rirs
ASN	26415
Looking glass	
Route server	
IRR AS set	AS-GTLD
Info type	NSP
Info prefixes4	300
Info prefixes6	50
Info traffic	
Info ratio	Mostly Outbound
Info scope	Global
Unicast	true
Multicast	false
IPv6	true
Never via route servers	false
Notes	Exchanges/facilities with a peering AS of 26415 denote a point of interconnection with Version's Regional Internet Resolution Site service. To obtain information, please visit http://www.verisign.com/rirs For all peering requests, please send email to peering@verisign.com
Policy URL	http://www.verisign.com/
Policy general	Open
Policy locations	Preferred
Policy ratio	false
Policy contracts	Not Required
Created	
Updated	
Status	ok
Allow IXP update	false
netixlan_updated	2021-09-22T00:08:26.672699Z
poc_updated	2021-05-27T16:15:36.993111Z
ix_count	71

Important Properties

Asn	26415
Info Type	NSP
Info Ratio	Mostly Outbound
Info Scope	Global

Peering Information

Policy Url	http://www.verisign.com/
Policy General	Open
Policy Locations	Preferred
Policy Contracts	Not Required

PeeringDB

View on PeeringDB

Notes

Exchanges/facilities with a peering AS of 26415 denote a point of interconnection with Version's Regional Internet Resolution Site service. To obtain information, please visit http://www.verisign.com/rirs

For all peering requests, please send email to peering@verisign.com

Incoming (2)

Company	VeriSign
Company	VeriSign

A Record

maltego.ARecord

www.evil.com

Weight	0
IPv4 Address	66.96.146.129
Time to Live (TTL)	0
DNS Name	www.evil.com
Time To Live	3600
Type	A
Shodan Last Update	2021-10-02T16:16:29.744256+00:00

Incoming (2)

DNS Name	www.evil.com
DNS Name	www.evil.com

PeeringDB Network

maltego.PeeringDBNetwork

Verisign

Weight	100
maltego.PeeringDBNetwork	Verisign
ID	873
Organization ID	1124
Org	
Name	Verisign
Also known as	
Website	http://www.verisign.com/
ASN	7342
Looking glass	
Route server	
IRR AS set	AS-GTLD
Info type	NSP
Info prefixes4	300
Info prefixes6	300
Info traffic	
Info ratio	Balanced
Info scope	Global
Unicast	true
Multicast	false
IPv6	true
Never via route servers	false
Notes	Exchanges/facilities with a peering AS of 7342 denote a point of interconnection with Verisign's global network To obtain information on adding a Verisign root, .COM or .NET authoritative DNS server to your network, please visit http://www.verisign.com/rirs
Policy URL	
Policy general	Open
Policy locations	Not Required
Policy ratio	false
Policy contracts	Not Required
Created	
Updated	
Status	ok
Allow IXP update	false
netixlan_updated	2021-09-22T00:07:41.256252Z
poc_updated	2020-01-22T04:24:13Z
ix_count	11
fac_count	11
netfac_updated	2021-06-01T17:56:46.130081Z

Important Properties

Asn	7342
Info Type	NSP
Info Ratio	Balanced
Info Scope	Global

Peering Information

Policy General	Open
Policy Locations	Not Required
Policy Contracts	Not Required

PeeringDB

View on PeeringDB

Notes

Exchanges/facilities with a peering AS of 7342 denote a point of interconnection with Verisign's global network

To obtain information on adding a Verisign root, .COM or .NET authoritative DNS server to your network, please visit http://www.verisign.com/rirs

Incoming (2)

Company	VeriSign
Company	VeriSign

Peering DB Organization

maltego.PeeringDBOrganization

VeriSign

Weight	100
ID	1124
Name	VeriSign
Website	http://www.verisign.com
Notes	
Address line 1	12061 Bluemont Way
Address line 2	
City	Reston,
Country	US
State	VA
ZIP code	20190
Created	
Updated	
Status	ok
Name	VeriSign

Details

VeriSign

Website

12061 Bluemont Way

PeeringDB

View on PeeringDB

Incoming (2)

Company	VeriSign
Company	VeriSign

Domain

maltego.Domain

c2.evil.com

Weight	0
Domain Name	c2.evil.com
WHOIS Info	Creation Date: 1995-04-10T04:00:00Z DNSSEC: unsigned Domain Name: EVIL.COM Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited Name Server: NS1.VERIO.COM Name Server: NS2.VERIO.COM Registrar Abuse Contact Email: abuse@web.com Registrar Abuse Contact Phone: +1.8003337680 Registrar IANA ID: 2 Registrar URL: http://networksolutions.com Registrar WHOIS Server: whois.networksolutions.com Registrar: Network Solutions, LLC Registry Domain ID: 1040763_DOMAIN_COM-VRSN Registry Expiry Date: 2023-04-11T04:00:00Z Updated Date: 2019-12-17T16:17:59Z

VirusTotal Domain Summary

VirusTotal Reputation	0
Tags	

VirusTotal Analysis Summary

Aggregate Result	harmless - 79 / 87

VirusTotal Analysis Stats

Analysis Type	Number of Analysis
Confirmed Timeout	0
Failure	0
Harmless	79
Malicious	0
Suspicious	0
Timeout	0
Type Unsupported	0
Undetected	8
Total	**87**

View on VirusTotal

GUI Url: https://www.virustotal.com/gui/domain/c2.evil.com

Categories

Engines	Category
Forcepoint ThreatSeeker	entertainment
BitDefender	hobbies

Community Votes

Total votes cast: 0

Incoming (2)

DNS Name	apitwitter.evil.com
DNS Name	www.evil.com

DNS Name

maltego.DNSName

*.to.w3snoop.com

Weight	0
DNS Name	*.to.w3snoop.com

Incoming (2)

DNS Name	w3snoop.com
DNS Name	w3snoop.com

DNS Name

maltego.DNSName

cf-ez-middleton.w3snoop.com

Weight	0
DNS Name	cf-ez-middleton.w3snoop.com

Incoming (2)

DNS Name	w3snoop.com
DNS Name	w3snoop.com

DNS Name

maltego.DNSName

*.lt.w3snoop.com

Weight	0
DNS Name	*.lt.w3snoop.com

Incoming (2)

DNS Name	w3snoop.com
DNS Name	w3snoop.com

DNS Name

maltego.DNSName

*.ee.w3snoop.com

Weight	0
DNS Name	*.ee.w3snoop.com

Incoming (2)

DNS Name	w3snoop.com
DNS Name	w3snoop.com

DNS Name

maltego.DNSName

*.hr.w3snoop.com

Weight	0
DNS Name	*.hr.w3snoop.com

Incoming (2)

DNS Name	w3snoop.com
DNS Name	w3snoop.com

DNS Name

maltego.DNSName

*.pk.w3snoop.com

Weight	0
DNS Name	*.pk.w3snoop.com

Incoming (2)

DNS Name	w3snoop.com
DNS Name	w3snoop.com

DNS Name

maltego.DNSName

*.hu.w3snoop.com

Weight	0
DNS Name	*.hu.w3snoop.com

Incoming (2)

DNS Name	w3snoop.com
DNS Name	w3snoop.com

DNS Name

maltego.DNSName

*.ac.uk.w3snoop.com

Weight	0
DNS Name	*.ac.uk.w3snoop.com

Incoming (2)

DNS Name	w3snoop.com
DNS Name	w3snoop.com

DNS Name

maltego.DNSName

*.ua.w3snoop.com

Weight	0
DNS Name	*.ua.w3snoop.com

Incoming (2)

DNS Name	w3snoop.com
DNS Name	w3snoop.com

DNS Name

maltego.DNSName

*.com.br.w3snoop.com

Weight	0
DNS Name	*.com.br.w3snoop.com

Incoming (2)

DNS Name	w3snoop.com
DNS Name	w3snoop.com

DNS Name

maltego.DNSName

*.lv.w3snoop.com

Weight	0
DNS Name	*.lv.w3snoop.com

Incoming (2)

DNS Name	w3snoop.com
DNS Name	w3snoop.com

Domain

maltego.Domain

hr.w3snoop.com

Weight	0
Domain Name	hr.w3snoop.com
WHOIS Info	Admin City: Tempe Admin Country: US Admin Email: c9b5a1cf1d0c3764s@domainsbyproxy.com Admin Organization: Domains By Proxy, LLC Admin Postal Code: 85284 Admin State/Province: Arizona Creation Date: 2011-06-05T21:04:22Z Creation Date: 2011-06-06T02:04:22Z DNSSEC: unsigned Domain Name: W3SNOOP.COM Domain Status: clientDeleteProhibited http://www.icann.org/epp#clientDeleteProhibited Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited Domain Status: clientRenewProhibited http://www.icann.org/epp#clientRenewProhibited Domain Status: clientRenewProhibited https://icann.org/epp#clientRenewProhibited Domain Status: clientTransferProhibited http://www.icann.org/epp#clientTransferProhibited Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Domain Status: clientUpdateProhibited http://www.icann.org/epp#clientUpdateProhibited Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited Name Server: INDRI.EZOICNS.COM Name Server: SAOLA.EZOICNS.COM Registrant City: a7319ae5e6c95df5 Registrant Country: US Registrant Email: c9b5a1cf1d0c3764s@domainsbyproxy.com Registrant Fax Ext: 3432650ec337c945 Registrant Fax: 9fad764be0c7e95d Registrant Name: 80315b2e6ac1a801 Registrant Organization: b46a98a26fe2fd9f Registrant Phone Ext: 3432650ec337c945 Registrant Phone: d5f66d3a005b000d Registrant Postal Code: 052e5bd148f904f9 Registrant State/Province: 30bdd2917a604c83 Registrant Street: 037792fd5a6fe619 Registrant Street: d733533b6a6c0c21 Registrar Abuse Contact Email: abuse@godaddy.com Registrar Abuse Contact Phone: +1.4806242505 Registrar Abuse Contact Phone: 480-624-2505 Registrar IANA ID: 146 Registrar Registration Expiration Date: 2023-06-05T21:04:22Z Registrar URL: http://www.godaddy.com Registrar WHOIS Server: whois.godaddy.com Registrar: GoDaddy.com, LLC Registry Admin ID: Not Available From Registry Registry Domain ID: 1660071767_DOMAIN_COM-VRSN Registry Expiry Date: 2023-06-06T02:04:22Z Registry Registrant ID: Not Available From Registry Registry Tech ID: Not Available From Registry Tech City: Tempe Tech Country: US Tech Email: c9b5a1cf1d0c3764s@domainsbyproxy.com Tech Organization: Domains By Proxy, LLC Tech Postal Code: 85284 Tech State/Province: Arizona Updated Date: 2020-02-09T21:49:40Z Updated Date: 2020-02-10T04:49:41Z

VirusTotal Domain Summary	
VirusTotal Reputation	0
Tags	

VirusTotal Analysis Summary	
Aggregate Result	harmless - 80 / 88

VirusTotal Analysis Stats	
Analysis Type	Number of Analysis
Confirmed Timeout	0
Failure	0
Harmless	80
Malicious	0
Suspicious	0
Timeout	0
Type Unsupported	0
Undetected	8
Total	**88**

View on VirusTotal

GUI Url: https://www.virustotal.com/gui/domain/hr.w3snoop.com

Community Votes

Total votes cast: 0

Incoming (2)

DNS Name	apitwitter.com.w3snoop.com
DNS Name	w3snoop.com

Domain

maltego.Domain

jp.w3snoop.com

Weight	0
Domain Name	jp.w3snoop.com
WHOIS Info	Admin City: Tempe Admin Country: US Admin Email: c9b5a1cf1d0c3764s@domainsbyproxy.com Admin Organization: Domains By Proxy, LLC Admin Postal Code: 85284 Admin State/Province: Arizona Creation Date: 2011-06-05T21:04:22Z Creation Date: 2011-06-06T02:04:22Z DNSSEC: unsigned Domain Name: W3SNOOP.COM Domain Status: clientDeleteProhibited http://www.icann.org/epp#clientDeleteProhibited Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited Domain Status: clientRenewProhibited http://www.icann.org/epp#clientRenewProhibited Domain Status: clientRenewProhibited https://icann.org/epp#clientRenewProhibited Domain Status: clientTransferProhibited http://www.icann.org/epp#clientTransferProhibited Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Domain Status: clientUpdateProhibited http://www.icann.org/epp#clientUpdateProhibited Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited Name Server: INDRI.EZOICNS.COM Name Server: SAOLA.EZOICNS.COM Registrant City: a7319ae5e6c95df5 Registrant Country: US Registrant Email: c9b5a1cf1d0c3764s@domainsbyproxy.com Registrant Fax Ext: 3432650ec337c945 Registrant Fax: 9fad764be0c7e95d Registrant Name: 80315b2e6ac1a801 Registrant Organization: b46a98a26fe2fd9f Registrant Phone Ext: 3432650ec337c945 Registrant Phone: d5f66d3a005b000d Registrant Postal Code: 052e5bd148f904f9 Registrant State/Province: 30bdd2917a604c83 Registrant Street: 037792fd5a6fe619 Registrant Street: d733533b6a6c0c21 Registrar Abuse Contact Email: abuse@godaddy.com Registrar Abuse Contact Phone: +1.4806242505 Registrar Abuse Contact Phone: 480-624-2505 Registrar IANA ID: 146 Registrar Registration Expiration Date: 2023-06-05T21:04:22Z Registrar URL: http://www.godaddy.com Registrar WHOIS Server: whois.godaddy.com Registrar: GoDaddy.com, LLC Registry Admin ID: Not Available From Registry Registry Domain ID: 1660071767_DOMAIN_COM-VRSN Registry Expiry Date: 2023-06-06T02:04:22Z Registry Registrant ID: Not Available From Registry Registry Tech ID: Not Available From Registry Tech City: Tempe Tech Country: US Tech Email: c9b5a1cf1d0c3764s@domainsbyproxy.com Tech Organization: Domains By Proxy, LLC Tech Postal Code: 85284 Tech State/Province: Arizona Updated Date: 2020-02-09T21:49:40Z Updated Date: 2020-02-10T04:49:41Z

VirusTotal Domain Summary

VirusTotal Reputation	0
Tags	

VirusTotal Analysis Summary	
Aggregate Result	harmless - 80 / 88

VirusTotal Analysis Stats	
Analysis Type	Number of Analysis
Confirmed Timeout	0
Failure	0
Harmless	80
Malicious	0
Suspicious	0
Timeout	0
Type Unsupported	0
Undetected	8
Total	**88**

View on VirusTotal

GUI Url: https://www.virustotal.com/gui/domain/jp.w3snoop.com

Categories	
Engines	Category
Forcepoint ThreatSeeker	information technology

Community Votes

Total votes cast: 0

Incoming (2)

DNS Name	apitwitter.com.w3snoop.com
DNS Name	w3snoop.com

Domain

maltego.Domain

ro.w3snoop.com

Weight	0
Domain Name	ro.w3snoop.com
WHOIS Info	Admin City: Tempe Admin Country: US Admin Email: c9b5a1cf1d0c3764s@domainsbyproxy.com Admin Organization: Domains By Proxy, LLC Admin Postal Code: 85284 Admin State/Province: Arizona Creation Date: 2011-06-05T21:04:22Z Creation Date: 2011-06-06T02:04:22Z DNSSEC: unsigned Domain Name: W3SNOOP.COM Domain Status: clientDeleteProhibited http://www.icann.org/epp#clientDeleteProhibited Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited Domain Status: clientRenewProhibited http://www.icann.org/epp#clientRenewProhibited Domain Status: clientRenewProhibited https://icann.org/epp#clientRenewProhibited Domain Status: clientTransferProhibited http://www.icann.org/epp#clientTransferProhibited Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Domain Status: clientUpdateProhibited http://www.icann.org/epp#clientUpdateProhibited Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited Name Server: INDRI.EZOICNS.COM Name Server: SAOLA.EZOICNS.COM Registrant City: a7319ae5e6c95df5 Registrant Country: US Registrant Email: c9b5a1cf1d0c3764s@domainsbyproxy.com Registrant Fax Ext: 3432650ec337c945 Registrant Fax: 9fad764be0c7e95d Registrant Name: 80315b2e6ac1a801 Registrant Organization: b46a98a26fe2fd9f Registrant Phone Ext: 3432650ec337c945 Registrant Phone: d5f66d3a005b000d Registrant Postal Code: 052e5bd148f904f9 Registrant State/Province: 30bdd2917a604c83 Registrant Street: 037792fd5a6fe619 Registrant Street: d733533b6a6c0c21 Registrar Abuse Contact Email: abuse@godaddy.com Registrar Abuse Contact Phone: +1.4806242505 Registrar Abuse Contact Phone: 480-624-2505 Registrar IANA ID: 146 Registrar Registration Expiration Date: 2023-06-05T21:04:22Z Registrar URL: http://www.godaddy.com Registrar WHOIS Server: whois.godaddy.com Registrar: GoDaddy.com, LLC Registry Admin ID: Not Available From Registry Registry Domain ID: 1660071767_DOMAIN_COM-VRSN Registry Expiry Date: 2023-06-06T02:04:22Z Registry Registrant ID: Not Available From Registry Registry Tech ID: Not Available From Registry Tech City: Tempe Tech Country: US Tech Email: c9b5a1cf1d0c3764s@domainsbyproxy.com Tech Organization: Domains By Proxy, LLC Tech Postal Code: 85284 Tech State/Province: Arizona Updated Date: 2020-02-09T21:49:40Z Updated Date: 2020-02-10T04:49:41Z

VirusTotal Domain Summary

VirusTotal Reputation	0
Tags	

VirusTotal Analysis Summary	
Aggregate Result	harmless - 80 / 88

VirusTotal Analysis Stats	
Analysis Type	Number of Analysis
Confirmed Timeout	0
Failure	0
Harmless	80
Malicious	0
Suspicious	0
Timeout	0
Type Unsupported	0
Undetected	8
Total	**88**

View on VirusTotal

GUI Url: https://www.virustotal.com/gui/domain/ro.w3snoop.com

Categories	
Engines	Category
Forcepoint ThreatSeeker	information technology

Community Votes

Total votes cast: 0

Incoming (2)

DNS Name	apitwitter.com.w3snoop.com
DNS Name	w3snoop.com

Domain

maltego.Domain

su.w3snoop.com

Weight	0
Domain Name	su.w3snoop.com
WHOIS Info	Admin City: Tempe Admin Country: US Admin Email: c9b5a1cf1d0c3764s@domainsbyproxy.com Admin Organization: Domains By Proxy, LLC Admin Postal Code: 85284 Admin State/Province: Arizona Creation Date: 2011-06-05T21:04:22Z Creation Date: 2011-06-06T02:04:22Z DNSSEC: unsigned Domain Name: W3SNOOP.COM Domain Status: clientDeleteProhibited http://www.icann.org/epp#clientDeleteProhibited Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited Domain Status: clientRenewProhibited http://www.icann.org/epp#clientRenewProhibited Domain Status: clientRenewProhibited https://icann.org/epp#clientRenewProhibited Domain Status: clientTransferProhibited http://www.icann.org/epp#clientTransferProhibited Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Domain Status: clientUpdateProhibited http://www.icann.org/epp#clientUpdateProhibited Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited Name Server: INDRI.EZOICNS.COM Name Server: SAOLA.EZOICNS.COM Registrant City: a7319ae5e6c95df5 Registrant Country: US Registrant Email: c9b5a1cf1d0c3764s@domainsbyproxy.com Registrant Fax Ext: 3432650ec337c945 Registrant Fax: 9fad764be0c7e95d Registrant Name: 80315b2e6ac1a801 Registrant Organization: b46a98a26fe2fd9f Registrant Phone Ext: 3432650ec337c945 Registrant Phone: d5f66d3a005b000d Registrant Postal Code: 052e5bd148f904f9 Registrant State/Province: 30bdd2917a604c83 Registrant Street: 037792fd5a6fe619 Registrant Street: d733533b6a6c0c21 Registrar Abuse Contact Email: abuse@godaddy.com Registrar Abuse Contact Phone: +1.4806242505 Registrar Abuse Contact Phone: 480-624-2505 Registrar IANA ID: 146 Registrar Registration Expiration Date: 2023-06-05T21:04:22Z Registrar URL: http://www.godaddy.com Registrar WHOIS Server: whois.godaddy.com Registrar: GoDaddy.com, LLC Registry Admin ID: Not Available From Registry Registry Domain ID: 1660071767_DOMAIN_COM-VRSN Registry Expiry Date: 2023-06-06T02:04:22Z Registry Registrant ID: Not Available From Registry Registry Tech ID: Not Available From Registry Tech City: Tempe Tech Country: US Tech Email: c9b5a1cf1d0c3764s@domainsbyproxy.com Tech Organization: Domains By Proxy, LLC Tech Postal Code: 85284 Tech State/Province: Arizona Updated Date: 2020-02-09T21:49:40Z Updated Date: 2020-02-10T04:49:41Z

VirusTotal Domain Summary

VirusTotal Reputation	0
Tags	

VirusTotal Analysis Summary	
Aggregate Result	harmless - 80 / 88

VirusTotal Analysis Stats	
Analysis Type	Number of Analysis
Confirmed Timeout	0
Failure	0
Harmless	80
Malicious	0
Suspicious	0
Timeout	0
Type Unsupported	0
Undetected	8
Total	**88**

View on VirusTotal

GUI Url: https://www.virustotal.com/gui/domain/su.w3snoop.com

Community Votes

Total votes cast: 0

Incoming (2)

DNS Name	apitwitter.com.w3snoop.com
DNS Name	w3snoop.com

Domain

maltego.Domain

ir.w3snoop.com

Weight	0
Domain Name	ir.w3snoop.com
WHOIS Info	Admin City: Tempe Admin Country: US Admin Email: c9b5a1cf1d0c3764s@domainsbyproxy.com Admin Organization: Domains By Proxy, LLC Admin Postal Code: 85284 Admin State/Province: Arizona Creation Date: 2011-06-05T21:04:22Z Creation Date: 2011-06-06T02:04:22Z DNSSEC: unsigned Domain Name: W3SNOOP.COM Domain Status: clientDeleteProhibited http://www.icann.org/epp#clientDeleteProhibited Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited Domain Status: clientRenewProhibited http://www.icann.org/epp#clientRenewProhibited Domain Status: clientRenewProhibited https://icann.org/epp#clientRenewProhibited Domain Status: clientTransferProhibited http://www.icann.org/epp#clientTransferProhibited Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Domain Status: clientUpdateProhibited http://www.icann.org/epp#clientUpdateProhibited Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited Name Server: INDRI.EZOICNS.COM Name Server: SAOLA.EZOICNS.COM Registrant City: a7319ae5e6c95df5 Registrant Country: US Registrant Email: c9b5a1cf1d0c3764s@domainsbyproxy.com Registrant Fax Ext: 3432650ec337c945 Registrant Fax: 9fad764be0c7e95d Registrant Name: 80315b2e6ac1a801 Registrant Organization: b46a98a26fe2fd9f Registrant Phone Ext: 3432650ec337c945 Registrant Phone: d5f66d3a005b000d Registrant Postal Code: 052e5bd148f904f9 Registrant State/Province: 30bdd2917a604c83 Registrant Street: 037792fd5a6fe619 Registrant Street: d733533b6a6c0c21 Registrar Abuse Contact Email: abuse@godaddy.com Registrar Abuse Contact Phone: +1.4806242505 Registrar Abuse Contact Phone: 480-624-2505 Registrar IANA ID: 146 Registrar Registration Expiration Date: 2023-06-05T21:04:22Z Registrar URL: http://www.godaddy.com Registrar WHOIS Server: whois.godaddy.com Registrar: GoDaddy.com, LLC Registry Admin ID: Not Available From Registry Registry Domain ID: 1660071767_DOMAIN_COM-VRSN Registry Expiry Date: 2023-06-06T02:04:22Z Registry Registrant ID: Not Available From Registry Registry Tech ID: Not Available From Registry Tech City: Tempe Tech Country: US Tech Email: c9b5a1cf1d0c3764s@domainsbyproxy.com Tech Organization: Domains By Proxy, LLC Tech Postal Code: 85284 Tech State/Province: Arizona Updated Date: 2020-02-09T21:49:40Z Updated Date: 2020-02-10T04:49:41Z

VirusTotal Domain Summary

VirusTotal Reputation	0
Tags	

VirusTotal Analysis Summary	
Aggregate Result	harmless - 80 / 88

VirusTotal Analysis Stats	
Analysis Type	Number of Analysis
Confirmed Timeout	0
Failure	0
Harmless	80
Malicious	0
Suspicious	0
Timeout	0
Type Unsupported	0
Undetected	8
Total	**88**

View on VirusTotal

GUI Url: https://www.virustotal.com/gui/domain/ir.w3snoop.com

Categories	
Engines	Category
Forcepoint ThreatSeeker	information technology

Community Votes

Total votes cast: 0

Incoming (2)

DNS Name	apitwitter.com.w3snoop.com
DNS Name	w3snoop.com

Domain

maltego.Domain

in.w3snoop.com

Weight	0
Domain Name	in.w3snoop.com
WHOIS Info	Admin City: Tempe Admin Country: US Admin Email: c9b5a1cf1d0c3764s@domainsbyproxy.com Admin Organization: Domains By Proxy, LLC Admin Postal Code: 85284 Admin State/Province: Arizona Creation Date: 2011-06-05T21:04:22Z Creation Date: 2011-06-06T02:04:22Z DNSSEC: unsigned Domain Name: W3SNOOP.COM Domain Status: clientDeleteProhibited http://www.icann.org/epp#clientDeleteProhibited Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited Domain Status: clientRenewProhibited http://www.icann.org/epp#clientRenewProhibited Domain Status: clientRenewProhibited https://icann.org/epp#clientRenewProhibited Domain Status: clientTransferProhibited http://www.icann.org/epp#clientTransferProhibited Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Domain Status: clientUpdateProhibited http://www.icann.org/epp#clientUpdateProhibited Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited Name Server: INDRI.EZOICNS.COM Name Server: SAOLA.EZOICNS.COM Registrant City: a7319ae5e6c95df5 Registrant Country: US Registrant Email: c9b5a1cf1d0c3764s@domainsbyproxy.com Registrant Fax Ext: 3432650ec337c945 Registrant Fax: 9fad764be0c7e95d Registrant Name: 80315b2e6ac1a801 Registrant Organization: b46a98a26fe2fd9f Registrant Phone Ext: 3432650ec337c945 Registrant Phone: d5f66d3a005b000d Registrant Postal Code: 052e5bd148f904f9 Registrant State/Province: 30bdd2917a604c83 Registrant Street: 037792fd5a6fe619 Registrant Street: d733533b6a6c0c21 Registrar Abuse Contact Email: abuse@godaddy.com Registrar Abuse Contact Phone: +1.4806242505 Registrar Abuse Contact Phone: 480-624-2505 Registrar IANA ID: 146 Registrar Registration Expiration Date: 2023-06-05T21:04:22Z Registrar URL: http://www.godaddy.com Registrar WHOIS Server: whois.godaddy.com Registrar: GoDaddy.com, LLC Registry Admin ID: Not Available From Registry Registry Domain ID: 1660071767_DOMAIN_COM-VRSN Registry Expiry Date: 2023-06-06T02:04:22Z Registry Registrant ID: Not Available From Registry Registry Tech ID: Not Available From Registry Tech City: Tempe Tech Country: US Tech Email: c9b5a1cf1d0c3764s@domainsbyproxy.com Tech Organization: Domains By Proxy, LLC Tech Postal Code: 85284 Tech State/Province: Arizona Updated Date: 2020-02-09T21:49:40Z Updated Date: 2020-02-10T04:49:41Z

VirusTotal Domain Summary	
VirusTotal Reputation	0
Tags	
Popularity Ranking	
Cisco Umbrella	
933689	

VirusTotal Analysis Summary	
Aggregate Result	harmless - 80 / 88

VirusTotal Analysis Stats	
Analysis Type	Number of Analysis
Confirmed Timeout	0
Failure	0
Harmless	80
Malicious	0
Suspicious	0
Timeout	0
Type Unsupported	0
Undetected	8
Total	**88**

View on VirusTotal

GUI Url: https://www.virustotal.com/gui/domain/in.w3snoop.com

Categories	
Engines	Category
Forcepoint ThreatSeeker	information technology
BitDefender	business

Community Votes

Total votes cast: 0

Incoming (2)

DNS Name	apitwitter.com.w3snoop.com
DNS Name	w3snoop.com

Domain

maltego.Domain

at.w3snoop.com

Weight	0
Domain Name	at.w3snoop.com
WHOIS Info	Admin City: Tempe Admin Country: US Admin Email: c9b5a1cf1d0c3764s@domainsbyproxy.com Admin Organization: Domains By Proxy, LLC Admin Postal Code: 85284 Admin State/Province: Arizona Creation Date: 2011-06-05T21:04:22Z Creation Date: 2011-06-06T02:04:22Z DNSSEC: unsigned Domain Name: W3SNOOP.COM Domain Status: clientDeleteProhibited http://www.icann.org/epp#clientDeleteProhibited Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited Domain Status: clientRenewProhibited http://www.icann.org/epp#clientRenewProhibited Domain Status: clientRenewProhibited https://icann.org/epp#clientRenewProhibited Domain Status: clientTransferProhibited http://www.icann.org/epp#clientTransferProhibited Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Domain Status: clientUpdateProhibited http://www.icann.org/epp#clientUpdateProhibited Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited Name Server: INDRI.EZOICNS.COM Name Server: SAOLA.EZOICNS.COM Registrant City: a7319ae5e6c95df5 Registrant Country: US Registrant Email: c9b5a1cf1d0c3764s@domainsbyproxy.com Registrant Fax Ext: 3432650ec337c945 Registrant Fax: 9fad764be0c7e95d Registrant Name: 80315b2e6ac1a801 Registrant Organization: b46a98a26fe2fd9f Registrant Phone Ext: 3432650ec337c945 Registrant Phone: d5f66d3a005b000d Registrant Postal Code: 052e5bd148f904f9 Registrant State/Province: 30bdd2917a604c83 Registrant Street: 037792fd5a6fe619 Registrant Street: d733533b6a6c0c21 Registrar Abuse Contact Email: abuse@godaddy.com Registrar Abuse Contact Phone: +1.4806242505 Registrar Abuse Contact Phone: 480-624-2505 Registrar IANA ID: 146 Registrar Registration Expiration Date: 2023-06-05T21:04:22Z Registrar URL: http://www.godaddy.com Registrar WHOIS Server: whois.godaddy.com Registrar: GoDaddy.com, LLC Registry Admin ID: Not Available From Registry Registry Domain ID: 1660071767_DOMAIN_COM-VRSN Registry Expiry Date: 2023-06-06T02:04:22Z Registry Registrant ID: Not Available From Registry Registry Tech ID: Not Available From Registry Tech City: Tempe Tech Country: US Tech Email: c9b5a1cf1d0c3764s@domainsbyproxy.com Tech Organization: Domains By Proxy, LLC Tech Postal Code: 85284 Tech State/Province: Arizona Updated Date: 2020-02-09T21:49:40Z Updated Date: 2020-02-10T04:49:41Z

VirusTotal Domain Summary	
VirusTotal Reputation	0
Tags	

VirusTotal Analysis Summary	
Aggregate Result	harmless - 80 / 88

VirusTotal Analysis Stats	
Analysis Type	Number of Analysis
Confirmed Timeout	0
Failure	0
Harmless	80
Malicious	0
Suspicious	0
Timeout	0
Type Unsupported	0
Undetected	8
Total	**88**

View on VirusTotal

GUI Url: https://www.virustotal.com/gui/domain/at.w3snoop.com

Community Votes

Total votes cast: 0

Incoming (2)

DNS Name	apitwitter.com.w3snoop.com
DNS Name	w3snoop.com

Domain

maltego.Domain

cc.w3snoop.com

Weight	0
Domain Name	cc.w3snoop.com
WHOIS Info	Admin City: Tempe Admin Country: US Admin Email: c9b5a1cf1d0c3764s@domainsbyproxy.com Admin Organization: Domains By Proxy, LLC Admin Postal Code: 85284 Admin State/Province: Arizona Creation Date: 2011-06-05T21:04:22Z Creation Date: 2011-06-06T02:04:22Z DNSSEC: unsigned Domain Name: W3SNOOP.COM Domain Status: clientDeleteProhibited http://www.icann.org/epp#clientDeleteProhibited Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited Domain Status: clientRenewProhibited http://www.icann.org/epp#clientRenewProhibited Domain Status: clientRenewProhibited https://icann.org/epp#clientRenewProhibited Domain Status: clientTransferProhibited http://www.icann.org/epp#clientTransferProhibited Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Domain Status: clientUpdateProhibited http://www.icann.org/epp#clientUpdateProhibited Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited Name Server: INDRI.EZOICNS.COM Name Server: SAOLA.EZOICNS.COM Registrant City: a7319ae5e6c95df5 Registrant Country: US Registrant Email: c9b5a1cf1d0c3764s@domainsbyproxy.com Registrant Fax Ext: 3432650ec337c945 Registrant Fax: 9fad764be0c7e95d Registrant Name: 80315b2e6ac1a801 Registrant Organization: b46a98a26fe2fd9f Registrant Phone Ext: 3432650ec337c945 Registrant Phone: d5f66d3a005b000d Registrant Postal Code: 052e5bd148f904f9 Registrant State/Province: 30bdd2917a604c83 Registrant Street: 037792fd5a6fe619 Registrant Street: d733533b6a6c0c21 Registrar Abuse Contact Email: abuse@godaddy.com Registrar Abuse Contact Phone: +1.4806242505 Registrar Abuse Contact Phone: 480-624-2505 Registrar IANA ID: 146 Registrar Registration Expiration Date: 2023-06-05T21:04:22Z Registrar URL: http://www.godaddy.com Registrar WHOIS Server: whois.godaddy.com Registrar: GoDaddy.com, LLC Registry Admin ID: Not Available From Registry Registry Domain ID: 1660071767_DOMAIN_COM-VRSN Registry Expiry Date: 2023-06-06T02:04:22Z Registry Registrant ID: Not Available From Registry Registry Tech ID: Not Available From Registry Tech City: Tempe Tech Country: US Tech Email: c9b5a1cf1d0c3764s@domainsbyproxy.com Tech Organization: Domains By Proxy, LLC Tech Postal Code: 85284 Tech State/Province: Arizona Updated Date: 2020-02-09T21:49:40Z Updated Date: 2020-02-10T04:49:41Z

VirusTotal Domain Summary

VirusTotal Reputation	0
Tags	

VirusTotal Analysis Summary	
Aggregate Result	harmless - 80 / 88

VirusTotal Analysis Stats	
Analysis Type	Number of Analysis
Confirmed Timeout	0
Failure	0
Harmless	80
Malicious	0
Suspicious	0
Timeout	0
Type Unsupported	0
Undetected	8
Total	**88**

View on VirusTotal

GUI Url: https://www.virustotal.com/gui/domain/cc.w3snoop.com

Categories	
Engines	Category
Forcepoint ThreatSeeker	information technology
BitDefender	business

Community Votes

Total votes cast: 0

Incoming (2)

DNS Name	apitwitter.com.w3snoop.com
DNS Name	w3snoop.com

Domain

maltego.Domain

cz.w3snoop.com

Weight	0
Domain Name	cz.w3snoop.com
WHOIS Info	Admin City: Tempe Admin Country: US Admin Email: c9b5a1cf1d0c3764s@domainsbyproxy.com Admin Organization: Domains By Proxy, LLC Admin Postal Code: 85284 Admin State/Province: Arizona Creation Date: 2011-06-05T21:04:22Z Creation Date: 2011-06-06T02:04:22Z DNSSEC: unsigned Domain Name: W3SNOOP.COM Domain Status: clientDeleteProhibited http://www.icann.org/epp#clientDeleteProhibited Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited Domain Status: clientRenewProhibited http://www.icann.org/epp#clientRenewProhibited Domain Status: clientRenewProhibited https://icann.org/epp#clientRenewProhibited Domain Status: clientTransferProhibited http://www.icann.org/epp#clientTransferProhibited Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Domain Status: clientUpdateProhibited http://www.icann.org/epp#clientUpdateProhibited Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited Name Server: INDRI.EZOICNS.COM Name Server: SAOLA.EZOICNS.COM Registrant City: a7319ae5e6c95df5 Registrant Country: US Registrant Email: c9b5a1cf1d0c3764s@domainsbyproxy.com Registrant Fax Ext: 3432650ec337c945 Registrant Fax: 9fad764be0c7e95d Registrant Name: 80315b2e6ac1a801 Registrant Organization: b46a98a26fe2fd9f Registrant Phone Ext: 3432650ec337c945 Registrant Phone: d5f66d3a005b000d Registrant Postal Code: 052e5bd148f904f9 Registrant State/Province: 30bdd2917a604c83 Registrant Street: 037792fd5a6fe619 Registrant Street: d733533b6a6c0c21 Registrar Abuse Contact Email: abuse@godaddy.com Registrar Abuse Contact Phone: +1.4806242505 Registrar Abuse Contact Phone: 480-624-2505 Registrar IANA ID: 146 Registrar Registration Expiration Date: 2023-06-05T21:04:22Z Registrar URL: http://www.godaddy.com Registrar WHOIS Server: whois.godaddy.com Registrar: GoDaddy.com, LLC Registry Admin ID: Not Available From Registry Registry Domain ID: 1660071767_DOMAIN_COM-VRSN Registry Expiry Date: 2023-06-06T02:04:22Z Registry Registrant ID: Not Available From Registry Registry Tech ID: Not Available From Registry Tech City: Tempe Tech Country: US Tech Email: c9b5a1cf1d0c3764s@domainsbyproxy.com Tech Organization: Domains By Proxy, LLC Tech Postal Code: 85284 Tech State/Province: Arizona Updated Date: 2020-02-09T21:49:40Z Updated Date: 2020-02-10T04:49:41Z

VirusTotal Domain Summary

VirusTotal Reputation	0
Tags	

VirusTotal Analysis Summary	
Aggregate Result	harmless - 80 / 88

VirusTotal Analysis Stats	
Analysis Type	Number of Analysis
Confirmed Timeout	0
Failure	0
Harmless	80
Malicious	0
Suspicious	0
Timeout	0
Type Unsupported	0
Undetected	8
Total	**88**

View on VirusTotal

GUI Url: https://www.virustotal.com/gui/domain/cz.w3snoop.com

Community Votes

Total votes cast: 0

Incoming (2)

DNS Name	apitwitter.com.w3snoop.com
DNS Name	w3snoop.com

Domain

maltego.Domain

co.w3snoop.com

Weight	0
Domain Name	co.w3snoop.com
WHOIS Info	Admin City: Tempe Admin Country: US Admin Email: c9b5a1cf1d0c3764s@domainsbyproxy.com Admin Organization: Domains By Proxy, LLC Admin Postal Code: 85284 Admin State/Province: Arizona Creation Date: 2011-06-05T21:04:22Z Creation Date: 2011-06-06T02:04:22Z DNSSEC: unsigned Domain Name: W3SNOOP.COM Domain Status: clientDeleteProhibited http://www.icann.org/epp#clientDeleteProhibited Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited Domain Status: clientRenewProhibited http://www.icann.org/epp#clientRenewProhibited Domain Status: clientRenewProhibited https://icann.org/epp#clientRenewProhibited Domain Status: clientTransferProhibited http://www.icann.org/epp#clientTransferProhibited Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Domain Status: clientUpdateProhibited http://www.icann.org/epp#clientUpdateProhibited Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited Name Server: INDRI.EZOICNS.COM Name Server: SAOLA.EZOICNS.COM Registrant City: a7319ae5e6c95df5 Registrant Country: US Registrant Email: c9b5a1cf1d0c3764s@domainsbyproxy.com Registrant Fax Ext: 3432650ec337c945 Registrant Fax: 9fad764be0c7e95d Registrant Name: 80315b2e6ac1a801 Registrant Organization: b46a98a26fe2fd9f Registrant Phone Ext: 3432650ec337c945 Registrant Phone: d5f66d3a005b000d Registrant Postal Code: 052e5bd148f904f9 Registrant State/Province: 30bdd2917a604c83 Registrant Street: 037792fd5a6fe619 Registrant Street: d733533b6a6c0c21 Registrar Abuse Contact Email: abuse@godaddy.com Registrar Abuse Contact Phone: +1.4806242505 Registrar Abuse Contact Phone: 480-624-2505 Registrar IANA ID: 146 Registrar Registration Expiration Date: 2023-06-05T21:04:22Z Registrar URL: http://www.godaddy.com Registrar WHOIS Server: whois.godaddy.com Registrar: GoDaddy.com, LLC Registry Admin ID: Not Available From Registry Registry Domain ID: 1660071767_DOMAIN_COM-VRSN Registry Expiry Date: 2023-06-06T02:04:22Z Registry Registrant ID: Not Available From Registry Registry Tech ID: Not Available From Registry Tech City: Tempe Tech Country: US Tech Email: c9b5a1cf1d0c3764s@domainsbyproxy.com Tech Organization: Domains By Proxy, LLC Tech Postal Code: 85284 Tech State/Province: Arizona Updated Date: 2020-02-09T21:49:40Z Updated Date: 2020-02-10T04:49:41Z

VirusTotal Domain Summary	
VirusTotal Reputation	0
Tags	
Popularity Ranking	
Cisco Umbrella	
998524	

VirusTotal Analysis Summary	
Aggregate Result	harmless - 80 / 88

VirusTotal Analysis Stats	
Analysis Type	Number of Analysis
Confirmed Timeout	0
Failure	0
Harmless	80
Malicious	0
Suspicious	0
Timeout	0
Type Unsupported	0
Undetected	8
Total	**88**

View on VirusTotal

GUI Url: https://www.virustotal.com/gui/domain/co.w3snoop.com

Categories	
Engines	Category
Forcepoint ThreatSeeker	information technology
BitDefender	business

Community Votes

Total votes cast: 0

Incoming (2)		
	DNS Name	apitwitter.com.w3snoop.com
	DNS Name	w3snoop.com

Domain

maltego.Domain

fi.w3snoop.com

Weight	0
Domain Name	fi.w3snoop.com
WHOIS Info	Admin City: Tempe Admin Country: US Admin Email: c9b5a1cf1d0c3764s@domainsbyproxy.com Admin Organization: Domains By Proxy, LLC Admin Postal Code: 85284 Admin State/Province: Arizona Creation Date: 2011-06-05T21:04:22Z Creation Date: 2011-06-06T02:04:22Z DNSSEC: unsigned Domain Name: W3SNOOP.COM Domain Status: clientDeleteProhibited http://www.icann.org/epp#clientDeleteProhibited Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited Domain Status: clientRenewProhibited http://www.icann.org/epp#clientRenewProhibited Domain Status: clientRenewProhibited https://icann.org/epp#clientRenewProhibited Domain Status: clientTransferProhibited http://www.icann.org/epp#clientTransferProhibited Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Domain Status: clientUpdateProhibited http://www.icann.org/epp#clientUpdateProhibited Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited Name Server: INDRI.EZOICNS.COM Name Server: SAOLA.EZOICNS.COM Registrant City: a7319ae5e6c95df5 Registrant Country: US Registrant Email: c9b5a1cf1d0c3764s@domainsbyproxy.com Registrant Fax Ext: 3432650ec337c945 Registrant Fax: 9fad764be0c7e95d Registrant Name: 80315b2e6ac1a801 Registrant Organization: b46a98a26fe2fd9f Registrant Phone Ext: 3432650ec337c945 Registrant Phone: d5f66d3a005b000d Registrant Postal Code: 052e5bd148f904f9 Registrant State/Province: 30bdd2917a604c83 Registrant Street: 037792fd5a6fe619 Registrant Street: d733533b6a6c0c21 Registrar Abuse Contact Email: abuse@godaddy.com Registrar Abuse Contact Phone: +1.4806242505 Registrar Abuse Contact Phone: 480-624-2505 Registrar IANA ID: 146 Registrar Registration Expiration Date: 2023-06-05T21:04:22Z Registrar URL: http://www.godaddy.com Registrar WHOIS Server: whois.godaddy.com Registrar: GoDaddy.com, LLC Registry Admin ID: Not Available From Registry Registry Domain ID: 1660071767_DOMAIN_COM-VRSN Registry Expiry Date: 2023-06-06T02:04:22Z Registry Registrant ID: Not Available From Registry Registry Tech ID: Not Available From Registry Tech City: Tempe Tech Country: US Tech Email: c9b5a1cf1d0c3764s@domainsbyproxy.com Tech Organization: Domains By Proxy, LLC Tech Postal Code: 85284 Tech State/Province: Arizona Updated Date: 2020-02-09T21:49:40Z Updated Date: 2020-02-10T04:49:41Z

VirusTotal Domain Summary	
VirusTotal Reputation	0
Tags	

VirusTotal Analysis Summary	
Aggregate Result	harmless - 80 / 88

VirusTotal Analysis Stats	
Analysis Type	Number of Analysis
Confirmed Timeout	0
Failure	0
Harmless	80
Malicious	0
Suspicious	0
Timeout	0
Type Unsupported	0
Undetected	8
Total	**88**

View on VirusTotal

GUI Url: https://www.virustotal.com/gui/domain/fi.w3snoop.com

Community Votes

Total votes cast: 0

Incoming (2)

DNS Name	apitwitter.com.w3snoop.com
DNS Name	w3snoop.com

Phone Number

maltego.PhoneNumber

+1 480 624 2598

Weight	100
Phone Number	+1 480 624 2598
Country Code	
City Code	
Area Code	
Last Digits	

Incoming (2)	
Domain	w3snoop.com
Domain	w3snoop.com

Phone Number

maltego.PhoneNumber

+1 480 624 2505

Weight	100
Phone Number	+1 480 624 2505
Country Code	
City Code	
Area Code	
Last Digits	

Incoming (2)	
Domain	w3snoop.com
Domain	w3snoop.com

SSL Certificate

maltego.X509Certificate

*.bizland.com

Weight	0
Subject	*.bizland.com
Issuer	Sectigo RSA Domain Validation Secure Server CA
Subject DN	
Issuer DN	
SKI	ca6a2ac69b3a568b9a1aaf8b241836edfa97c722
AKI	
Serial	783b186c2d4bb32c07a71cc233683843
SAN	[*.bizland.com, bizland.com]
Usage	
Issuance ID	
Valid From	Wed Jun 02 00:00:00 GMT 2021
Valid Until	Sun Jul 03 00:00:00 GMT 2022
Country	
Organization	

Incoming (2)	
DNS Name	apitwitter.com.evil.com
DNS Name	apitwitter.com.evil.com

Domain

maltego.Domain

com.evil.co

Weight	0
Domain Name	com.evil.co
WHOIS Info	Admin City: REDACTED FOR PRIVACY Admin Country: REDACTED FOR PRIVACY Admin Organization: REDACTED FOR PRIVACY Admin Postal Code: REDACTED FOR PRIVACY Admin State/Province: REDACTED FOR PRIVACY Creation Date: 2019-10-05T17:00:14Z DNSSEC: unsigned Domain Name: evil.co Domain Status: clientDeleteProhibited http://www.icann.org/epp#clientDeleteProhibited Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited Domain Status: clientRenewProhibited http://www.icann.org/epp#clientRenewProhibited Domain Status: clientRenewProhibited https://icann.org/epp#clientRenewProhibited Domain Status: clientTransferProhibited http://www.icann.org/epp#clientTransferProhibited Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Domain Status: clientUpdateProhibited http://www.icann.org/epp#clientUpdateProhibited Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited Name Server: NS1.UNIREGISTRYMARKET.LINK Name Server: NS2.UNIREGISTRYMARKET.LINK Name Server: ns1.uniregistrymarket.link Name Server: ns2.uniregistrymarket.link Registrant City: 1f8f4166599d23ee Registrant Country: US Registrant Email: 44f8172ee385b60bs@ Registrant Email: f651612a2f356ad3s@ Registrant Fax Ext: 1f8f4166599d23ee Registrant Fax: 1f8f4166599d23ee Registrant Name: 1f8f4166599d23ee Registrant Organization: 3432650ec337c945 Registrant Phone Ext: 1f8f4166599d23ee Registrant Phone: 1f8f4166599d23ee Registrant Postal Code: 1f8f4166599d23ee Registrant State/Province: c5117919ef41a795 Registrant Street: 1f8f4166599d23ee Registrar Abuse Contact Email: abuse@godaddy.com Registrar Abuse Contact Phone: +1.4806242505 Registrar IANA ID: 146 Registrar Registration Expiration Date: 2022-10-05T17:00:14Z Registrar URL: http://www.godaddy.com Registrar URL: whois.godaddy.com Registrar WHOIS Server: whois.godaddy.com Registrar: GoDaddy.com, LLC Registry Admin ID: REDACTED FOR PRIVACY Registry Domain ID: D8A750721BA904C4A90CFDA260DBE314E-NSR Registry Expiry Date: 2022-10-05T17:00:14Z Registry Registrant ID: REDACTED FOR PRIVACY Registry Tech ID: REDACTED FOR PRIVACY Tech City: REDACTED FOR PRIVACY Tech Country: REDACTED FOR PRIVACY Tech Organization: REDACTED FOR PRIVACY Tech Postal Code: REDACTED FOR PRIVACY Tech State/Province: REDACTED FOR PRIVACY Updated Date: 2021-06-17T12:14:42Z Updated Date: 2021-06-22T19:14:40Z

VirusTotal Domain Summary

VirusTotal Reputation	0
Tags	

VirusTotal Analysis Summary

Aggregate Result	harmless - 86 / 86

VirusTotal Analysis Stats

Analysis Type	Number of Analysis
Confirmed Timeout	0
Failure	0
Harmless	86
Malicious	0
Suspicious	0
Timeout	0
Type Unsupported	0
Undetected	0
Total	**86**

View on VirusTotal

GUI Url: https://www.virustotal.com/gui/domain/com.evil.co

Community Votes

Total votes cast: 0

Incoming (2)

DNS Name	apitwitter.com.evil.co
DNS Name	evil.co

A Record

maltego.ARecord

w3snoop.com

Weight	0
IPv4 Address	35.175.60.16
Time to Live (TTL)	0
DNS Name	w3snoop.com
Time To Live	60
Type	A
Shodan Last Update	2019-11-17T12:23:02.308756+00:00

Incoming (2)

DNS Name	w3snoop.com
DNS Name	w3snoop.com

NS Record

maltego.NSRecord

saola.ezoicns.com

Weight	0
NS Record	saola.ezoicns.com
Time To Live	21600
Type	NS
Shodan Last Update	2021-10-02T09:07:32.588446+00:00

Incoming (2)

DNS Name	w3snoop.com
DNS Name	w3snoop.com

Email Address

maltego.EmailAddress

eig-abuse@endurance.com

Weight	100
Email Address	eig-abuse@endurance.com

Incoming (2)

IPv4 Address	66.96.146.129
IPv4 Address	66.96.146.129

IPv4 Address

maltego.IPv4Address

192.220.74.179

Weight	0
IP Address	192.220.74.179
Internal	false
Date Resolved	2013-10-02T00:00Z
Resolver	VirusTotal

Incoming (2)

DNS Name	evil.com
DNS Name	www.evil.com

IPv4 Address

maltego.IPv4Address

3.127.76.126

Weight	0
IP Address	3.127.76.126
Internal	false
Date Resolved	2020-09-06T01:24:49Z
Resolver	VirusTotal

Incoming (2)

DNS Name	apitwitter.com.w3snoop.com
DNS Name	w3snoop.com

Snapshot

maltego.wayback.Snapshot

2000 Mar 03: http://www.evil.com:80/

Weight	2193218
Timestamp	20000303013812
Description	2000 Mar 03: http://www.evil.com:80/
Web Archive URL	https://web.archive.org/web/20000303013812/http://www.evil.com:80/
Original URL	http://www.evil.com:80/
DateTime	03 Mar 2000 01:38:12 +0000
HTTP Status	200
Short title	
URL	https://web.archive.org/web/20000303013812if_/http://www.evil.com:80/
Title	https://web.archive.org/web/20000303013812if_/http://www.evil.com:80/

Entity Data

Archived Page URL	https://web.archive.org/web/20000303013812if_/http://www.evil.com:80/
Web Archive URL	https://web.archive.org/web/20000303013812/http://www.evil.com:80/
Snapshot DateTime	03 Mar 2000 01:38:12 +0000
Original URL	http://www.evil.com:80/

Incoming (2)

Domain	evil.com
Domain	evil.com

Snapshot

maltego.wayback.Snapshot

2000 Mar 04: http://www.evil.com:80/

Weight	2194932
Timestamp	20000304061215
Description	2000 Mar 04: http://www.evil.com:80/
Web Archive URL	https://web.archive.org/web/20000304061215/http://www.evil.com:80/
Original URL	http://www.evil.com:80/
DateTime	04 Mar 2000 06:12:15 +0000
HTTP Status	200
Short title	
URL	https://web.archive.org/web/20000304061215if_/http://www.evil.com:80/
Title	https://web.archive.org/web/20000304061215if_/http://www.evil.com:80/

Entity Data	
Archived Page URL	https://web.archive.org/web/20000304061215if_/http://www.evil.com:80/
Web Archive URL	https://web.archive.org/web/20000304061215/http://www.evil.com:80/
Snapshot DateTime	04 Mar 2000 06:12:15 +0000
Original URL	http://www.evil.com:80/

Incoming (2)		
	Domain	evil.com
	Domain	evil.com

Snapshot

maltego.wayback.Snapshot

2000 Feb 29: http://www.evil.com:80/

Weight	2189697
Timestamp	20000229145706
Description	2000 Feb 29: http://www.evil.com:80/
Web Archive URL	https://web.archive.org/web/20000229145706/http://www.evil.com:80/
Original URL	http://www.evil.com:80/
DateTime	29 Feb 2000 14:57:06 +0000
HTTP Status	200
Short title	
URL	https://web.archive.org/web/20000229145706if_/http://www.evil.com:80/
Title	https://web.archive.org/web/20000229145706if_/http://www.evil.com:80/

Entity Data	
Archived Page URL	https://web.archive.org/web/20000229145706if_/http://www.evil.com:80/
Web Archive URL	https://web.archive.org/web/20000229145706/http://www.evil.com:80/
Snapshot DateTime	29 Feb 2000 14:57:06 +0000
Original URL	http://www.evil.com:80/

Incoming (2)		
	Domain	evil.com
	Domain	evil.com

DNS Name

maltego.DNSName

ns1.verio.com

Weight	0
DNS Name	ns1.verio.com
Record Last Seen	2021-09-29T05:55:26.569810+00:00
DNS Record Type	SOA

Incoming (2)

DNS Name	evil.com
Website	evil.com

IPv4 Address

maltego.IPv4Address

45.56.91.58

Weight	0
IP Address	45.56.91.58
Internal	false

Incoming (2)

DNS Name	evil.com
Website	evil.com

A Record

maltego.ARecord

apitwitter.w3snoop.com

Weight	0
IPv4 Address	50.16.49.81
Time to Live (TTL)	0
DNS Name	apitwitter.w3snoop.com
Time To Live	60
Type	A

Incoming (1)

DNS Name	apitwitter.w3snoop.com

Domain

maltego.Domain

apitwitter.com.evil.com

Weight	0
Domain Name	apitwitter.com.evil.com
WHOIS Info	Creation Date: 1995-04-10T04:00:00Z DNSSEC: unsigned Domain Name: EVIL.COM Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited Name Server: NS1.VERIO.COM Name Server: NS2.VERIO.COM Registrar Abuse Contact Email: abuse@web.com Registrar Abuse Contact Phone: +1.8003337680 Registrar IANA ID: 2 Registrar URL: http://networksolutions.com Registrar WHOIS Server: whois.networksolutions.com Registrar: Network Solutions, LLC Registry Domain ID: 1040763_DOMAIN_COM-VRSN Registry Expiry Date: 2023-04-11T04:00:00Z Updated Date: 2019-12-17T16:17:59Z

VirusTotal Domain Summary

VirusTotal Reputation	0
Tags	

VirusTotal Analysis Summary

Aggregate Result	harmless - 86 / 86

VirusTotal Analysis Stats

Analysis Type	Number of Analysis
Confirmed Timeout	0
Failure	0
Harmless	86
Malicious	0
Suspicious	0
Timeout	0
Type Unsupported	0
Undetected	0
Total	**86**

View on VirusTotal

GUI Url: https://www.virustotal.com/gui/domain/apitwitter.com.evil.com

Community Votes

Total votes cast: 0

Incoming (1)

DNS Name	apitwitter.com.evil.com

Domain

maltego.Domain

com.w3snoop.com

Weight	0
Domain Name	com.w3snoop.com
WHOIS Info	Admin City: Tempe Admin Country: US Admin Email: c9b5a1cf1d0c3764s@domainsbyproxy.com Admin Organization: Domains By Proxy, LLC Admin Postal Code: 85284 Admin State/Province: Arizona Creation Date: 2011-06-05T21:04:22Z Creation Date: 2011-06-06T02:04:22Z DNSSEC: unsigned Domain Name: W3SNOOP.COM Domain Status: clientDeleteProhibited http://www.icann.org/epp#clientDeleteProhibited Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited Domain Status: clientRenewProhibited http://www.icann.org/epp#clientRenewProhibited Domain Status: clientRenewProhibited https://icann.org/epp#clientRenewProhibited Domain Status: clientTransferProhibited http://www.icann.org/epp#clientTransferProhibited Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Domain Status: clientUpdateProhibited http://www.icann.org/epp#clientUpdateProhibited Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited Name Server: INDRI.EZOICNS.COM Name Server: SAOLA.EZOICNS.COM Registrant City: a7319ae5e6c95df5 Registrant Country: US Registrant Email: c9b5a1cf1d0c3764s@domainsbyproxy.com Registrant Fax Ext: 3432650ec337c945 Registrant Fax: 9fad764be0c7e95d Registrant Name: 80315b2e6ac1a801 Registrant Organization: b46a98a26fe2fd9f Registrant Phone Ext: 3432650ec337c945 Registrant Phone: d5f66d3a005b000d Registrant Postal Code: 052e5bd148f904f9 Registrant State/Province: 30bdd2917a604c83 Registrant Street: 037792fd5a6fe619 Registrant Street: d733533b6a6c0c21 Registrar Abuse Contact Email: abuse@godaddy.com Registrar Abuse Contact Phone: +1.4806242505 Registrar Abuse Contact Phone: 480-624-2505 Registrar IANA ID: 146 Registrar Registration Expiration Date: 2023-06-05T21:04:22Z Registrar URL: http://www.godaddy.com Registrar WHOIS Server: whois.godaddy.com Registrar: GoDaddy.com, LLC Registry Admin ID: Not Available From Registry Registry Domain ID: 1660071767_DOMAIN_COM-VRSN Registry Expiry Date: 2023-06-06T02:04:22Z Registry Registrant ID: Not Available From Registry Registry Tech ID: Not Available From Registry Tech City: Tempe Tech Country: US Tech Email: c9b5a1cf1d0c3764s@domainsbyproxy.com Tech Organization: Domains By Proxy, LLC Tech Postal Code: 85284 Tech State/Province: Arizona Updated Date: 2020-02-09T21:49:40Z Updated Date: 2020-02-10T04:49:41Z

VirusTotal Domain Summary	
VirusTotal Reputation	0
Tags	
Popularity Ranking	
Cisco Umbrella	
342079	

VirusTotal Analysis Summary	
Aggregate Result	harmless - 80 / 88

VirusTotal Analysis Stats	
Analysis Type	Number of Analysis
Confirmed Timeout	0
Failure	0
Harmless	80
Malicious	0
Suspicious	0
Timeout	0
Type Unsupported	0
Undetected	8
Total	**88**

View on VirusTotal

GUI Url: https://www.virustotal.com/gui/domain/com.w3snoop.com

Categories

Engines	Category
Forcepoint ThreatSeeker	information technology
BitDefender	business

Community Votes

Total votes cast: 0

Incoming (1)

	DNS Name	apitwitter.com.w3snoop.com

IPv4 Address

maltego.IPv4Address

50.17.255.255

Weight	43
IP Address	50.17.255.255
Internal	false

Info

Relevance:	0.437367
Count:	1

Incoming (1)

IPv4 Address	50.16.49.81

IPv4 Address

maltego.IPv4Address

50.19.255.255

Weight	43
IP Address	50.19.255.255
Internal	false

Info

Relevance:	0.437367
Count:	1

Incoming (1)

IPv4 Address	50.16.49.81

A Record

maltego.ARecord

apitwitter.evil.co

Weight	0
IPv4 Address	52.128.23.153
Time to Live (TTL)	0
DNS Name	apitwitter.evil.co
Time To Live	3600
Type	A

Incoming (1)

DNS Name	apitwitter.evil.co

IPv4 Address

maltego.IPv4Address

50.16.0.0

Weight	43
IP Address	50.16.0.0
Internal	false

Info

Relevance:	0.437367
Count:	2

Incoming (1)

IPv4 Address	50.16.49.81

Email Address

maltego.EmailAddress

devilteachme@evil.com

Weight	0
Email Address	devilteachme@evil.com

Info

View PGP Public Keys

1. bed745bffe9d4930

Signatures

SN	Key ID	Created	Expiry	View URL
1	bed745bffe9d4930	2015-03-19T14:06:24Z	2124-06-11T19:30:40Z	[selfsig]

Incoming (1)

Domain	evil.com

Email Address

maltego.EmailAddress

slaytanic@evil.com

Weight	0
Email Address	slaytanic@evil.com

Info

View PGP Public Keys

1. e1d2d93ec60ea033

Signatures

SN	Key ID	Created	Expiry	View URL
1	e1d2d93ec60ea033	2016-06-29T15:16:56Z		[selfsig]

Incoming (1)

Domain	evil.com

Domain

maltego.Domain

brandsight-whois.com

Weight	100
Domain Name	brandsight-whois.com
WHOIS Info	

Incoming (1)

NS Record	ns2.uniregistrymarket.link

A Record

maltego.ARecord

wildcard-in-use.apitwitter.evil.co

Weight	0
IPv4 Address	52.128.23.153
Time to Live (TTL)	0
DNS Name	wildcard-in-use.apitwitter.evil.co
Time To Live	3600
Type	A

Incoming (1)

DNS Name	wildcard-in-use.apitwitter.evil.co

Email Address

maltego.EmailAddress

devil@evil.com

Weight	0
Email Address	devil@evil.com

Info

View PGP Public Keys

1. a82acf8c1ac73b64

Signatures

SN	Key ID	Created	Expiry	View URL
1	a82acf8c1ac73b64	2015-03-27T19:44Z		[selfsig]

Incoming (1)

Domain	evil.com

Domain

maltego.Domain

com.evil.com

Weight	0
Domain Name	com.evil.com
WHOIS Info	Creation Date: 1995-04-10T04:00:00Z DNSSEC: unsigned Domain Name: EVIL.COM Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited Name Server: NS1.VERIO.COM Name Server: NS2.VERIO.COM Registrar Abuse Contact Email: abuse@web.com Registrar Abuse Contact Phone: +1.8003337680 Registrar IANA ID: 2 Registrar URL: http://networksolutions.com Registrar WHOIS Server: whois.networksolutions.com Registrar: Network Solutions, LLC Registry Domain ID: 1040763_DOMAIN_COM-VRSN Registry Expiry Date: 2023-04-11T04:00:00Z Updated Date: 2019-12-17T16:17:59Z

VirusTotal Domain Summary

VirusTotal Reputation	0
Tags	
Popularity Ranking	
Cisco Umbrella	
961934	

VirusTotal Analysis Summary

Aggregate Result	harmless - 86 / 86

VirusTotal Analysis Stats

Analysis Type	Number of Analysis
Confirmed Timeout	0
Failure	0
Harmless	86
Malicious	0
Suspicious	0
Timeout	0
Type Unsupported	0
Undetected	0
Total	**86**

View on VirusTotal

GUI Url: https://www.virustotal.com/gui/domain/com.evil.com

Community Votes

Total votes cast: 0

Incoming (1)

DNS Name	apitwitter.com.evil.com

Email Address

maltego.EmailAddress

crart@evil.com

Weight	0
Email Address	crart@evil.com

Info

View PGP Public Keys

1. 1c96279827864f22

Signatures

SN	Key ID	Created	Expiry	View URL
1	1c96279827864f22	2017-07-01T22:06:26Z		[selfsig]

Incoming (1)

Domain	evil.com

VirusTotal Comment

maltego.virustotal.Comment

Evil.com is reco...

Weight	0
Short Text	Evil.com is reco...
Date	2021-03-31T20:31:14Z
Comment Id	d-evil.com-630740db
Tags	phishing,malicious,unsafe,systemthreat,c26y,t1m
Comment Votes	Abuse:0, Negative:0, Positive:0
Text	Evil.com is recognized is a phishing site. #Phishing #Malicious #Unsafe #0/82 Threat #SystemThreat #C26Y #T1M Evil.com is recognized as a phishing site.

Comment Text

Evil.com is recognized is a phishing site.
#Phishing
#Malicious
#Unsafe
#0/82 Threat
#SystemThreat
#C26Y
#T1M
Evil.com is recognized as a phishing site.

Incoming (1)

DNS Name	evil.com

VirusTotal Comment

maltego.virustotal.Comment

I Mean Makes sen...

Weight	0
Short Text	I Mean Makes sen...
Date	2021-02-18T14:24:49Z
Comment Id	d-evil.com-01fd09e0
Tags	phising,malware,notsafe,bruh
Comment Votes	Abuse:0, Negative:0, Positive:0
Text	I Mean Makes sence evil is evil... Also phising site i went there and it spreeds mis infomation #phising #malware #notsafe #bruh

Comment Text

I Mean Makes sence evil is evil…
Also phising site i went there and it spreeds mis infomation
#phising
#malware
#notsafe
#bruh

Incoming (1)

DNS Name	evil.com

A Record

maltego.ARecord

apitwitter.evil.com

Weight	0
IPv4 Address	66.96.146.129
Time to Live (TTL)	0
DNS Name	apitwitter.evil.com
Time To Live	3600
Type	A

Incoming (1)

DNS Name	apitwitter.evil.com

Location

maltego.Location

FL

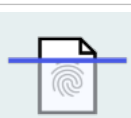
Weight	30
Name	FL
Country	
City	
Street Address	
Area	
Area Code	
Country Code	
Longitude	0.0
Latitude	0.0

Info

Relevance:	0.30889
Count:	3

Incoming (1)

Domain	evil.com



VirusTotal File

maltego.virustotal.File

Zalando-Rechnung-234541.pdf .exe

Weight	0
MeaningfulName	Zalando-Rechnung-234541.pdf .exe
File Id	9bbb4c4605e965e93b56992fd70296bf101ff2ad37e6f243b536bf9acec0718a
Names	Zalando-Rechnung-234541.pdf .exe
File Type	PEEXE
File Type Description	Win32 EXE
MD5	406650bfca5983cc1914e04efebc3dbd
SHA-1	8c06340d5c03560422851d4f37b17a51ac1b0324
SHA-256	9bbb4c4605e965e93b56992fd70296bf101ff2ad37e6f243b536bf9acec0718a
Vhash	026056655d15756210b02002300a46z161d013zf2za0030e039z
Authentihash	c888b3e68014c08430c63360445c2041743143260fbe045099d271341170ba3d
SSDEEP	49152:cw80cTsjkWacmwkbOLpC/Da0yUhfdBYHZ/lbZTTg7lffDfbQqv1+YE64Z/:98sjkz4pAaQVd2RlZ3gNDf8I1O6E
Magic	PE32 executable for MS Windows (GUI) Intel 80386 32-bit
File Size	2832896
Tags	peexe
Capability Tags	
Downloadable	null
Creation Date	2016-01-21T20:55:54Z
First Submission Date	2016-02-04T07:48:49Z
Last Submission Date	2016-02-04T07:48:49Z
Last Analysis Date	2016-02-04T07:52:21Z
Total Votes - Harmless	0
Total Votes - Malicious	0
Submissions	1
Reputation	0

View on VirusTotal

GUI Url:
https://www.virustotal.com/gui/file/9bbb4c4605e965e93b56992fd70296bf101ff2ad37e6f243b536bf9acec0718a

File Summary

Names	Zalando-Rechnung-234541.pdf .exe
File Type	peexe
File Type Description	Win32 EXE
Tags	peexe
Times Submitted	1

TrID - file type identification tool	
File Type	Probability %
Win32 Dynamic Link Library (generic)	43.5
Win32 Executable (generic)	29.8
Generic Win/DOS Executable	13.2
DOS Executable Generic	13.2

VirusTotal Analysis Summary	
Aggregate Result	undetected - 43 / 53

VirusTotal Analysis Stats	
Analysis Type	Number of Analysis
Confirmed Timeout	0
Failure	0
Harmless	0
Malicious	10
Suspicious	0
Timeout	0
Type Unsupported	0
Undetected	43
Total	**53**

Community Votes

Total votes cast: 0

Incoming (1)

DNS	DNS Name	www.evil.com

VirusTotal File

maltego.virustotal.File

appke.exe

Weight	0
MeaningfulName	appke.exe
File Id	ba7b6649cc794a43eecfae56b28ddbdec793da0d8a44886fc046fa166f35c9de
Names	appke.exe
File Type	PEEXE
File Type Description	Win32 EXE
MD5	5e0a083a0ac34c17d2a5547232ec5061
SHA-1	b6acef56fdb2c72ce284b88b7d1669c9d1eb4bb7
SHA-256	ba7b6649cc794a43eecfae56b28ddbdec793da0d8a44886fc046fa166f35c9de
Vhash	055076551d155d15151128z5e36z37z2bzb6z2
Authentihash	cb3ac9c4ed286e0007a665efde46153856b181690fb2c8b9f88124d776f8d9d6
SSDEEP	6144:nl32b/5YA7u/d4ry4MPxjTRwouajokogMyxCcTQZ2fsvk:8dG6MPxjDIyxtTQk
Magic	PE32+ executable for MS Windows (console) Mono/.Net assembly
File Size	585216
Tags	64bits, peexe, assembly
Capability Tags	
Downloadable	null
Creation Date	2019-08-24T20:28:42Z
First Submission Date	2019-09-25T15:36:05Z
Last Submission Date	2019-09-25T15:36:05Z
Last Analysis Date	2019-10-10T23:22:57Z
Total Votes - Harmless	0
Total Votes - Malicious	0
Submissions	1
Reputation	0

View on VirusTotal

GUI Url:
https://www.virustotal.com/gui/file/ba7b6649cc794a43eecfae56b28ddbdec793da0d8a44886fc046fa166f35c9de

File Summary

Names	appke.exe
File Type	peexe
File Type Description	Win32 EXE
Tags	64bits, peexe, assembly
Times Submitted	1

TrID - file type identification tool	
File Type	Probability %
InstallShield setup	46.1
Win64 Executable (generic)	29.6
Microsoft Visual C++ compiled executable (generic)	17.7
OS/2 Executable (generic)	2.1
Generic Win/DOS Executable	2.1

VirusTotal Analysis Summary	
Aggregate Result	undetected - 69 / 71

VirusTotal Analysis Stats	
Analysis Type	Number of Analysis
Confirmed Timeout	0
Failure	0
Harmless	0
Malicious	0
Suspicious	0
Timeout	0
Type Unsupported	2
Undetected	69
Total	**71**

Community Votes

Total votes cast: 0

Incoming (1)

DNS Name	www.evil.com

Person

maltego.Person

NETWORK SOLUTIONS, LLC.

Weight	100
Full Name	NETWORK SOLUTIONS, LLC.
First Names	
Surname	

Incoming (1)

Domain	evil.com

VirusTotal File

maltego.virustotal.File

MalwareDropper.pdf.exe

Weight	0
MeaningfulName	MalwareDropper.pdf.exe
File Id	20617b000124ae3aab89a3c9617015231ba44ebab062b2b14a153a39abf5c5d4
Names	MalwareDropper.pdf.exe
File Type	PEEXE
File Type Description	Win32 EXE
MD5	78e88586a5f7f477577698516b123358
SHA-1	02d6d6a2a798c5eac55a3f1c066a741732a94570
SHA-256	20617b000124ae3aab89a3c9617015231ba44ebab062b2b14a153a39abf5c5d4
Vhash	02603e0f7d70101011z11z67z101013z13z10101019z
Authentihash	6af1777bfea7ed44c0c36256f90096764081d00bd8343d04bf43ef9b58fb8e9e
SSDEEP	49152:2shdadB1iAv3xSsX2a07z0pCxA/fiQEb90B:+vixlspQAp
Magic	PE32 executable for MS Windows (GUI) Intel 80386 32-bit
File Size	2316464
Tags	peexe, signed, upx, overlay
Capability Tags	
Downloadable	null
Creation Date	2016-01-26T16:14:27Z
First Submission Date	2016-01-27T12:07:45Z
Last Submission Date	2016-01-27T12:07:45Z
Last Analysis Date	2020-09-23T20:32:56Z
Total Votes - Harmless	0
Total Votes - Malicious	0
Submissions	1
Reputation	0

View on VirusTotal

GUI Url:
https://www.virustotal.com/gui/file/20617b000124ae3aab89a3c9617015231ba44ebab062b2b14a153a39abf5c5d4

File Summary

Names	MalwareDropper.pdf.exe
File Type	peexe
File Type Description	Win32 EXE
Tags	peexe, signed, upx, overlay
Times Submitted	1

TrID - file type identification tool

File Type	Probability %
UPX compressed Win32 Executable	30.6
Win64 Executable (generic)	27.6
Win32 EXE Yoda's Crypter	26.6
Win32 Dynamic Link Library (generic)	6.5
Win32 Executable (generic)	4.5

VirusTotal Analysis Summary

Aggregate Result	malicious - 34 / 56

VirusTotal Analysis Stats

Analysis Type	Number of Analysis
Confirmed Timeout	0
Failure	0
Harmless	0
Malicious	34
Suspicious	0
Timeout	0
Type Unsupported	0
Undetected	22
Total	**56**

Community Votes

Total votes cast: 0

Incoming (1)

DNS Name	www.evil.com

VirusTotal File

maltego.virustotal.File

minilab_3-1.exe

Weight	0
MeaningfulName	minilab_3-1.exe
File Id	d167d1b450fde5775ee3231764ec11d9c265fcf6517e95347a547a2c453f2b11
Names	minilab_3-1.exe
File Type	PEEXE
File Type Description	Win32 EXE
MD5	3c31d9d9acfca8810785b76406c2d999
SHA-1	a41069c727255c8103a732bba60a3c78a7ee672b
SHA-256	d167d1b450fde5775ee3231764ec11d9c265fcf6517e95347a547a2c453f2b11
Vhash	093056655d15551az12nz15z907001e1z
Authentihash	045bd66f171afed605c9332a5e355d1a93fea6c21f4b8200b3bb0403c9579794
SSDEEP	192:2DAb7yn8XW8hB46kD4eHkkt+xGPCSzruGQG67Vaou:iAb7y8XW8U6kD5PCSHuGs
Magic	PE32 executable for MS Windows (console) Intel 80386 32-bit
File Size	9728
Tags	peexe
Capability Tags	
Downloadable	null
Creation Date	2016-06-14T00:12:25Z
First Submission Date	2018-06-20T13:02:17Z
Last Submission Date	2018-06-20T13:02:17Z
Last Analysis Date	2018-07-19T06:03:41Z
Total Votes - Harmless	0
Total Votes - Malicious	0
Submissions	1
Reputation	0

View on VirusTotal

GUI Url:
https://www.virustotal.com/gui/file/d167d1b450fde5775ee3231764ec11d9c265fcf6517e95347a547a2c453f2b11

File Summary

Names	minilab_3-1.exe
File Type	peexe
File Type Description	Win32 EXE
Tags	peexe
Times Submitted	1

TrID - file type identification tool

File Type	Probability %
Win64 Executable (generic)	61.7
Win32 Dynamic Link Library (generic)	14.7
Win32 Executable (generic)	10.0
OS/2 Executable (generic)	4.5
Generic Win/DOS Executable	4.4

VirusTotal Analysis Summary

Aggregate Result	undetected - 67 / 70

VirusTotal Analysis Stats

Analysis Type	Number of Analysis
Confirmed Timeout	0
Failure	0
Harmless	0
Malicious	1
Suspicious	0
Timeout	0
Type Unsupported	2
Undetected	67
Total	**70**

Community Votes

Total votes cast: 0

Incoming (1)

DNS Name	www.evil.com

Location

maltego.Location

Jacksonville, US

Weight	66
Name	Jacksonville, US
Country	US
City	Jacksonville
Street Address	5335 Gate Parkway care of Network Solutions PO Box 459
Area	
Area Code	32256
Country Code	
Longitude	0.0
Latitude	0.0

Info

Relevance:	0.329012
Count:	3

Incoming (1)

Domain	evil.com

A Record

maltego.ARecord

apitwitter.com.evil.co

Weight	0
IPv4 Address	52.128.23.153
Time to Live (TTL)	0
DNS Name	apitwitter.com.evil.co
Time To Live	3600
Type	A

Incoming (1)

DNS Name	apitwitter.com.evil.co

Email Address

maltego.EmailAddress

evil@unspeakable-evil.com

Weight	9
Email Address	evil@unspeakable-evil.com
Urls	https://www.unspeakable-evil.com/ Unspeakable Evil

Snippets

From Bing Search: ["evil.com" contact; Page 7]

Unspeakable Evil

[https://www.unspeakable-evil.com]

Unspeakable Evil All-Hand-Made / All-Natural / Pure-Evil. Evil is here. Shop - Unspeakable Evil on Etsy. Evil is nice. Contact us: E vil@Unspeakable-Evil.com. contact: evil@unspeakable-evil.com est. 2020, Brooklyn, NY . Page updated. Google Sites. Report abuse ...

2021-10-03T15:13:00.0000000Z

Incoming (1)

Domain	evil.com

Email Address

maltego.EmailAddress

vil@unspeakable-evil.com

Weight	18
Email Address	vil@unspeakable-evil.com
Urls	https://www.unspeakable-evil.com/ Unspeakable Evil

Snippets

From Bing Search: ["evil.com" contact; Page 7]

Unspeakable Evil

[https://www.unspeakable-evil.com]

Unspeakable Evil All-Hand-Made / All-Natural / Pure-Evil. Evil is here. Shop - Unspeakable Evil on Etsy. Evil is nice. Contact us: E vil@Unspeakable-Evil.com. contact: evil@unspeakable-evil.com est. 2020, Brooklyn, NY . Page updated. Google Sites. Report abuse ...

2021-10-03T15:13:00.0000000Z

Incoming (1)

Domain	evil.com

Email Address

maltego.EmailAddress

zen@evil.com

Weight	59
Email Address	zen@evil.com
Urls	https://sites.google.com/a/devitto.com/dom/Dom-De-Vitto-DeVitto-Brain-Sprinkles/Dom-De-Vitto-DeVitto-Brain-Sprinkles-Security Security - Dom De Vitto's Home Page - Google Search

Snippets

Incoming (1)

Domain	evil.com

VirusTotal File

maltego.virustotal.File

06-gotor-action.pdf

Weight	0
MeaningfulName	06-gotor-action.pdf
File Id	b1cfa0b0205e3722107cc9c3300924f1b707116c88bf63a184203c0291aad329
Names	06-gotor-action.pdf
File Type	PDF
File Type Description	PDF
MD5	02728f5b60f8f3b32483edfaec60d371
SHA-1	210df6bab5e8ce1dbba89308342352a322503d86
SHA-256	b1cfa0b0205e3722107cc9c3300924f1b707116c88bf63a184203c0291aad329
Vhash	90961a5aeeabe9904e9511d7e27cc011e
Authentihash	
SSDEEP	12:IC2NF0sFb4uxmVqeg4FOK45nL/dek3UdlcSgoiUDOB5dp4duSQD+jaCWyG8KxsRU:1EPxPeLQUlcSwuONpiuDajIYTC
Magic	PDF document, version 1.7
File Size	954
Tags	cve-2018-4993, runtime-modules, detect-debug-environment, exploit, autoaction, checks-user-input, pdf, direct-cpu-clock-access
Capability Tags	
Downloadable	null
Creation Date	
First Submission Date	2020-08-12T10:07:11Z
Last Submission Date	2020-08-12T10:07:11Z
Last Analysis Date	2021-02-12T20:48:50Z
Total Votes - Harmless	0
Total Votes - Malicious	0
Submissions	1
Reputation	0

View on VirusTotal

GUI Url:
https://www.virustotal.com/gui/file/b1cfa0b0205e3722107cc9c3300924f1b707116c88bf63a184203c0291aad329

File Summary	
Names	06-gotor-action.pdf
File Type	pdf
File Type Description	PDF
Tags	cve-2018-4993, runtime-modules, detect-debug-environment, exploit, autoaction, checks-user-input, pdf, direct-cpu-clock-access
Times Submitted	1

TrID - file type identification tool	
File Type	Probability %
Adobe Portable Document Format	100.0

VirusTotal Analysis Summary	
Aggregate Result	undetected - 57 / 73

VirusTotal Analysis Stats	
Analysis Type	Number of Analysis
Confirmed Timeout	0
Failure	3
Harmless	0
Malicious	1
Suspicious	0
Timeout	0
Type Unsupported	12
Undetected	57
Total	**73**

Community Votes

Total votes cast: 0

Incoming (1)

DNS Name	evil.com

Email Address

maltego.EmailAddress

hacker@evil.com

Weight	68
Email Address	hacker@evil.com
Urls	https://inst.eecs.berkeley.edu/~cs161/sp14/slides/2.10.Webinject.pdf Server-side Web Security and Injection Attacks

Snippets

From Bing Search: [inbody:"evil.com" mail; Page 3]

Server-side Web Security and Injection Attacks

[https://inst.eecs.berkeley.edu/~cs161/sp14/slides/2.10.Webinject.pdf]

"grep 'foo\\\'; mail -s hacker@evil.com

2021-08-28T11:52:00.0000000Z

Incoming (1)

Domain	evil.com

VirusTotal File

maltego.virustotal.File

binded_server.exe

Weight	0
MeaningfulName	binded_server.exe
File Id	255b7fdd8acc692ee4eea996fe7a24e0d02b0c71b1cd621fe53e619cd2c3bc3b
Names	binded_server.exe
File Type	PEEXE
File Type Description	Win32 EXE
MD5	b49b9f9e16f9d557c1fb98c446c2890e
SHA-1	3c080e93cefa94a7fb2c5b48b5efe5c8100c5952
SHA-256	255b7fdd8acc692ee4eea996fe7a24e0d02b0c71b1cd621fe53e619cd2c3bc3b
Vhash	04502d0d5bz2!z
Authentihash	508456bd92fd9ff0e5a97dba02ddd4b5ac121dd1abb39c3703cab22c21d98d3b
SSDEEP	12288:sqmpplpGoGL3etQoMiXM8gxf/Sj4yEbMDRxT:u563ey8gZqj4yEWL
Magic	MS-DOS executable, MZ for MS-DOS
File Size	439013
Tags	peexe, overlay, runtime-modules, fsg
Capability Tags	
Downloadable	null
Creation Date	1987-09-11T01:35:02Z
First Submission Date	2019-11-22T18:03:07Z
Last Submission Date	2019-11-22T18:03:07Z
Last Analysis Date	2019-11-22T18:27:25Z
Total Votes - Harmless	0
Total Votes - Malicious	0
Submissions	1
Reputation	0

View on VirusTotal

GUI Url:
https://www.virustotal.com/gui/file/255b7fdd8acc692ee4eea996fe7a24e0d02b0c71b1cd621fe53e619cd2c3bc3b

File Summary

Names	binded_server.exe
File Type	peexe
File Type Description	Win32 EXE
Tags	peexe, overlay, runtime-modules, fsg
Times Submitted	1

TrID - file type identification tool

File Type	Probability %
Win32 Executable (generic)	52.9
Generic Win/DOS Executable	23.5
DOS Executable Generic	23.5

VirusTotal Analysis Summary

Aggregate Result	malicious - 58 / 69

VirusTotal Analysis Stats

Analysis Type	Number of Analysis
Confirmed Timeout	0
Failure	0
Harmless	0
Malicious	58
Suspicious	0
Timeout	0
Type Unsupported	2
Undetected	9
Total	**69**

Community Votes

Total votes cast: 0

Incoming (1)

DNS Name	evil.com

Email Address

maltego.EmailAddress

collect@evil.com

Weight	77
Email Address	collect@evil.com
Urls	https://www.theregister.com/2007/09/26/gmail_backdoor_vulnerability/ New cracks in Google mail • The Register https://www.theregister.com/2007/09/26/gmail_backdoor_vulnerability/ New cracks in Google mail • The Register

Snippets

From Bing Search: [inbody:"evil.com" mail; Page 3]

New cracks in Google mail • The Register

[https://www.theregister.com/2007/09/26/gmail_backdoor_vulnerability]

The naughty site uses a sleight of hand known as a multipart/form-data POST, which writes a filter to Gmail that causes all email with attachments to be forwarded to collect@evil.com. Petkov didn't provide a proof of concept or detailed documentation, but Ryan Naraine of the Zero Day blog writes here that the exploit was demonstrated for him.

2021-07-17T06:24:00.0000000Z

New cracks in Google mail • The Register

[https://www.theregister.com/2007/09/26/gmail_backdoor_vulnerability]

The naughty site uses a sleight of hand known as a multipart/form-data POST, which writes a filter to Gmail that causes all email with attachments to be forwarded to collect@evil.com. Petkov didn't provide a proof of concept or detailed documentation, but Ryan Naraine of the Zero Day blog writes here that the exploit was demonstrated for him.

2021-07-17T06:24:00.0000000Z

Incoming (1)

Domain	evil.com

VirusTotal File

maltego.virustotal.File

dropper.exe

Weight	0
MeaningfulName	dropper.exe
File Id	e624a71d0e0a8080a098c2a8f8bb84b2f1871ce0bd5bafbbeaccde00993c6b7a
Names	dropper.exe
File Type	PEEXE
File Type Description	Win32 EXE
MD5	2c4cf27f3697e6f60bf8b66467babf05
SHA-1	9b66ed046bb130e22a678d5bf11ca4980650bd39
SHA-256	e624a71d0e0a8080a098c2a8f8bb84b2f1871ce0bd5bafbbeaccde00993c6b7a
Vhash	0351175d1555151c0d1d1018z211ffz11z1031z4bz
Authentihash	a6bc16ad6d2fc7586edd10917c4f76d2173265504c041ab547ac2f928fdff0b7
SSDEEP	6144:NIpXMLiDQM+r0L0kp/kuSwbEBUCq3sBD4xzQrdk+sIXl81WugZ:qyl5QVy4Qi022KnhwZ
Magic	PE32+ executable for MS Windows (console) Mono/.Net assembly
File Size	394897
Tags	peexe, assembly, overlay, runtime-modules, checks-network-adapters, direct-cpu-clock-access, 64bits
Capability Tags	
Downloadable	null
Creation Date	2021-02-13T15:08:54Z
First Submission Date	2021-02-13T14:09:59Z
Last Submission Date	2021-02-13T14:09:59Z
Last Analysis Date	2021-02-17T15:40:11Z
Total Votes - Harmless	0
Total Votes - Malicious	0
Submissions	1
Reputation	0

View on VirusTotal

GUI Url:
https://www.virustotal.com/gui/file/e624a71d0e0a8080a098c2a8f8bb84b2f1871ce0bd5bafbbeaccde00993c6b7a

File Summary

Names	dropper.exe
File Type	peexe
File Type Description	Win32 EXE
Tags	peexe, assembly, overlay, runtime-modules, checks-network-adapters, direct-cpu-clock-access, 64bits
Times Submitted	1

TrID - file type identification tool	
File Type	Probability %
Microsoft Visual C++ compiled executable (generic)	41.1
Win64 Executable (generic)	26.2
Win16 NE executable (generic)	17.5
OS/2 Executable (generic)	5.0
Generic Win/DOS Executable	4.9

VirusTotal Analysis Summary	
Aggregate Result	undetected - 40 / 76

VirusTotal Analysis Stats	
Analysis Type	Number of Analysis
Confirmed Timeout	0
Failure	0
Harmless	0
Malicious	31
Suspicious	0
Timeout	0
Type Unsupported	5
Undetected	40
Total	**76**

Community Votes

Total votes cast: 0

Incoming (1)

DNS Name	evil.com

Email Address

maltego.EmailAddress

site@evil.com

Weight	84
Email Address	site@evil.com
Urls	https://softwareengineering.stackexchange.com/questions/216605/how-do-web-servers-enforce-the-same-origin-policy web development - How do web servers enforce the same ...

Snippets

From Bing Search: [inbody:"evil.com" mail; Page 3]

web development - How do web servers enforce the same ...

[https://softwareengineering.stackexchange.com/questions/216605]

If the SOP were not in place, and I was signed into Gmail, the script at evil.com could see my inbox. If the site at evil.com wants to load mail.google.com without my cookies, it can just use a proxy server; the public contents of mail.google.com are not a secret (but the contents of mail.google.com when accessed with my cookies are a secret).

2021-09-16T17:33:00.0000000Z

Incoming (1)

Domain	evil.com

VirusTotal File

maltego.virustotal.File

evilback.exe.bin

Weight	0
MeaningfulName	evilback.exe.bin
File Id	046217f5bae309bf79fff719e18892570aa092febb0096b9169760ae2bab24c2
Names	evilback.exe.bin, evilback.exe, 4c2.exe
File Type	PEEXE
File Type Description	Win32 EXE
MD5	24f8149fff603a301af21b169d4075a2
SHA-1	900c7a962b4f83e68242d6e901875c0e9a51be64
SHA-256	046217f5bae309bf79fff719e18892570aa092febb0096b9169760ae2bab24c2
Vhash	0150f76d155c0d1d1d151az1625=z
Authentihash	0db9600ffddf0de052bb65199ce9aa140869b817b6cd82a050bfbed447baf8b9
SSDEEP	1536:4MMD2tpNcLyWG3sTmoAWoPIN1yNfiHuf3Ou3q2OWbSXIWcnxOxo:4MMDMpNcLb+2mlwQfiHmW6Eo
Magic	PE32 executable for MS Windows (GUI) Intel 80386 32-bit
File Size	109279
Tags	peexe, overlay
Capability Tags	
Downloadable	null
Creation Date	2017-01-30T12:29:56Z
First Submission Date	2017-01-30T06:49:15Z
Last Submission Date	2017-01-30T06:49:15Z
Last Analysis Date	2020-11-15T14:43:10Z
Total Votes - Harmless	0
Total Votes - Malicious	0
Submissions	1
Reputation	0

View on VirusTotal

GUI Url:
https://www.virustotal.com/gui/file/046217f5bae309bf79fff719e18892570aa092febb0096b9169760ae2bab24c2

File Summary	
Names	evilback.exe.bin, evilback.exe, 4c2.exe
File Type	peexe
File Type Description	Win32 EXE
Tags	peexe, overlay
Times Submitted	1

TrID - file type identification tool	
File Type	Probability %
Win64 Executable (generic)	36.6
Microsoft Visual C++ compiled executable (generic)	21.9
Win16 NE executable (generic)	18.6
Win32 Dynamic Link Library (generic)	8.7
Win32 Executable (generic)	5.9

VirusTotal Analysis Summary	
Aggregate Result	malicious - 50 / 73

VirusTotal Analysis Stats	
Analysis Type	Number of Analysis
Confirmed Timeout	0
Failure	0
Harmless	0
Malicious	50
Suspicious	0
Timeout	0
Type Unsupported	3
Undetected	20
Total	**73**

Community Votes

Total votes cast: 0

Incoming (1)

DNS Name	evil.com

A Record

maltego.ARecord

apitwitter.com.evil.com

Weight	0
IPv4 Address	66.96.146.129
Time to Live (TTL)	0
DNS Name	apitwitter.com.evil.com
Time To Live	3600
Type	A

Incoming (1)

DNS Name	apitwitter.com.evil.com

Email Address

maltego.EmailAddress

talk2us@lesserevil.com

Weight	26
Email Address	talk2us@lesserevil.com
Urls	https://lesserevil.com/pages/contact Contact LesserEvil | Contact Lesser Evil | Healthy Snacks

Snippets

From Bing Search: ["evil.com" contact; Page 7]

Contact LesserEvil | Contact Lesser Evil | Healthy Snacks

[https://lesserevil.com/pages/contact]

Contact. NAME EMAIL SUBJECT. MESSAGE. Reach Us (203) 529-3551 x 100 talk2us@lesserevil.com. Office Hours Monday - Friday 8:30am - 5:00pm EST Snail Mail 41 Eagle Rd Danbury, CT 06810 YOUR CART. CONTINUE SHOPPING $ Subtotal. Checkout. temp. Shop All; Shop Wholesale ...

2021-09-30T19:34:00.0000000Z

Incoming (1)

Domain	evil.com

VirusTotal File

maltego.virustotal.File

notevil.exe

Weight	0
MeaningfulName	notevil.exe
File Id	79809204ed4200b14dafd46d7e65135a453332f8b7d4c82bbb5869127f13f209
Names	notevil.exe
File Type	PEEXE
File Type Description	Win32 EXE
MD5	08b291ffc1e3af6f62770a28e2351e38
SHA-1	eeabf6b918a16632e6eecd820694002e69657f10
SHA-256	79809204ed4200b14dafd46d7e65135a453332f8b7d4c82bbb5869127f13f209
Vhash	025036151e6bz2!z
Authentihash	148aa595b8f29cf6d5a9527ce97e9612aa3e458565fee3f28e36e3896a9ab97d
SSDEEP	3072:Yqgp8+K0FG6nYvyG6nYIBwcMMLTR5Tr1jYgLDiE6678Jj69bsjIGa:n81nLGSsc5LTnPNYgLDQjq
Magic	PE32+ executable for MS Windows (GUI) Mono/.Net assembly
File Size	207872
Tags	peexe, assembly, invalid-rich-pe-linker-version, runtime-modules, malware, checks-network-adapters, direct-cpu-clock-access, 64bits
Capability Tags	
Downloadable	null
Creation Date	2010-04-14T22:06:53Z
First Submission Date	2021-07-14T20:10:44Z
Last Submission Date	2021-07-14T20:10:44Z
Last Analysis Date	2021-07-23T13:03:46Z
Total Votes - Harmless	0
Total Votes - Malicious	0
Submissions	1
Reputation	0

View on VirusTotal

GUI Url:
https://www.virustotal.com/gui/file/79809204ed4200b14dafd46d7e65135a453332f8b7d4c82bbb5869127f13f209

File Summary

Names	notevil.exe
File Type	peexe
File Type Description	Win32 EXE
Tags	peexe, assembly, invalid-rich-pe-linker-version, runtime-modules, malware, checks-network-adapters, direct-cpu-clock-access, 64bits
Times Submitted	1

TrID - file type identification tool	
File Type	Probability %
Win64 Executable (generic)	48.7
Win16 NE executable (generic)	23.3
OS/2 Executable (generic)	9.3
Generic Win/DOS Executable	9.2
DOS Executable Generic	9.2

VirusTotal Analysis Summary	
Aggregate Result	malicious - 48 / 74

VirusTotal Analysis Stats	
Analysis Type	Number of Analysis
Confirmed Timeout	1
Failure	0
Harmless	0
Malicious	48
Suspicious	0
Timeout	0
Type Unsupported	5
Undetected	20
Total	**74**

Community Votes

Total votes cast: 0

Incoming (1)

DNS Name	evil.com

Email Address

maltego.EmailAddress

attacker@evil.com

Weight	34
Email Address	attacker@evil.com
Urls	https://blog.sucuri.net/2019/10/an-indirect-way-to-change-cpanel-passwords.html An Indirect Way to Change cPanel Passwords

Snippets

From Bing Search: [inbody:"evil.com" contact; Page 6]

An Indirect Way to Change cPanel Passwords

[https://blog.sucuri.net/2019/10/an-indirect-way-to-change-cpanel-passwords.html]

Secondary contact email addresses configured in this manner can also be silently removed during this modification process for the primary contact email address. "email": 'attacker@evil.com' "notify_contact_address_change": 0

2021-09-29T04:45:00.0000000Z

Incoming (1)

Domain	evil.com

VirusTotal File

maltego.virustotal.File

b37bea1d85faf990730dff11fbfc5c71c9ac4c3a472c77c6ecf9b41b675c908b~

Weight	0
MeaningfulName	b37bea1d85faf990730dff11fbfc5c71c9ac4c3a472c77c6ecf9b41b675c908b~
File Id	974b58d772306dde16e4bed2ecb1c91b8d70a4dc035152010f6816093338d67e
Names	b37bea1d85faf990730dff11fbfc5c71c9ac4c3a472c77c6ecf9b41b675c908b~
File Type	DOC
File Type Description	MS Word Document
MD5	c69f533fc9841df5b35ef7a46f245eab
SHA-1	f2e7ffa187d582f780cb41583e92a8e940027c4a
SHA-256	974b58d772306dde16e4bed2ecb1c91b8d70a4dc035152010f6816093338d67e
Vhash	7a765e90b83f31e4d24daaf369125b9e
Authentihash	
SSDEEP	12288:nEMTlJ1+RjQPfrvwd0wmJ5FYU7yBZvsXiAuipadc+Y6Rs45XPzJBn8zWSW0Rvbnk:nl17wdlmJL7762luipaFY6Rejk
Magic	CDF V2 Document, Little Endian, Os: Windows, Version 10.0, Code page: 1252, Author: Harold Harepus, Template: Normal.dotm, Last Saved By: Harold Harepus, Revision Number: 2, Name of Creating Application: Microsoft Office Word, Create Time/Date: Sat Mar 20 15:31:00 2021, Last Saved Time/Date: Sat Mar 20 15:31:00 2021, Number of Pages: 1, Number of Words: 165, Number of Characters: 165, Security: 0
File Size	730112
Tags	doc, macros
Capability Tags	
Downloadable	null
Creation Date	2021-03-21T15:31Z
First Submission Date	2021-03-23T00:54:11Z
Last Submission Date	2021-03-23T00:54:11Z
Last Analysis Date	2021-04-28T11:47:50Z
Total Votes - Harmless	0
Total Votes - Malicious	0
Submissions	1
Reputation	0

View on VirusTotal

GUI Url:
https://www.virustotal.com/gui/file/974b58d772306dde16e4bed2ecb1c91b8d70a4dc035152010f6816093338d67e

File Summary

Names	b37bea1d85faf990730dff11fbfc5c71c9ac4c3a472c77c6ecf9b41b675c908b~
File Type	doc
File Type Description	MS Word Document
Tags	doc, macros
Times Submitted	1

TrID - file type identification tool

File Type	Probability %
Microsoft Word document	39.2
Kingsoft WPS Office document (alt.)	25.4
Microsoft Word document (old ver.)	24.8
Generic OLE2 / Multistream Compound	10.4

VirusTotal Analysis Summary

Aggregate Result	undetected - 32 / 76

VirusTotal Analysis Stats

Analysis Type	Number of Analysis
Confirmed Timeout	0
Failure	0
Harmless	0
Malicious	31
Suspicious	0
Timeout	0
Type Unsupported	13
Undetected	32
Total	**76**

Community Votes

Total votes cast: 0

Incoming (1)

DNS Name	evil.com

Email Address

maltego.EmailAddress

info@mid-evil.com

Weight	45
Email Address	info@mid-evil.com
Urls	https://www.mid-evil.com/contact/ Contact | Mid-Evil Industries https://www.mid-evil.com/products/ Products | Mid-Evil Industries https://www.mid-evil.com/contact/ Contact | Mid-Evil Industries

Snippets

From Bing Search: [inbody:"evil.com" contact; Page 6]

Contact | Mid-Evil Industries

[https://www.mid-evil.com/contact]

Phone: (844) 556-GRIP (4747) PO Box 7735 San Diego, CA 92167, USA Email: info@mid-evil.com Hours: Mon-Fri 9am-5pm PST

2021-10-08T17:27:00.0000000Z

Products | Mid-Evil Industries

[https://www.mid-evil.com/products]

Contact. Phone: (844) 556-GRIP (4747) PO Box 7735 San Diego, CA 92167, USA Email: info@mid-evil.com Hours: Mon-Fri 9am-5pm PST . Newsletter Sign-up. Sign-up for our newsletter to stay in-the-know on news, new product releases and special deals! Name * Email * Website. Sign Me Up! Search by Keyword. Search for: ...

2021-10-05T15:11:00.0000000Z

Contact | Mid-Evil Industries

[https://www.mid-evil.com/contact]

Phone: (844) 556-GRIP (4747) PO Box 7735 San Diego, CA 92167, USA Email: info@mid-evil.com Hours: Mon-Fri 9am-5pm PST

2021-10-08T17:27:00.0000000Z

Incoming (1)

Domain	evil.com

VirusTotal File

maltego.virustotal.File

pnuqpywn.exe

Weight	0
MeaningfulName	pnuqpywn.exe
File Id	74447979a99e329ef9cf977b22fc9047e30c41c2aae2f844accde73b858016de
Names	pnuqpywn.exe, hdxdjldu.exe, uszvudbs.exe, vyggecgp.exe
File Type	PEEXE
File Type Description	Win32 EXE
MD5	69177c319f27e9335922ce73ace1f99d
SHA-1	82cd8ecbd094e5e80d188e58a9320af83fa1f7b0
SHA-256	74447979a99e329ef9cf977b22fc9047e30c41c2aae2f844accde73b858016de
Vhash	017056157d191560e8z1ehzc0e1zcfz
Authentihash	3ab0cfc981a6258261c9466c790d536f6e3d388b54bee1dcc93eca19f9a1ba42
SSDEEP	49152:zjrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrr/:j
Magic	PE32 executable for MS Windows (GUI) Intel 80386 32-bit
File Size	12949504
Tags	peexe, direct-cpu-clock-access, checks-network-adapters, long-sleeps, checks-disk-space, runtime-modules, persistence, checks-cpu-name, detect-debug-environment, self-delete
Capability Tags	
Downloadable	null
Creation Date	2014-03-07T18:46:41Z
First Submission Date	2021-08-28T06:48:30Z
Last Submission Date	2021-08-28T06:48:30Z
Last Analysis Date	2021-09-03T16:31:16Z
Total Votes - Harmless	0
Total Votes - Malicious	0
Submissions	1
Reputation	0

View on VirusTotal

GUI Url:
https://www.virustotal.com/gui/file/74447979a99e329ef9cf977b22fc9047e30c41c2aae2f844accde73b858016de

File Summary

Names	pnuqpywn.exe, hdxdjldu.exe, uszvudbs.exe, vyggecgp.exe
File Type	peexe
File Type Description	Win32 EXE
Tags	peexe, direct-cpu-clock-access, checks-network-adapters, long-sleeps, checks-disk-space, runtime-modules, persistence, checks-cpu-name, detect-debug-environment, self-delete
Times Submitted	1

TrID - file type identification tool	
File Type	Probability %
Win64 Executable (generic)	30.2
Win32 Dynamic Link Library (generic)	18.9
Win16 NE executable (generic)	14.4
Win32 Executable (generic)	12.9
Win16/32 Executable Delphi generic	5.9

VirusTotal Analysis Summary	
Aggregate Result	malicious - 48 / 73

VirusTotal Analysis Stats	
Analysis Type	Number of Analysis
Confirmed Timeout	0
Failure	0
Harmless	0
Malicious	48
Suspicious	0
Timeout	0
Type Unsupported	5
Undetected	20
Total	**73**

Community Votes

Total votes cast: 0

Incoming (1)

DNS Name	evil.com

Email Address

maltego.EmailAddress

info@crackevil.com

Weight	52
Email Address	info@crackevil.com
Urls	https://crackevil.com/crackevil/wordpress-16-9-apk WordPress 16.9 APK - FREE DOWNLOAD - crackevil.com https://crackevil.com/wordpress-themes/newspaper-9-1-wordpress-news-theme Newspaper V9.1 – WordPress News Theme - FREE DOWNLOAD

Snippets

From Bing Search: ["evil.com" mail; Page 4]

WordPress 16.9 APK - FREE DOWNLOAD - crackevil.com

[https://crackevil.com/crackevil/wordpress-16-9-apk]

Crack Evil is the best platform to get the Premium Themes and Templates for free. Enjoy! ... And if the developers feel bad about sharing their templates, please kindly mail us at info@crackevil.com, we will remove your templates immediately. Mission News Theme by Compete Themes.

2021-08-29T19:43:00.0000000Z

Newspaper V9.1 – WordPress News Theme - FREE DOWNLOAD

[https://crackevil.com/wordpress-themes/newspaper-9-1-wordpress-news-theme]

Crack Evil is the best platform to get the Premium Themes and Templates for free. Enjoy! ... And if the developers feel bad about sharing their templates, please kindly mail us at info@crackevil.com, we will remove your templates immediately. Mission News Theme by Compete Themes.

2021-09-15T07:13:00.0000000Z

Incoming (1)

Domain	evil.com

VirusTotal File

maltego.virustotal.File

notevil_50M.exe

Weight	0
MeaningfulName	notevil_50M.exe
File Id	e4688c38dce9a012f0fc6cc63a4b27e638c6346b8da67d19ca80a6b584ce36f9
Names	notevil_50M.exe
File Type	PEEXE
File Type Description	Win32 EXE
MD5	2579ca3856362cd6993018a3d93dce90
SHA-1	5fc6bcd6644b0eb401c452c8328ce5e7800d4e32
SHA-256	e4688c38dce9a012f0fc6cc63a4b27e638c6346b8da67d19ca80a6b584ce36f9
Vhash	057036151e6bz2!z
Authentihash	aff1e82ada1e774871815c08fd6aa5776ce5003f7a06b1343ddff4f9a0e48716
SSDEEP	1572864:28iriwdLIfzJjl/h3tvFjapHZAayFr0c7m458n:krVdECh3lWgc735e
Magic	PE32+ executable for MS Windows (GUI) Mono/.Net assembly
File Size	52636672
Tags	malware, assembly, invalid-rich-pe-linker-version, overlay, runtime-modules, peexe, detect-debug-environment, checks-network-adapters, long-sleeps, direct-cpu-clock-access, 64bits
Capability Tags	
Downloadable	null
Creation Date	2010-04-14T22:06:53Z
First Submission Date	2021-07-14T20:10:53Z
Last Submission Date	2021-07-14T20:10:53Z
Last Analysis Date	2021-07-23T13:03:46Z
Total Votes - Harmless	0
Total Votes - Malicious	0
Submissions	1
Reputation	0

View on VirusTotal

GUI Url:
https://www.virustotal.com/gui/file/e4688c38dce9a012f0fc6cc63a4b27e638c6346b8da67d19ca80a6b584ce36f9

File Summary

Names	notevil_50M.exe
File Type	peexe
File Type Description	Win32 EXE
Tags	malware, assembly, invalid-rich-pe-linker-version, overlay, runtime-modules, peexe, detect-debug-environment, checks-network-adapters, long-sleeps, direct-cpu-clock-access, 64bits
Times Submitted	1

TrID - file type identification tool

File Type	Probability %
Win64 Executable (generic)	48.7
Win16 NE executable (generic)	23.3
OS/2 Executable (generic)	9.3
Generic Win/DOS Executable	9.2
DOS Executable Generic	9.2

VirusTotal Analysis Summary

Aggregate Result	malicious - 35 / 74

VirusTotal Analysis Stats

Analysis Type	Number of Analysis
Confirmed Timeout	1
Failure	0
Harmless	0
Malicious	35
Suspicious	0
Timeout	0
Type Unsupported	8
Undetected	30
Total	**74**

Community Votes

Total votes cast: 0

Incoming (1)

DNS Name	evil.com

VirusTotal File

maltego.virustotal.File

svowuweo.exe

Weight	0
MeaningfulName	svowuweo.exe
File Id	e4a1901cf10117176366b4e2a125278cbdf28fd760fa73081e8535b8c0cee1ab
Names	svowuweo.exe
File Type	PEEXE
File Type Description	Win32 EXE
MD5	ec10d2e5a0e667ca562ec8209fbfb180
SHA-1	bed09e52ecabd689654bb5c4c7fc21acb8f4e558
SHA-256	e4a1901cf10117176366b4e2a125278cbdf28fd760fa73081e8535b8c0cee1ab
Vhash	017056655d75551018z71!z
Authentihash	3ca21b1f56b6e659421da61924d98217fbd52eef96e4485205b89945f73c4494
SSDEEP	6144:16QKIBQEbw3wv/wGw+R7c2nM6F4VDeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeee7:16QKIBQEbFvY+ldq
Magic	PE32 executable for MS Windows (GUI) Intel 80386 32-bit
File Size	13807616
Tags	peexe, checks-disk-space, runtime-modules, checks-network-adapters, long-sleeps, direct-cpu-clock-access, persistence, checks-cpu-name, detect-debug-environment, self-delete, nxdomain
Capability Tags	
Downloadable	null
Creation Date	2020-08-28T10:07:41Z
First Submission Date	2021-10-01T19:10:44Z
Last Submission Date	2021-10-01T19:10:44Z
Last Analysis Date	2021-10-05T18:20:50Z
Total Votes - Harmless	0
Total Votes - Malicious	0
Submissions	1
Reputation	0

View on VirusTotal

GUI Url:
https://www.virustotal.com/gui/file/e4a1901cf10117176366b4e2a125278cbdf28fd760fa73081e8535b8c0cee1ab

File Summary

Names	svowuweo.exe
File Type	peexe
File Type Description	Win32 EXE
Tags	peexe, checks-disk-space, runtime-modules, checks-network-adapters, long-sleeps, direct-cpu-clock-access, persistence, checks-cpu-name, detect-debug-environment, self-delete, nxdomain
Times Submitted	1

TrID - file type identification tool	
File Type	Probability %
Windows Control Panel Item (generic)	88.3
Win64 Executable (generic)	4.7
Win16 NE executable (generic)	2.2
Win32 Executable (generic)	2.0
OS/2 Executable (generic)	0.9

VirusTotal Analysis Summary	
Aggregate Result	malicious - 41 / 73

VirusTotal Analysis Stats	
Analysis Type	Number of Analysis
Confirmed Timeout	0
Failure	0
Harmless	0
Malicious	41
Suspicious	0
Timeout	0
Type Unsupported	5
Undetected	27
Total	**73**

Community Votes

Total votes cast: 0

Incoming (1)

DNS Name	evil.com

VirusTotal File

maltego.virustotal.File

bbagrfmp.exe

Weight	0
MeaningfulName	bbagrfmp.exe
File Id	259405c50a2c672f8b80d960f722cb99358c02fb0dc944b74bce26a85c93ec4f
Names	bbagrfmp.exe
File Type	PEEXE
File Type Description	Win32 EXE
MD5	768856847477a0c8d5438866e94c54ff
SHA-1	f54424538f8a6451c65eceb47852f4781638ab0b
SHA-256	259405c50a2c672f8b80d960f722cb99358c02fb0dc944b74bce26a85c93ec4f
Vhash	01705e751c1d156az14!z
Authentihash	63a2aa2f603bab3b0ff7000430f1849521752c91239521236796b6c967838218
SSDEEP	3072:LfwfP1U/zlSXrGoaPgg5K6uUUEG/FJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJD:L2dU/CrS30B/
Magic	PE32 executable for MS Windows (GUI) Intel 80386 32-bit
File Size	12918272
Tags	peexe, direct-cpu-clock-access, checks-network-adapters, long-sleeps, checks-disk-space, runtime-modules, persistence, checks-cpu-name, detect-debug-environment, self-delete, nxdomain
Capability Tags	
Downloadable	null
Creation Date	2014-09-17T23:06:57Z
First Submission Date	2021-09-30T13:46:45Z
Last Submission Date	2021-09-30T13:46:45Z
Last Analysis Date	2021-10-04T14:57:23Z
Total Votes - Harmless	0
Total Votes - Malicious	0
Submissions	1
Reputation	0

View on VirusTotal

GUI Url:
https://www.virustotal.com/gui/file/259405c50a2c672f8b80d960f722cb99358c02fb0dc944b74bce26a85c93ec4f

File Summary

Names	bbagrfmp.exe
File Type	peexe
File Type Description	Win32 EXE
Tags	peexe, direct-cpu-clock-access, checks-network-adapters, long-sleeps, checks-disk-space, runtime-modules, persistence, checks-cpu-name, detect-debug-environment, self-delete, nxdomain
Times Submitted	1

TrID - file type identification tool	
File Type	Probability %
Win32 Dynamic Link Library (generic)	27.1
Win16 NE executable (generic)	20.7
Win32 Executable (generic)	18.5
Win16/32 Executable Delphi generic	8.5
OS/2 Executable (generic)	8.3

VirusTotal Analysis Summary	
Aggregate Result	malicious - 49 / 74

VirusTotal Analysis Stats	
Analysis Type	Number of Analysis
Confirmed Timeout	1
Failure	0
Harmless	0
Malicious	49
Suspicious	0
Timeout	1
Type Unsupported	5
Undetected	18
Total	**74**

Community Votes

Total votes cast: 0

Incoming (1)

DNS Name	evil.com

VirusTotal File

maltego.virustotal.File

gibmtbpf.exe

Weight	0
MeaningfulName	gibmtbpf.exe
File Id	149d456be883f6844fb9378b2992e5597d6efd4401c8fc108bed8160070fe09e
Names	gibmtbpf.exe, eclmvrgc.exe, jaigqlsg.exe, ejtoiurt.exe, tphhetsg.exe
File Type	PEEXE
File Type Description	Win32 EXE
MD5	3eb9f7f66313863c5b90f00819e68cfb
SHA-1	d5c23aed5ec81049f8cf1c6c3de3260e9544dd59
SHA-256	149d456be883f6844fb9378b2992e5597d6efd4401c8fc108bed8160070fe09e
Vhash	017046755d155az61!z
Authentihash	d83d8e3e372118c403f04ede06ab01aef1851e47b712522dff21bed40a05fbb8
SSDEEP	12288:DQuDiqkdsom6FLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLb:DQykdsY
Magic	PE32 executable for MS Windows (GUI) Intel 80386 32-bit
File Size	12859392
Tags	peexe, direct-cpu-clock-access, checks-network-adapters, long-sleeps, checks-disk-space, runtime-modules, persistence, calls-wmi, detect-debug-environment, checks-cpu-name, self-delete, nxdomain
Capability Tags	
Downloadable	null
Creation Date	2019-09-11T09:10:53Z
First Submission Date	2021-10-07T04:52:32Z
Last Submission Date	2021-10-07T04:52:32Z
Last Analysis Date	2021-10-11T06:02:19Z
Total Votes - Harmless	0
Total Votes - Malicious	0
Submissions	1
Reputation	0

View on VirusTotal

GUI Url:
https://www.virustotal.com/gui/file/149d456be883f6844fb9378b2992e5597d6efd4401c8fc108bed8160070fe09e

File Summary

Names	gibmtbpf.exe, eclmvrgc.exe, jaigqlsg.exe, ejtoiurt.exe, tphhetsg.exe
File Type	peexe
File Type Description	Win32 EXE
Tags	peexe, direct-cpu-clock-access, checks-network-adapters, long-sleeps, checks-disk-space, runtime-modules, persistence, calls-wmi, detect-debug-environment, checks-cpu-name, self-delete, nxdomain
Times Submitted	1

TrID - file type identification tool

File Type	Probability %
Win32 Executable MS Visual C++ (generic)	48.8
Win64 Executable (generic)	16.4
Win32 Dynamic Link Library (generic)	10.2
Win16 NE executable (generic)	7.8
Win32 Executable (generic)	7.0

VirusTotal Analysis Summary

Aggregate Result	malicious - 52 / 74

VirusTotal Analysis Stats

Analysis Type	Number of Analysis
Confirmed Timeout	0
Failure	0
Harmless	0
Malicious	52
Suspicious	0
Timeout	0
Type Unsupported	5
Undetected	17
Total	**74**

Community Votes

Total votes cast: 0

Incoming (1)

DNS Name	evil.com

VirusTotal File

maltego.virustotal.File

yfighhxl.exe

Weight	0
MeaningfulName	yfighhxl.exe
File Id	74b585db2b23c02c943b7e21066e278fbf850298af966e8b094195a926b713ec
Names	yfighhxl.exe
File Type	PEEXE
File Type Description	Win32 EXE
MD5	b5e86ccb94a426b9f10eb983830d7066
SHA-1	314873f9ce54a2cb31efff2c3b4bfce263769897
SHA-256	74b585db2b23c02c943b7e21066e278fbf850298af966e8b094195a926b713ec
Vhash	017056651d75551az6b!z
Authentihash	afb7151bc1445056fbf43e88edca0fa026494b1a183594997ca4ef6631252035
SSDEEP	196608:pPRMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMk:p
Magic	PE32 executable for MS Windows (GUI) Intel 80386 32-bit
File Size	12210176
Tags	peexe, nxdomain
Capability Tags	
Downloadable	null
Creation Date	2020-04-10T01:12:36Z
First Submission Date	2021-10-10T01:25:05Z
Last Submission Date	2021-10-10T01:25:05Z
Last Analysis Date	2021-10-11T03:31:53Z
Total Votes - Harmless	0
Total Votes - Malicious	0
Submissions	1
Reputation	0

View on VirusTotal

GUI Url:
https://www.virustotal.com/gui/file/74b585db2b23c02c943b7e21066e278fbf850298af966e8b094195a926b713ec

File Summary

Names	yfighhxl.exe
File Type	peexe
File Type Description	Win32 EXE
Tags	peexe, nxdomain
Times Submitted	1

TrID - file type identification tool

File Type	Probability %
Win32 Executable MS Visual C++ (generic)	48.8
Win64 Executable (generic)	16.4
Win32 Dynamic Link Library (generic)	10.2
Win16 NE executable (generic)	7.8
Win32 Executable (generic)	7.0

VirusTotal Analysis Summary

Aggregate Result	malicious - 41 / 72

VirusTotal Analysis Stats

Analysis Type	Number of Analysis
Confirmed Timeout	0
Failure	0
Harmless	0
Malicious	41
Suspicious	0
Timeout	0
Type Unsupported	5
Undetected	26
Total	**72**

Community Votes

Total votes cast: 0

Incoming (1)

DNS Name	evil.com

Email Address

maltego.EmailAddress

script@evil.com

Weight	93
Email Address	script@evil.com
Urls	https://softwareengineering.stackexchange.com/questions/216605/how-do-web-servers-enforce-the-same-origin-policy web development - How do web servers enforce the same ...

Snippets

From Bing Search: [inbody:"evil.com" mail; Page 3]

web development - How do web servers enforce the same ...

[https://softwareengineering.stackexchange.com/questions/216605]

If the SOP were not in place, and I was signed into Gmail, the script at evil.com could see my inbox. If the site at evil.com wants to load mail.google.com without my cookies, it can just use a proxy server; the public contents of mail.google.com are not a secret (but the contents of mail.google.com when accessed with my cookies are a secret).

2021-09-16T17:33:00.0000000Z

Incoming (1)

Domain	evil.com

Email Address

maltego.EmailAddress

alice@evil.com

Weight	102
Email Address	alice@evil.com
Urls	https://security.stackexchange.com/questions/214925/mail-interception-fraud email - Mail interception fraud - Information Security ... https://security.stackexchange.com/questions/214925/mail-interception-fraud email - Mail interception fraud - Information Security ...

Snippets

From Bing Search: [inbody:"evil.com" mail; Page 3]

email - Mail interception fraud - Information Security ...

[https://security.stackexchange.com/questions/214925/mail-interception-fraud]

Shortly after alice@evil.com also sends a reminder mail to the customer. In this reminder there is also a pdf attachment that's nearly identical to the one Alice send, only the payment information has been altered. The customer also has a conversation with Alice about the change of bank account and always receives answers. My boss is cc'ed in ...

2021-10-04T19:21:00.0000000Z

email - Mail interception fraud - Information Security ...

[https://security.stackexchange.com/questions/214925/mail-interception-fraud]

Shortly after alice@evil.com also sends a reminder mail to the customer. In this reminder there is also a pdf attachment that's nearly identical to the one Alice send, only the payment information has been altered. The customer also has a conversation with Alice about the change of bank account and always receives answers. My boss is cc'ed in ...

2021-10-04T19:21:00.0000000Z

Incoming (1)

Domain	evil.com

STIX2 X509 Certificate

maltego.STIX2.x509-certificate

x509-certificate--e72c2a81-44d5-5c56-b9fb-9cc476194843

Weight	100
type	x509-certificate
spec_version	2.1
object_marking_refs	
granular_markings	
defanged	False
id	x509-certificate--e72c2a81-44d5-5c56-b9fb-9cc476194843
extensions	
serial	4e7eefa66e979c3d6ddafbdc4dc9df0eb95
issuer	R3
validFrom	2021-08-06 00:00:00+00:00
validTo	2021-11-04 00:00:00+00:00
subject	*.evil.com
is_self_signed	
hashes	
version	
signature_algorithm	
subject_public_key_algorithm	
subject_public_key_modulus	
subject_public_key_exponent	
x509_v3_extensions	
x_maltego_recovery_property_mapping	{"subject": ["subject"], "serial": ["serial_number"], "issuer": ["issuer"], "validFrom": ["validity_not_before"], "validTo": ["validity_not_after"]}
Subject DN	
Issuer DN	
SKI	daad26d1d9c7901537e84a12886ef8ddc37132e5
AKI	
SAN	[*.evil.com, evil.com]
Usage	
Issuance ID	
Country	
Organization	
x_maltego_marking_color	
x_maltego_marking_text	

Incoming (1)

SSL Certificate	*.evil.com

STIX2 X509 Certificate

maltego.STIX2.x509-certificate

x509-certificate--f2d07fae-c770-5241-b074-1ad8137ce391

Weight	100
type	x509-certificate
spec_version	2.1
object_marking_refs	
granular_markings	
defanged	False
id	x509-certificate--f2d07fae-c770-5241-b074-1ad8137ce391
extensions	
serial	3cf1a21b5354a66ac415c5041bad6394456
issuer	Let's Encrypt Authority X3
validFrom	2020-07-20 00:00:00+00:00
validTo	2020-10-18 00:00:00+00:00
subject	*.evil.com
is_self_signed	
hashes	
version	
signature_algorithm	
subject_public_key_algorithm	
subject_public_key_modulus	
subject_public_key_exponent	
x509_v3_extensions	
x_maltego_recovery_property_mapping	{"subject": ["subject"], "serial": ["serial_number"], "issuer": ["issuer"], "validFrom": ["validity_not_before"], "validTo": ["validity_not_after"]}
Subject DN	
Issuer DN	
SKI	daad26d1d9c7901537e84a12886ef8ddc37132e5
AKI	
SAN	[*.evil.com, evil.com]
Usage	
Issuance ID	
Country	
Organization	
x_maltego_marking_color	
x_maltego_marking_text	

Incoming (1)

SSL Certificate	*.evil.com

STIX2 X509 Certificate

maltego.STIX2.x509-certificate

x509-certificate--1ce7e13b-39f8-5d85-94ab-7567aadfe9d9

Weight	100
type	x509-certificate
spec_version	2.1
object_marking_refs	
granular_markings	
defanged	False
id	x509-certificate--1ce7e13b-39f8-5d85-94ab-7567aadfe9d9
extensions	
serial	4271acbc2e3b0e9d85a50d383cf03f22d22
issuer	R3
validFrom	2021-01-27 00:00:00+00:00
validTo	2021-04-27 00:00:00+00:00
subject	*.evil.com
is_self_signed	
hashes	
version	
signature_algorithm	
subject_public_key_algorithm	
subject_public_key_modulus	
subject_public_key_exponent	
x509_v3_extensions	
x_maltego_recovery_property_mapping	{"subject": ["subject"], "serial": ["serial_number"], "issuer": ["issuer"], "validFrom": ["validity_not_before"], "validTo": ["validity_not_after"]}
Subject DN	
Issuer DN	
SKI	daad26d1d9c7901537e84a12886ef8ddc37132e5
AKI	
SAN	[*.evil.com, evil.com]
Usage	
Issuance ID	
Country	
Organization	
x_maltego_marking_color	
x_maltego_marking_text	

Incoming (1)

SSL Certificate	*.evil.com

Domain

maltego.Domain

komikaze.com

Weight	100
Domain Name	komikaze.com
WHOIS Info	

Incoming (1)

NS Record	ns1.uniregistrymarket.link

LittleSis Public Company

maltego.littlesis.PublicCompany

VeriSign, Inc.

Weight	100
Name	VeriSign, Inc.
ID	119008
Blurb	
Primary extension	Org
Summary	
Website	www.verisigninc.com
Incorporation/Start date	
End date	
Parent ID	
Updated at	2021-04-06T20:36:45Z
Extensions	[Organization, Business, Public Company]
Aliases	[Verisign Inc, VeriSign, Inc.]
ticker	VRSN
revenue	1059366
sec_cik	1014473
name_nick	VERISIGN

Description

VeriSign, Inc.

Website

Website

www.verisigninc.com

LittleSis web link

Open on LittleSis.org

"

Incoming (1)

Company	VeriSign

STIX2 X509 Certificate

maltego.STIX2.x509-certificate

x509-certificate--87052faa-ce0b-55a0-b253-95e2150038fc

Weight	100
type	x509-certificate
spec_version	2.1
object_marking_refs	
granular_markings	
defanged	False
id	x509-certificate--87052faa-ce0b-55a0-b253-95e2150038fc
extensions	
serial	4425cf6c15690ba3f7635882e17b14c4e94
issuer	R3
validFrom	2021-03-29 00:00:00+00:00
validTo	2021-06-27 00:00:00+00:00
subject	*.evil.com
is_self_signed	
hashes	
version	
signature_algorithm	
subject_public_key_algorithm	
subject_public_key_modulus	
subject_public_key_exponent	
x509_v3_extensions	
x_maltego_recovery_property_mapping	{"subject": ["subject"], "serial": ["serial_number"], "issuer": ["issuer"], "validFrom": ["validity_not_before"], "validTo": ["validity_not_after"]}
Subject DN	
Issuer DN	
SKI	daad26d1d9c7901537e84a12886ef8ddc37132e5
AKI	
SAN	[*.evil.com, evil.com]
Usage	
Issuance ID	
Country	
Organization	
x_maltego_marking_color	
x_maltego_marking_text	

Incoming (1)

SSL Certificate	*.evil.com

LittleSis Organization

maltego.littlesis.Organization

Verisign Inc. PAC

Weight	100
Name	Verisign Inc. PAC
ID	32229
Blurb	
Primary extension	Org
Summary	
Website	
Incorporation/Start date	
End date	
Parent ID	
Updated at	2019-03-08T22:23:25Z
Extensions	[Organization, Political Fundraising Committee]
Aliases	[Verisign Inc. PAC]
fec_id	C00359240

Description

Verisign Inc. PAC

LittleSis web link

Open on LittleSis.org

"

Incoming (1)

Company	VeriSign

DNS Name

maltego.DNSName

*.com.w3snoop.com

Weight	0
DNS Name	*.com.w3snoop.com

Incoming (1)

DNS Name	w3snoop.com

SSL Certificate

maltego.X509Certificate

w3snoop.com

Weight	0
Subject	w3snoop.com
Issuer	Let's Encrypt Authority X3
Subject DN	
Issuer DN	
SKI	a13562a999cef6ce348132541ebe6b51a377518d
AKI	
Serial	434ef11ce69c119a226871134d297f5a430
SAN	[*.w3snoop.com, w3snoop.com]
Usage	
Issuance ID	
Valid From	Mon Nov 30 00:00:00 GMT 2020
Valid Until	Sun Feb 28 00:00:00 GMT 2021
Country	
Organization	

Incoming (1)

DNS Name	w3snoop.com

SSL Certificate

maltego.X509Certificate

w3snoop.com

Weight	0
Subject	w3snoop.com
Issuer	Let's Encrypt Authority X3
Subject DN	
Issuer DN	
SKI	8bbb47b373b03c0f3c1654bfe65d8b31161253a8
AKI	
Serial	336242b2eccd653d98fcddf75977b17ca9e
SAN	[*.w3snoop.com, w3snoop.com]
Usage	
Issuance ID	
Valid From	Thu Oct 01 00:00:00 GMT 2020
Valid Until	Wed Dec 30 00:00:00 GMT 2020
Country	
Organization	

Incoming (1)

DNS Name	w3snoop.com

SSL Certificate

maltego.X509Certificate

w3snoop.com

Weight	0
Subject	w3snoop.com
Issuer	R3
Subject DN	
Issuer DN	
SKI	6368b4b424d21c5186fcd5773ff1c0ab584867fa
AKI	
Serial	3d522f62451afd12b5be35f64fc8bed0af6
SAN	[*.w3snoop.com, w3snoop.com]
Usage	
Issuance ID	
Valid From	Thu Jul 29 00:00:00 GMT 2021
Valid Until	Wed Oct 27 00:00:00 GMT 2021
Country	
Organization	

Incoming (1)

DNS Name	w3snoop.com

SSL Certificate

maltego.X509Certificate

w3snoop.com

Weight	0
Subject	w3snoop.com
Issuer	Let's Encrypt Authority X3
Subject DN	
Issuer DN	
SKI	2f17a7770b501f725e22c88e9ac5f43fd0104715
AKI	
Serial	44921f382bfd58b2b57e14e86c013cd656a
SAN	[*.w3snoop.com, w3snoop.com]
Usage	
Issuance ID	
Valid From	Sun Aug 02 00:00:00 GMT 2020
Valid Until	Sat Oct 31 00:00:00 GMT 2020
Country	
Organization	

Incoming (1)

DNS Name	w3snoop.com

SSL Certificate

maltego.X509Certificate

w3snoop.com

Weight	0
Subject	w3snoop.com
Issuer	R3
Subject DN	
Issuer DN	
SKI	2f1ee27a1d398a9798e0935e67d7815801510925
AKI	
Serial	4fea1c86c8968088d56cf1b8dd05d48d5cb
SAN	[*.w3snoop.com, w3snoop.com]
Usage	
Issuance ID	
Valid From	Fri Jan 29 00:00:00 GMT 2021
Valid Until	Thu Apr 29 00:00:00 GMT 2021
Country	
Organization	

Incoming (1)

DNS Name	w3snoop.com

SSL Certificate

maltego.X509Certificate

w3snoop.com

Weight	0
Subject	w3snoop.com
Issuer	R3
Subject DN	
Issuer DN	
SKI	88423e9012b624795b86b7dca485e8da4bebe9c3
AKI	
Serial	3ad6f57ed0d38cc62b90eaeb63255bb9000
SAN	[*.w3snoop.com, w3snoop.com]
Usage	
Issuance ID	
Valid From	Wed Mar 31 00:00:00 GMT 2021
Valid Until	Tue Jun 29 00:00:00 GMT 2021
Country	
Organization	

Incoming (1)

DNS Name	w3snoop.com

SSL Certificate

maltego.X509Certificate

w3snoop.com

Weight	0
Subject	w3snoop.com
Issuer	Let's Encrypt Authority X3
Subject DN	
Issuer DN	
SKI	2a553be787a81957f51f9555078139d59b28e3fc
AKI	
Serial	3d2cee68d569140f2660089ac544f781c41
SAN	[*.ac.in.w3snoop.com, *.ac.uk.w3snoop.com, *.ae.w3snoop.com, *.at.w3snoop.com, *.az.w3snoop.com, *.be.w3snoop.com, *.bg.w3snoop.com, *.biz.w3snoop.com, *.by.w3snoop.com, *.ca.w3snoop.com, *.cc.w3snoop.com, *.ch.w3snoop.com, *.cl.w3snoop.com, *.cn.w3snoop.com, *.co.id.w3snoop.com, *.co.il.w3snoop.com, *.co.in.w3snoop.com, *.co.jp.w3snoop.com, *.co.kr.w3snoop.com, *.co.nz.w3snoop.com, *.co.uk.w3snoop.com, *.co.w3snoop.com, *.co.za.w3snoop.com, *.com.ar.w3snoop.com, *.com.au.w3snoop.com, *.com.br.w3snoop.com, *.com.cn.w3snoop.com, *.com.co.w3snoop.com, *.com.hk.w3snoop.com, *.com.mx.w3snoop.com, *.com.my.w3snoop.com, *.com.pk.w3snoop.com, *.com.pl.w3snoop.com, *.com.sg.w3snoop.com, *.com.tr.w3snoop.com, *.com.tw.w3snoop.com, *.com.ua.w3snoop.com, *.com.vn.w3snoop.com, *.com.w3snoop.com, *.cz.w3snoop.com, *.de.w3snoop.com, *.dk.w3snoop.com, *.edu.w3snoop.com, *.ee.w3snoop.com, *.es.w3snoop.com, *.eu.w3snoop.com, *.fi.w3snoop.com, *.fm.w3snoop.com, *.fr.w3snoop.com, *.gov.cn.w3snoop.com, *.gov.w3snoop.com, *.gr.w3snoop.com, *.hk.w3snoop.com, *.hr.w3snoop.com, *.hu.w3snoop.com, *.ie.w3snoop.com, *.in.w3snoop.com, *.info.w3snoop.com, *.io.w3snoop.com, *.ir.w3snoop.com, *.it.w3snoop.com, *.jp.w3snoop.com, *.kz.w3snoop.com, *.lt.w3snoop.com, *.lv.w3snoop.com, *.md.w3snoop.com, *.me.w3snoop.com, *.mobi.w3snoop.com, *.mx.w3snoop.com, *.name.w3snoop.com, *.ne.jp.w3snoop.com, *.net.au.w3snoop.com, *.net.w3snoop.com, *.nl.w3snoop.com, *.no.w3snoop.com, *.nu.w3snoop.com, *.or.jp.w3snoop.com, *.org.au.w3snoop.com, *.org.br.w3snoop.com, *.org.uk.w3snoop.com, *.org.w3snoop.com, *.pk.w3snoop.com, *.pl.w3snoop.com, *.pt.w3snoop.com, *.ro.w3snoop.com, *.rs.w3snoop.com, *.ru.w3snoop.com, *.se.w3snoop.com, *.si.w3snoop.com, *.sk.w3snoop.com, *.su.w3snoop.com, *.tk.w3snoop.com, *.to.w3snoop.com, *.tv.w3snoop.com, *.ua.w3snoop.com, *.us.w3snoop.com, *.vn.w3snoop.com, *.w3snoop.com, *.ws.w3snoop.com, w3snoop.com]
Usage	
Issuance ID	
Valid From	Sat Mar 28 00:00:00 GMT 2020
Valid Until	Fri Jun 26 00:00:00 GMT 2020
Country	
Organization	

Incoming (1)

DNS Name	w3snoop.com

SSL Certificate

maltego.X509Certificate

w3snoop.com

Weight	0
Subject	w3snoop.com
Issuer	Let's Encrypt Authority X3
Subject DN	
Issuer DN	
SKI	2a553be787a81957f51f9555078139d59b28e3fc
AKI	
Serial	46eb1f031bdc2cae7f3d746be75eeccec5f
SAN	[*.ac.in.w3snoop.com, *.ac.uk.w3snoop.com, *.ae.w3snoop.com, *.at.w3snoop.com, *.az.w3snoop.com, *.be.w3snoop.com, *.bg.w3snoop.com, *.biz.w3snoop.com, *.by.w3snoop.com, *.ca.w3snoop.com, *.cc.w3snoop.com, *.ch.w3snoop.com, *.cl.w3snoop.com, *.cn.w3snoop.com, *.co.id.w3snoop.com, *.co.il.w3snoop.com, *.co.in.w3snoop.com, *.co.jp.w3snoop.com, *.co.kr.w3snoop.com, *.co.nz.w3snoop.com, *.co.uk.w3snoop.com, *.co.w3snoop.com, *.co.za.w3snoop.com, *.com.ar.w3snoop.com, *.com.au.w3snoop.com, *.com.br.w3snoop.com, *.com.cn.w3snoop.com, *.com.co.w3snoop.com, *.com.hk.w3snoop.com, *.com.mx.w3snoop.com, *.com.my.w3snoop.com, *.com.pk.w3snoop.com, *.com.pl.w3snoop.com, *.com.sg.w3snoop.com, *.com.tr.w3snoop.com, *.com.tw.w3snoop.com, *.com.ua.w3snoop.com, *.com.vn.w3snoop.com, *.com.w3snoop.com, *.cz.w3snoop.com, *.de.w3snoop.com, *.dk.w3snoop.com, *.edu.w3snoop.com, *.ee.w3snoop.com, *.es.w3snoop.com, *.eu.w3snoop.com, *.fi.w3snoop.com, *.fm.w3snoop.com, *.fr.w3snoop.com, *.gov.cn.w3snoop.com, *.gov.w3snoop.com, *.gr.w3snoop.com, *.hk.w3snoop.com, *.hr.w3snoop.com, *.hu.w3snoop.com, *.ie.w3snoop.com, *.in.w3snoop.com, *.info.w3snoop.com, *.io.w3snoop.com, *.ir.w3snoop.com, *.it.w3snoop.com, *.jp.w3snoop.com, *.kz.w3snoop.com, *.lt.w3snoop.com, *.lv.w3snoop.com, *.md.w3snoop.com, *.me.w3snoop.com, *.mobi.w3snoop.com, *.mx.w3snoop.com, *.name.w3snoop.com, *.ne.jp.w3snoop.com, *.net.au.w3snoop.com, *.net.w3snoop.com, *.nl.w3snoop.com, *.no.w3snoop.com, *.nu.w3snoop.com, *.or.jp.w3snoop.com, *.org.au.w3snoop.com, *.org.br.w3snoop.com, *.org.uk.w3snoop.com, *.org.w3snoop.com, *.pk.w3snoop.com, *.pl.w3snoop.com, *.pt.w3snoop.com, *.ro.w3snoop.com, *.rs.w3snoop.com, *.ru.w3snoop.com, *.se.w3snoop.com, *.si.w3snoop.com, *.sk.w3snoop.com, *.su.w3snoop.com, *.tk.w3snoop.com, *.to.w3snoop.com, *.tv.w3snoop.com, *.ua.w3snoop.com, *.us.w3snoop.com, *.vn.w3snoop.com, *.w3snoop.com, *.ws.w3snoop.com, w3snoop.com]
Usage	
Issuance ID	
Valid From	Mon Jun 08 00:00:00 GMT 2020
Valid Until	Sun Sep 06 00:00:00 GMT 2020
Country	
Organization	

Incoming (1)

DNS Name	w3snoop.com

SSL Certificate

maltego.X509Certificate

w3snoop.com

Weight	0
Subject	w3snoop.com
Issuer	Let's Encrypt Authority X3
Subject DN	
Issuer DN	
SKI	2a553be787a81957f51f9555078139d59b28e3fc
AKI	
Serial	3af0af729afe30a620ee729d409e2696cc0
SAN	[*.ac.in.w3snoop.com, *.ac.uk.w3snoop.com, *.ae.w3snoop.com, *.at.w3snoop.com, *.az.w3snoop.com, *.be.w3snoop.com, *.bg.w3snoop.com, *.biz.w3snoop.com, *.by.w3snoop.com, *.ca.w3snoop.com, *.cc.w3snoop.com, *.ch.w3snoop.com, *.cl.w3snoop.com, *.cn.w3snoop.com, *.co.id.w3snoop.com, *.co.il.w3snoop.com, *.co.in.w3snoop.com, *.co.jp.w3snoop.com, *.co.kr.w3snoop.com, *.co.nz.w3snoop.com, *.co.uk.w3snoop.com, *.co.w3snoop.com, *.co.za.w3snoop.com, *.com.ar.w3snoop.com, *.com.au.w3snoop.com, *.com.br.w3snoop.com, *.com.cn.w3snoop.com, *.com.co.w3snoop.com, *.com.hk.w3snoop.com, *.com.mx.w3snoop.com, *.com.my.w3snoop.com, *.com.pk.w3snoop.com, *.com.pl.w3snoop.com, *.com.sg.w3snoop.com, *.com.tr.w3snoop.com, *.com.tw.w3snoop.com, *.com.ua.w3snoop.com, *.com.vn.w3snoop.com, *.com.w3snoop.com, *.cz.w3snoop.com, *.de.w3snoop.com, *.dk.w3snoop.com, *.edu.w3snoop.com, *.ee.w3snoop.com, *.es.w3snoop.com, *.eu.w3snoop.com, *.fi.w3snoop.com, *.fm.w3snoop.com, *.fr.w3snoop.com, *.gov.cn.w3snoop.com, *.gov.w3snoop.com, *.gr.w3snoop.com, *.hk.w3snoop.com, *.hr.w3snoop.com, *.hu.w3snoop.com, *.ie.w3snoop.com, *.in.w3snoop.com, *.info.w3snoop.com, *.io.w3snoop.com, *.ir.w3snoop.com, *.it.w3snoop.com, *.jp.w3snoop.com, *.kz.w3snoop.com, *.lt.w3snoop.com, *.lv.w3snoop.com, *.md.w3snoop.com, *.me.w3snoop.com, *.mobi.w3snoop.com, *.mx.w3snoop.com, *.name.w3snoop.com, *.ne.jp.w3snoop.com, *.net.au.w3snoop.com, *.net.w3snoop.com, *.nl.w3snoop.com, *.no.w3snoop.com, *.nu.w3snoop.com, *.or.jp.w3snoop.com, *.org.au.w3snoop.com, *.org.br.w3snoop.com, *.org.uk.w3snoop.com, *.org.w3snoop.com, *.pk.w3snoop.com, *.pl.w3snoop.com, *.pt.w3snoop.com, *.ro.w3snoop.com, *.rs.w3snoop.com, *.ru.w3snoop.com, *.se.w3snoop.com, *.si.w3snoop.com, *.sk.w3snoop.com, *.su.w3snoop.com, *.tk.w3snoop.com, *.to.w3snoop.com, *.tv.w3snoop.com, *.ua.w3snoop.com, *.us.w3snoop.com, *.vn.w3snoop.com, *.w3snoop.com, *.ws.w3snoop.com, w3snoop.com]
Usage	
Issuance ID	
Valid From	Fri Jan 03 00:00:00 GMT 2020
Valid Until	Thu Apr 02 00:00:00 GMT 2020
Country	
Organization	

Incoming (1)

DNS Name	w3snoop.com

SSL Certificate

maltego.X509Certificate

w3snoop.com

Weight	0
Subject	w3snoop.com
Issuer	R3
Subject DN	
Issuer DN	
SKI	16204939be3b4106837db76421cb2f3c9db2f95c
AKI	
Serial	38c7a6b0ecec8f3f7ad04cbdccf1adf5b8d
SAN	[*.w3snoop.com, w3snoop.com]
Usage	
Issuance ID	
Valid From	Sun May 30 00:00:00 GMT 2021
Valid Until	Sat Aug 28 00:00:00 GMT 2021
Country	
Organization	

Incoming (1)

DNS Name	w3snoop.com

SSL Certificate

maltego.X509Certificate

w3snoop.com

Weight	0
Subject	w3snoop.com
Issuer	Let's Encrypt Authority X3
Subject DN	
Issuer DN	
SKI	2a553be787a81957f51f9555078139d59b28e3fc
AKI	
Serial	4be80e199a0a2d58a5e421450ee5facb460
SAN	[*.ac.in.w3snoop.com, *.ac.uk.w3snoop.com, *.ae.w3snoop.com, *.at.w3snoop.com, *.az.w3snoop.com, *.be.w3snoop.com, *.bg.w3snoop.com, *.biz.w3snoop.com, *.by.w3snoop.com, *.ca.w3snoop.com, *.cc.w3snoop.com, *.ch.w3snoop.com, *.cl.w3snoop.com, *.cn.w3snoop.com, *.co.id.w3snoop.com, *.co.il.w3snoop.com, *.co.in.w3snoop.com, *.co.jp.w3snoop.com, *.co.kr.w3snoop.com, *.co.nz.w3snoop.com, *.co.uk.w3snoop.com, *.co.w3snoop.com, *.co.za.w3snoop.com, *.com.ar.w3snoop.com, *.com.au.w3snoop.com, *.com.br.w3snoop.com, *.com.cn.w3snoop.com, *.com.co.w3snoop.com, *.com.hk.w3snoop.com, *.com.mx.w3snoop.com, *.com.my.w3snoop.com, *.com.pk.w3snoop.com, *.com.pl.w3snoop.com, *.com.sg.w3snoop.com, *.com.tr.w3snoop.com, *.com.tw.w3snoop.com, *.com.ua.w3snoop.com, *.com.vn.w3snoop.com, *.com.w3snoop.com, *.cz.w3snoop.com, *.de.w3snoop.com, *.dk.w3snoop.com, *.edu.w3snoop.com, *.ee.w3snoop.com, *.es.w3snoop.com, *.eu.w3snoop.com, *.fi.w3snoop.com, *.fm.w3snoop.com, *.fr.w3snoop.com, *.gov.cn.w3snoop.com, *.gov.w3snoop.com, *.gr.w3snoop.com, *.hk.w3snoop.com, *.hr.w3snoop.com, *.hu.w3snoop.com, *.ie.w3snoop.com, *.in.w3snoop.com, *.info.w3snoop.com, *.io.w3snoop.com, *.ir.w3snoop.com, *.it.w3snoop.com, *.jp.w3snoop.com, *.kz.w3snoop.com, *.lt.w3snoop.com, *.lv.w3snoop.com, *.md.w3snoop.com, *.me.w3snoop.com, *.mobi.w3snoop.com, *.mx.w3snoop.com, *.name.w3snoop.com, *.ne.jp.w3snoop.com, *.net.au.w3snoop.com, *.net.w3snoop.com, *.nl.w3snoop.com, *.no.w3snoop.com, *.nu.w3snoop.com, *.or.jp.w3snoop.com, *.org.au.w3snoop.com, *.org.br.w3snoop.com, *.org.uk.w3snoop.com, *.org.w3snoop.com, *.pk.w3snoop.com, *.pl.w3snoop.com, *.pt.w3snoop.com, *.ro.w3snoop.com, *.rs.w3snoop.com, *.ru.w3snoop.com, *.se.w3snoop.com, *.si.w3snoop.com, *.sk.w3snoop.com, *.su.w3snoop.com, *.tk.w3snoop.com, *.to.w3snoop.com, *.tv.w3snoop.com, *.ua.w3snoop.com, *.us.w3snoop.com, *.vn.w3snoop.com, *.w3snoop.com, *.ws.w3snoop.com, w3snoop.com]
Usage	
Issuance ID	
Valid From	Tue Oct 29 00:00:00 GMT 2019
Valid Until	Mon Jan 27 00:00:00 GMT 2020
Country	
Organization	

Incoming (1)

DNS Name	w3snoop.com

Person

maltego.Person

GoDaddy.com, LLC

Weight	100
Full Name	GoDaddy.com, LLC
First Names	
Surname	

Incoming (1)

Domain	w3snoop.com

Company

maltego.Company

Domains By Proxy, LLC

Weight	100
Name	Domains By Proxy, LLC

Incoming (1)

Domain	w3snoop.com

Location

maltego.Location

Tempe, US

Weight	66
Name	Tempe, US
Country	US
City	Tempe
Street Address	DomainsByProxy.com
Area	
Area Code	85284
Country Code	
Longitude	0.0
Latitude	0.0

Info

Relevance:	0.321451
Count:	3

Incoming (1)

Domain	w3snoop.com

Domain

maltego.Domain

ws.w3snoop.com

Weight	0
Domain Name	ws.w3snoop.com
WHOIS Info	Admin City: Tempe Admin Country: US Admin Email: c9b5a1cf1d0c3764s@domainsbyproxy.com Admin Organization: Domains By Proxy, LLC Admin Postal Code: 85284 Admin State/Province: Arizona Creation Date: 2011-06-05T21:04:22Z Creation Date: 2011-06-06T02:04:22Z DNSSEC: unsigned Domain Name: W3SNOOP.COM Domain Status: clientDeleteProhibited http://www.icann.org/epp#clientDeleteProhibited Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited Domain Status: clientRenewProhibited http://www.icann.org/epp#clientRenewProhibited Domain Status: clientRenewProhibited https://icann.org/epp#clientRenewProhibited Domain Status: clientTransferProhibited http://www.icann.org/epp#clientTransferProhibited Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Domain Status: clientUpdateProhibited http://www.icann.org/epp#clientUpdateProhibited Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited Name Server: INDRI.EZOICNS.COM Name Server: SAOLA.EZOICNS.COM Registrant City: a7319ae5e6c95df5 Registrant Country: US Registrant Email: c9b5a1cf1d0c3764s@domainsbyproxy.com Registrant Fax Ext: 3432650ec337c945 Registrant Fax: 9fad764be0c7e95d Registrant Name: 80315b2e6ac1a801 Registrant Organization: b46a98a26fe2fd9f Registrant Phone Ext: 3432650ec337c945 Registrant Phone: d5f66d3a005b000d Registrant Postal Code: 052e5bd148f904f9 Registrant State/Province: 30bdd2917a604c83 Registrant Street: 037792fd5a6fe619 Registrant Street: d733533b6a6c0c21 Registrar Abuse Contact Email: abuse@godaddy.com Registrar Abuse Contact Phone: +1.4806242505 Registrar Abuse Contact Phone: 480-624-2505 Registrar IANA ID: 146 Registrar Registration Expiration Date: 2023-06-05T21:04:22Z Registrar URL: http://www.godaddy.com Registrar WHOIS Server: whois.godaddy.com Registrar: GoDaddy.com, LLC Registry Admin ID: Not Available From Registry Registry Domain ID: 1660071767_DOMAIN_COM-VRSN Registry Expiry Date: 2023-06-06T02:04:22Z Registry Registrant ID: Not Available From Registry Registry Tech ID: Not Available From Registry Tech City: Tempe Tech Country: US Tech Email: c9b5a1cf1d0c3764s@domainsbyproxy.com Tech Organization: Domains By Proxy, LLC Tech Postal Code: 85284 Tech State/Province: Arizona Updated Date: 2020-02-09T21:49:40Z Updated Date: 2020-02-10T04:49:41Z

VirusTotal Domain Summary

VirusTotal Reputation	0
Tags	

VirusTotal Analysis Summary	
Aggregate Result	harmless - 80 / 88

VirusTotal Analysis Stats	
Analysis Type	Number of Analysis
Confirmed Timeout	0
Failure	0
Harmless	80
Malicious	0
Suspicious	0
Timeout	0
Type Unsupported	0
Undetected	8
Total	**88**

View on VirusTotal

GUI Url: https://www.virustotal.com/gui/domain/ws.w3snoop.com

Categories	
Engines	Category
Forcepoint ThreatSeeker	information technology
BitDefender	business

Community Votes

Total votes cast: 0

Incoming (1)

DNS Name	apitwitter.com.w3snoop.com

DNS Name

maltego.DNSName

*.pl.w3snoop.com

Weight	0
DNS Name	*.pl.w3snoop.com

Incoming (1)

DNS Name	w3snoop.com

IPv4 Address

maltego.IPv4Address

18.159.80.129

Weight	0
IP Address	18.159.80.129
Internal	false

Incoming (1)

DNS Name	apitwitter.com.w3snoop.com

VirusTotal Category

maltego.virustotal.Category

information technology

Weight	0
Text	information technology
Partner Name	Sophos

Incoming (1)

DNS Name	w3snoop.com

VirusTotal Category

maltego.virustotal.Category

hobbies

Weight	0
Text	hobbies
Partner Name	BitDefender

Incoming (1)

DNS Name	www.evil.com

VirusTotal Category

maltego.virustotal.Category

entertainment

Weight	0
Text	entertainment
Partner Name	Forcepoint ThreatSeeker

Incoming (1)

DNS Name	www.evil.com

VirusTotal Category

maltego.virustotal.Category

Entertainment

Weight	0
Text	Entertainment
Partner Name	alphaMountain.ai

Incoming (1)

DNS Name	evil.com

Domain

maltego.Domain

box.evil.co

Weight	0
Domain Name	box.evil.co
WHOIS Info	Admin City: REDACTED FOR PRIVACY Admin Country: REDACTED FOR PRIVACY Admin Organization: REDACTED FOR PRIVACY Admin Postal Code: REDACTED FOR PRIVACY Admin State/Province: REDACTED FOR PRIVACY Creation Date: 2019-10-05T17:00:14Z DNSSEC: unsigned Domain Name: evil.co Domain Status: clientDeleteProhibited http://www.icann.org/epp#clientDeleteProhibited Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited Domain Status: clientRenewProhibited http://www.icann.org/epp#clientRenewProhibited Domain Status: clientRenewProhibited https://icann.org/epp#clientRenewProhibited Domain Status: clientTransferProhibited http://www.icann.org/epp#clientTransferProhibited Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Domain Status: clientUpdateProhibited http://www.icann.org/epp#clientUpdateProhibited Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited Name Server: NS1.UNIREGISTRYMARKET.LINK Name Server: NS2.UNIREGISTRYMARKET.LINK Name Server: ns1.uniregistrymarket.link Name Server: ns2.uniregistrymarket.link Registrant City: 1f8f4166599d23ee Registrant Country: US Registrant Email: 44f8172ee385b60bs@ Registrant Email: f651612a2f356ad3s@ Registrant Fax Ext: 1f8f4166599d23ee Registrant Fax: 1f8f4166599d23ee Registrant Name: 1f8f4166599d23ee Registrant Organization: 3432650ec337c945 Registrant Phone Ext: 1f8f4166599d23ee Registrant Phone: 1f8f4166599d23ee Registrant Postal Code: 1f8f4166599d23ee Registrant State/Province: c5117919ef41a795 Registrant Street: 1f8f4166599d23ee Registrar Abuse Contact Email: abuse@godaddy.com Registrar Abuse Contact Phone: +1.4806242505 Registrar IANA ID: 146 Registrar Registration Expiration Date: 2022-10-05T17:00:14Z Registrar URL: http://www.godaddy.com Registrar URL: whois.godaddy.com Registrar WHOIS Server: whois.godaddy.com Registrar: GoDaddy.com, LLC Registry Admin ID: REDACTED FOR PRIVACY Registry Domain ID: D8A750721BA904C4A90CFDA260DBE314E-NSR Registry Expiry Date: 2022-10-05T17:00:14Z Registry Registrant ID: REDACTED FOR PRIVACY Registry Tech ID: REDACTED FOR PRIVACY Tech City: REDACTED FOR PRIVACY Tech Country: REDACTED FOR PRIVACY Tech Organization: REDACTED FOR PRIVACY Tech Postal Code: REDACTED FOR PRIVACY Tech State/Province: REDACTED FOR PRIVACY Updated Date: 2021-06-17T12:14:42Z Updated Date: 2021-06-22T19:14:40Z

VirusTotal Domain Summary

VirusTotal Reputation	0
Tags	

VirusTotal Analysis Summary

Aggregate Result	harmless - 86 / 86

VirusTotal Analysis Stats

Analysis Type	Number of Analysis
Confirmed Timeout	0
Failure	0
Harmless	86
Malicious	0
Suspicious	0
Timeout	0
Type Unsupported	0
Undetected	0
Total	**86**

View on VirusTotal

GUI Url: https://www.virustotal.com/gui/domain/box.evil.co

Community Votes

Total votes cast: 0

Incoming (1)

DNS Name	evil.co

VirusTotal File

maltego.virustotal.File

all_data.tar

Weight	0
MeaningfulName	all_data.tar
File Id	4906fca1ee4b3ca7a60c00ade5e0014758b3e4c84a566bf25187471b5e9dd6eb
Names	all_data.tar
File Type	TAR
File Type Description	TAR
MD5	572dab5da157d2207ccc2cf05932ae7b
SHA-1	675bfeaf57ab02e541d1a9ae99d5a0b0a0be0ea5
SHA-256	4906fca1ee4b3ca7a60c00ade5e0014758b3e4c84a566bf25187471b5e9dd6eb
Vhash	3fcf1cb291a059acad36bf35d2e13142
Authentihash	
SSDEEP	24576:fUem3zLCH2SgXGyxVU3wkYOc9EDJWo205YkdxHxDRXzQMCD1bhkP92mrO:O3CH2SgXGyxRkYNywV0H5dclsBrO
Magic	POSIX tar archive (GNU)
File Size	10593105
Tags	tar
Capability Tags	
Downloadable	null
Creation Date	
First Submission Date	2020-11-07T09:38:15Z
Last Submission Date	2020-11-07T09:38:15Z
Last Analysis Date	2020-11-07T11:38:36Z
Total Votes - Harmless	0
Total Votes - Malicious	0
Submissions	1
Reputation	0

View on VirusTotal

GUI Url:
https://www.virustotal.com/gui/file/4906fca1ee4b3ca7a60c00ade5e0014758b3e4c84a566bf25187471b5e9dd6eb

File Summary

Names	all_data.tar
File Type	tar
File Type Description	TAR
Tags	tar
Times Submitted	1

TrID - file type identification tool

File Type	Probability %
TAR - Tape ARchive (GNU)	62.9
TAR - Tape ARchive (directory)	37.0

VirusTotal Analysis Summary

Aggregate Result	undetected - 53 / 75

VirusTotal Analysis Stats

Analysis Type	Number of Analysis
Confirmed Timeout	0
Failure	1
Harmless	0
Malicious	8
Suspicious	0
Timeout	0
Type Unsupported	13
Undetected	53
Total	**75**

Community Votes

Total votes cast: 0

Incoming (1)

	DNS Name	www.evil.com

Domain

maltego.Domain

pop3.evil.co

Weight	0
Domain Name	pop3.evil.co
WHOIS Info	Admin City: REDACTED FOR PRIVACY Admin Country: REDACTED FOR PRIVACY Admin Organization: REDACTED FOR PRIVACY Admin Postal Code: REDACTED FOR PRIVACY Admin State/Province: REDACTED FOR PRIVACY Creation Date: 2019-10-05T17:00:14Z DNSSEC: unsigned Domain Name: evil.co Domain Status: clientDeleteProhibited http://www.icann.org/epp#clientDeleteProhibited Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited Domain Status: clientRenewProhibited http://www.icann.org/epp#clientRenewProhibited Domain Status: clientRenewProhibited https://icann.org/epp#clientRenewProhibited Domain Status: clientTransferProhibited http://www.icann.org/epp#clientTransferProhibited Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Domain Status: clientUpdateProhibited http://www.icann.org/epp#clientUpdateProhibited Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited Name Server: NS1.UNIREGISTRYMARKET.LINK Name Server: NS2.UNIREGISTRYMARKET.LINK Name Server: ns1.uniregistrymarket.link Name Server: ns2.uniregistrymarket.link Registrant City: 1f8f4166599d23ee Registrant Country: US Registrant Email: 44f8172ee385b60bs@ Registrant Email: f651612a2f356ad3s@ Registrant Fax Ext: 1f8f4166599d23ee Registrant Fax: 1f8f4166599d23ee Registrant Name: 1f8f4166599d23ee Registrant Organization: 3432650ec337c945 Registrant Phone Ext: 1f8f4166599d23ee Registrant Phone: 1f8f4166599d23ee Registrant Postal Code: 1f8f4166599d23ee Registrant State/Province: c5117919ef41a795 Registrant Street: 1f8f4166599d23ee Registrar Abuse Contact Email: abuse@godaddy.com Registrar Abuse Contact Phone: +1.4806242505 Registrar IANA ID: 146 Registrar Registration Expiration Date: 2022-10-05T17:00:14Z Registrar URL: http://www.godaddy.com Registrar URL: whois.godaddy.com Registrar WHOIS Server: whois.godaddy.com Registrar: GoDaddy.com, LLC Registry Admin ID: REDACTED FOR PRIVACY Registry Domain ID: D8A750721BA904C4A90CFDA260DBE314E-NSR Registry Expiry Date: 2022-10-05T17:00:14Z Registry Registrant ID: REDACTED FOR PRIVACY Registry Tech ID: REDACTED FOR PRIVACY Tech City: REDACTED FOR PRIVACY Tech Country: REDACTED FOR PRIVACY Tech Organization: REDACTED FOR PRIVACY Tech Postal Code: REDACTED FOR PRIVACY Tech State/Province: REDACTED FOR PRIVACY Updated Date: 2021-06-17T12:14:42Z Updated Date: 2021-06-22T19:14:40Z

VirusTotal Domain Summary

VirusTotal Reputation	0
Tags	

VirusTotal Analysis Summary

Aggregate Result	harmless - 86 / 86

VirusTotal Analysis Stats

Analysis Type	Number of Analysis
Confirmed Timeout	0
Failure	0
Harmless	86
Malicious	0
Suspicious	0
Timeout	0
Type Unsupported	0
Undetected	0
Total	**86**

View on VirusTotal

GUI Url: https://www.virustotal.com/gui/domain/pop3.evil.co

Community Votes

Total votes cast: 0

Incoming (1)

DNS Name	evil.co

Domain

maltego.Domain

poczta.evil.co

Weight	0
Domain Name	poczta.evil.co
WHOIS Info	Admin City: REDACTED FOR PRIVACY Admin Country: REDACTED FOR PRIVACY Admin Organization: REDACTED FOR PRIVACY Admin Postal Code: REDACTED FOR PRIVACY Admin State/Province: REDACTED FOR PRIVACY Creation Date: 2019-10-05T17:00:14Z DNSSEC: unsigned Domain Name: evil.co Domain Status: clientDeleteProhibited http://www.icann.org/epp#clientDeleteProhibited Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited Domain Status: clientRenewProhibited http://www.icann.org/epp#clientRenewProhibited Domain Status: clientRenewProhibited https://icann.org/epp#clientRenewProhibited Domain Status: clientTransferProhibited http://www.icann.org/epp#clientTransferProhibited Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Domain Status: clientUpdateProhibited http://www.icann.org/epp#clientUpdateProhibited Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited Name Server: NS1.UNIREGISTRYMARKET.LINK Name Server: NS2.UNIREGISTRYMARKET.LINK Name Server: ns1.uniregistrymarket.link Name Server: ns2.uniregistrymarket.link Registrant City: 1f8f4166599d23ee Registrant Country: US Registrant Email: 44f8172ee385b60bs@ Registrant Email: f651612a2f356ad3s@ Registrant Fax Ext: 1f8f4166599d23ee Registrant Fax: 1f8f4166599d23ee Registrant Name: 1f8f4166599d23ee Registrant Organization: 3432650ec337c945 Registrant Phone Ext: 1f8f4166599d23ee Registrant Phone: 1f8f4166599d23ee Registrant Postal Code: 1f8f4166599d23ee Registrant State/Province: c5117919ef41a795 Registrant Street: 1f8f4166599d23ee Registrar Abuse Contact Email: abuse@godaddy.com Registrar Abuse Contact Phone: +1.4806242505 Registrar IANA ID: 146 Registrar Registration Expiration Date: 2022-10-05T17:00:14Z Registrar URL: http://www.godaddy.com Registrar URL: whois.godaddy.com Registrar WHOIS Server: whois.godaddy.com Registrar: GoDaddy.com, LLC Registry Admin ID: REDACTED FOR PRIVACY Registry Domain ID: D8A750721BA904C4A90CFDA260DBE314E-NSR Registry Expiry Date: 2022-10-05T17:00:14Z Registry Registrant ID: REDACTED FOR PRIVACY Registry Tech ID: REDACTED FOR PRIVACY Tech City: REDACTED FOR PRIVACY Tech Country: REDACTED FOR PRIVACY Tech Organization: REDACTED FOR PRIVACY Tech Postal Code: REDACTED FOR PRIVACY Tech State/Province: REDACTED FOR PRIVACY Updated Date: 2021-06-17T12:14:42Z Updated Date: 2021-06-22T19:14:40Z

VirusTotal Domain Summary

VirusTotal Reputation	0
Tags	

VirusTotal Analysis Summary

Aggregate Result	harmless - 86 / 86

VirusTotal Analysis Stats

Analysis Type	Number of Analysis
Confirmed Timeout	0
Failure	0
Harmless	86
Malicious	0
Suspicious	0
Timeout	0
Type Unsupported	0
Undetected	0
Total	**86**

View on VirusTotal

GUI Url: https://www.virustotal.com/gui/domain/poczta.evil.co

Community Votes

Total votes cast: 0

Incoming (1)

DNS Name evil.co

VirusTotal File

maltego.virustotal.File

web hacking tutorial.doc

Weight	0
MeaningfulName	web hacking tutorial.doc
File Id	800af2fec6f3bad6cd796fc775f607db18ba29f0bb38962470fa84fc8b1b2ddc
Names	web hacking tutorial.doc
File Type	DOC
File Type Description	MS Word Document
MD5	1e3e1ea6c3ebfed593d8c420fb910b3e
SHA-1	f90841d6d4e9a2e8103f80c5cb4a4dd1bad7a6ba
SHA-256	800af2fec6f3bad6cd796fc775f607db18ba29f0bb38962470fa84fc8b1b2ddc
Vhash	3aaae21f66199ad073e3af07b66d011d
Authentihash	
SSDEEP	768:u1S8L9mMUn9IrGKHhxqANkdYibEsI5t+tCD:u1z9m7n9Irhh4ANgYidIbi
Magic	CDF V2 Document, Little Endian, Os: Windows, Version 5.1, Code page: 1252, Author: Khurram Shahzad Kazmi, Template: Normal.dot, Last Saved By: Khurram Shahzad Kazmi, Revision Number: 3, Name of Creating Application: Microsoft Office Word, Total Editing Time: 01:00, Create Time/Date: Thu Nov 25 23:19:00 2010, Last Saved Time/Date: Thu Nov 25 23:20:00 2010, Number of Pages: 1, Number of Words: 3681, Number of Characters: 20988, Security: 0
File Size	78848
Tags	doc
Capability Tags	
Downloadable	null
Creation Date	2010-11-26T23:19Z
First Submission Date	2021-02-07T22:25:59Z
Last Submission Date	2021-02-07T22:25:59Z
Last Analysis Date	2021-02-16T13:33:12Z
Total Votes - Harmless	0
Total Votes - Malicious	0
Submissions	1
Reputation	0

View on VirusTotal

GUI Url:
https://www.virustotal.com/gui/file/800af2fec6f3bad6cd796fc775f607db18ba29f0bb38962470fa84fc8b1b2ddc

File Summary

Names	web hacking tutorial.doc
File Type	doc
File Type Description	MS Word Document
Tags	doc
Times Submitted	1

TrID - file type identification tool

File Type	Probability %
Microsoft Word document	78.9
Generic OLE2 / Multistream Compound	21.0

VirusTotal Analysis Summary	
Aggregate Result	undetected - 60 / 75

VirusTotal Analysis Stats	
Analysis Type	Number of Analysis
Confirmed Timeout	0
Failure	0
Harmless	0
Malicious	1
Suspicious	0
Timeout	0
Type Unsupported	14
Undetected	60
Total	**75**

Community Votes

Total votes cast: 0

Incoming (1)

DNS Name	www.evil.com

Domain

maltego.Domain

imap1.evil.co

Weight	0
Domain Name	imap1.evil.co
WHOIS Info	Admin City: REDACTED FOR PRIVACY Admin Country: REDACTED FOR PRIVACY Admin Organization: REDACTED FOR PRIVACY Admin Postal Code: REDACTED FOR PRIVACY Admin State/Province: REDACTED FOR PRIVACY Creation Date: 2019-10-05T17:00:14Z DNSSEC: unsigned Domain Name: evil.co Domain Status: clientDeleteProhibited http://www.icann.org/epp#clientDeleteProhibited Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited Domain Status: clientRenewProhibited http://www.icann.org/epp#clientRenewProhibited Domain Status: clientRenewProhibited https://icann.org/epp#clientRenewProhibited Domain Status: clientTransferProhibited http://www.icann.org/epp#clientTransferProhibited Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Domain Status: clientUpdateProhibited http://www.icann.org/epp#clientUpdateProhibited Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited Name Server: NS1.UNIREGISTRYMARKET.LINK Name Server: NS2.UNIREGISTRYMARKET.LINK Name Server: ns1.uniregistrymarket.link Name Server: ns2.uniregistrymarket.link Registrant City: 1f8f4166599d23ee Registrant Country: US Registrant Email: 44f8172ee385b60bs@ Registrant Email: f651612a2f356ad3s@ Registrant Fax Ext: 1f8f4166599d23ee Registrant Fax: 1f8f4166599d23ee Registrant Name: 1f8f4166599d23ee Registrant Organization: 3432650ec337c945 Registrant Phone Ext: 1f8f4166599d23ee Registrant Phone: 1f8f4166599d23ee Registrant Postal Code: 1f8f4166599d23ee Registrant State/Province: c5117919ef41a795 Registrant Street: 1f8f4166599d23ee Registrar Abuse Contact Email: abuse@godaddy.com Registrar Abuse Contact Phone: +1.4806242505 Registrar IANA ID: 146 Registrar Registration Expiration Date: 2022-10-05T17:00:14Z Registrar URL: http://www.godaddy.com Registrar URL: whois.godaddy.com Registrar WHOIS Server: whois.godaddy.com Registrar: GoDaddy.com, LLC Registry Admin ID: REDACTED FOR PRIVACY Registry Domain ID: D8A750721BA904C4A90CFDA260DBE314E-NSR Registry Expiry Date: 2022-10-05T17:00:14Z Registry Registrant ID: REDACTED FOR PRIVACY Registry Tech ID: REDACTED FOR PRIVACY Tech City: REDACTED FOR PRIVACY Tech Country: REDACTED FOR PRIVACY Tech Organization: REDACTED FOR PRIVACY Tech Postal Code: REDACTED FOR PRIVACY Tech State/Province: REDACTED FOR PRIVACY Updated Date: 2021-06-17T12:14:42Z Updated Date: 2021-06-22T19:14:40Z

VirusTotal Domain Summary

VirusTotal Reputation	0
Tags	

VirusTotal Analysis Summary

Aggregate Result	harmless - 86 / 86

VirusTotal Analysis Stats

Analysis Type	Number of Analysis
Confirmed Timeout	0
Failure	0
Harmless	86
Malicious	0
Suspicious	0
Timeout	0
Type Unsupported	0
Undetected	0
Total	**86**

View on VirusTotal

GUI Url: https://www.virustotal.com/gui/domain/imap1.evil.co

Community Votes

Total votes cast: 0

Incoming (1)

DNS Name	evil.co

VirusTotal File

maltego.virustotal.File

code-editor-master.tar

Weight	0
MeaningfulName	code-editor-master.tar
File Id	e523fc36d84219f5d83709cc78f2d0e5a627ac1c4637ee647b2ad747b15008fb
Names	code-editor-master.tar
File Type	TAR
File Type Description	TAR
MD5	64d183d438098b699dd5a768f7dcfec4
SHA-1	22815b375b3ca4a1fedc6e992c62a33192e1f6de
SHA-256	e523fc36d84219f5d83709cc78f2d0e5a627ac1c4637ee647b2ad747b15008fb
Vhash	65b3e7259cf1cc1c4f8f065137a6922a
Authentihash	
SSDEEP	393216:c19sqejCkuXQrfGZ3U42K5nm2XfDyr5xkzDyr5xU:c0zjVuXOfklL5nm2Wr5xTr5x
Magic	POSIX tar archive
File Size	38906880
Tags	tar
Capability Tags	
Downloadable	null
Creation Date	
First Submission Date	2021-01-11T05:00:26Z
Last Submission Date	2021-01-11T05:00:26Z
Last Analysis Date	2021-01-11T08:33:20Z
Total Votes - Harmless	0
Total Votes - Malicious	0
Submissions	1
Reputation	0

View on VirusTotal

GUI Url:
https://www.virustotal.com/gui/file/e523fc36d84219f5d83709cc78f2d0e5a627ac1c4637ee647b2ad747b15008fb

File Summary

Names	code-editor-master.tar
File Type	tar
File Type Description	TAR
Tags	tar
Times Submitted	1

TrID - file type identification tool

File Type	Probability %
Obfuscated subsetted Font	99.8
TAR - Tape ARchive (POSIX)	0.0
TAR - Tape ARchive (directory)	0.0

VirusTotal Analysis Summary	
Aggregate Result	undetected - 56 / 75

VirusTotal Analysis Stats	
Analysis Type	Number of Analysis
Confirmed Timeout	0
Failure	2
Harmless	0
Malicious	1
Suspicious	0
Timeout	1
Type Unsupported	15
Undetected	56
Total	**75**

Community Votes

Total votes cast: 0

Incoming (1)

DNS Name	www.evil.com

Domain

maltego.Domain

mx.evil.co

Weight	0
Domain Name	mx.evil.co
WHOIS Info	Admin City: REDACTED FOR PRIVACY Admin Country: REDACTED FOR PRIVACY Admin Organization: REDACTED FOR PRIVACY Admin Postal Code: REDACTED FOR PRIVACY Admin State/Province: REDACTED FOR PRIVACY Creation Date: 2019-10-05T17:00:14Z DNSSEC: unsigned Domain Name: evil.co Domain Status: clientDeleteProhibited http://www.icann.org/epp#clientDeleteProhibited Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited Domain Status: clientRenewProhibited http://www.icann.org/epp#clientRenewProhibited Domain Status: clientRenewProhibited https://icann.org/epp#clientRenewProhibited Domain Status: clientTransferProhibited http://www.icann.org/epp#clientTransferProhibited Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Domain Status: clientUpdateProhibited http://www.icann.org/epp#clientUpdateProhibited Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited Name Server: NS1.UNIREGISTRYMARKET.LINK Name Server: NS2.UNIREGISTRYMARKET.LINK Name Server: ns1.uniregistrymarket.link Name Server: ns2.uniregistrymarket.link Registrant City: 1f8f4166599d23ee Registrant Country: US Registrant Email: 44f8172ee385b60bs@ Registrant Email: f651612a2f356ad3s@ Registrant Fax Ext: 1f8f4166599d23ee Registrant Fax: 1f8f4166599d23ee Registrant Name: 1f8f4166599d23ee Registrant Organization: 3432650ec337c945 Registrant Phone Ext: 1f8f4166599d23ee Registrant Phone: 1f8f4166599d23ee Registrant Postal Code: 1f8f4166599d23ee Registrant State/Province: c5117919ef41a795 Registrant Street: 1f8f4166599d23ee Registrar Abuse Contact Email: abuse@godaddy.com Registrar Abuse Contact Phone: +1.4806242505 Registrar IANA ID: 146 Registrar Registration Expiration Date: 2022-10-05T17:00:14Z Registrar URL: http://www.godaddy.com Registrar URL: whois.godaddy.com Registrar WHOIS Server: whois.godaddy.com Registrar: GoDaddy.com, LLC Registry Admin ID: REDACTED FOR PRIVACY Registry Domain ID: D8A750721BA904C4A90CFDA260DBE314E-NSR Registry Expiry Date: 2022-10-05T17:00:14Z Registry Registrant ID: REDACTED FOR PRIVACY Registry Tech ID: REDACTED FOR PRIVACY Tech City: REDACTED FOR PRIVACY Tech Country: REDACTED FOR PRIVACY Tech Organization: REDACTED FOR PRIVACY Tech Postal Code: REDACTED FOR PRIVACY Tech State/Province: REDACTED FOR PRIVACY Updated Date: 2021-06-17T12:14:42Z Updated Date: 2021-06-22T19:14:40Z

VirusTotal Domain Summary

VirusTotal Reputation	0
Tags	

VirusTotal Analysis Summary

Aggregate Result	harmless - 86 / 86

VirusTotal Analysis Stats

Analysis Type	Number of Analysis
Confirmed Timeout	0
Failure	0
Harmless	86
Malicious	0
Suspicious	0
Timeout	0
Type Unsupported	0
Undetected	0
Total	**86**

View on VirusTotal

GUI Url: https://www.virustotal.com/gui/domain/mx.evil.co

Community Votes

Total votes cast: 0

Incoming (1)

DNS Name	evil.co

VirusTotal File

maltego.virustotal.File

25c55cd1571c3bab3a1db71f26d7b20c4c4f0ae46374f0db251c2febaf0cd9e6

Weight	0
MeaningfulName	25c55cd1571c3bab3a1db71f26d7b20c4c4f0ae46374f0db251c2febaf0cd9e6
File Id	25c55cd1571c3bab3a1db71f26d7b20c4c4f0ae46374f0db251c2febaf0cd9e6
Names	
File Type	XML
File Type Description	XML
MD5	b83f4fdf2fac9e4b5930bbdab45acfce
SHA-1	6cac8e4a8dc6721c00aec8c9081dc9a7c87ad27c
SHA-256	25c55cd1571c3bab3a1db71f26d7b20c4c4f0ae46374f0db251c2febaf0cd9e6
Vhash	
Authentihash	
SSDEEP	6144:Vu0KwZ/Bwr79Uh/AM5DaR6RbMpP3by6S7EA8xft9X8aJtY2fpUX0u1zcDosx:VuvwZ/Bwr7XP35ZxV9XJJtU0uZ8oC
Magic	XML document text
File Size	553088
Tags	xml
Capability Tags	
Downloadable	null
Creation Date	
First Submission Date	2021-03-10T17:18:39Z
Last Submission Date	2021-03-10T17:18:39Z
Last Analysis Date	2021-03-10T19:19:40Z
Total Votes - Harmless	0
Total Votes - Malicious	0
Submissions	1
Reputation	0

View on VirusTotal

GUI Url:
https://www.virustotal.com/gui/file/25c55cd1571c3bab3a1db71f26d7b20c4c4f0ae46374f0db251c2febaf0cd9e6

File Summary

Names	
File Type	xml
File Type Description	XML
Tags	xml
Times Submitted	1

TrID - file type identification tool

File Type	Probability %
Scalable Vector Graphics (var.3)	52.7
Synchronized Multimedia Integration Language	18.1
Generic XML (ASCII)	18.1
HyperText Markup Language	10.9

VirusTotal Analysis Summary	
Aggregate Result	undetected - 53 / 74

VirusTotal Analysis Stats	
Analysis Type	Number of Analysis
Confirmed Timeout	0
Failure	1
Harmless	0
Malicious	4
Suspicious	0
Timeout	0
Type Unsupported	16
Undetected	53
Total	**74**

Community Votes

Total votes cast: 0

Incoming (1)

	DNS Name	www.evil.com

Domain

maltego.Domain

mailrelay.evil.co

Weight	0
Domain Name	mailrelay.evil.co
WHOIS Info	Admin City: REDACTED FOR PRIVACY Admin Country: REDACTED FOR PRIVACY Admin Organization: REDACTED FOR PRIVACY Admin Postal Code: REDACTED FOR PRIVACY Admin State/Province: REDACTED FOR PRIVACY Creation Date: 2019-10-05T17:00:14Z DNSSEC: unsigned Domain Name: evil.co Domain Status: clientDeleteProhibited http://www.icann.org/epp#clientDeleteProhibited Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited Domain Status: clientRenewProhibited http://www.icann.org/epp#clientRenewProhibited Domain Status: clientRenewProhibited https://icann.org/epp#clientRenewProhibited Domain Status: clientTransferProhibited http://www.icann.org/epp#clientTransferProhibited Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Domain Status: clientUpdateProhibited http://www.icann.org/epp#clientUpdateProhibited Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited Name Server: NS1.UNIREGISTRYMARKET.LINK Name Server: NS2.UNIREGISTRYMARKET.LINK Name Server: ns1.uniregistrymarket.link Name Server: ns2.uniregistrymarket.link Registrant City: 1f8f4166599d23ee Registrant Country: US Registrant Email: 44f8172ee385b60bs@ Registrant Email: f651612a2f356ad3s@ Registrant Fax Ext: 1f8f4166599d23ee Registrant Fax: 1f8f4166599d23ee Registrant Name: 1f8f4166599d23ee Registrant Organization: 3432650ec337c945 Registrant Phone Ext: 1f8f4166599d23ee Registrant Phone: 1f8f4166599d23ee Registrant Postal Code: 1f8f4166599d23ee Registrant State/Province: c5117919ef41a795 Registrant Street: 1f8f4166599d23ee Registrar Abuse Contact Email: abuse@godaddy.com Registrar Abuse Contact Phone: +1.4806242505 Registrar IANA ID: 146 Registrar Registration Expiration Date: 2022-10-05T17:00:14Z Registrar URL: http://www.godaddy.com Registrar URL: whois.godaddy.com Registrar WHOIS Server: whois.godaddy.com Registrar: GoDaddy.com, LLC Registry Admin ID: REDACTED FOR PRIVACY Registry Domain ID: D8A750721BA904C4A90CFDA260DBE314E-NSR Registry Expiry Date: 2022-10-05T17:00:14Z Registry Registrant ID: REDACTED FOR PRIVACY Registry Tech ID: REDACTED FOR PRIVACY Tech City: REDACTED FOR PRIVACY Tech Country: REDACTED FOR PRIVACY Tech Organization: REDACTED FOR PRIVACY Tech Postal Code: REDACTED FOR PRIVACY Tech State/Province: REDACTED FOR PRIVACY Updated Date: 2021-06-17T12:14:42Z Updated Date: 2021-06-22T19:14:40Z

VirusTotal Domain Summary

VirusTotal Reputation	0
Tags	

VirusTotal Analysis Summary

Aggregate Result	harmless - 86 / 86

VirusTotal Analysis Stats

Analysis Type	Number of Analysis
Confirmed Timeout	0
Failure	0
Harmless	86
Malicious	0
Suspicious	0
Timeout	0
Type Unsupported	0
Undetected	0
Total	**86**

View on VirusTotal

GUI Url: https://www.virustotal.com/gui/domain/mailrelay.evil.co

Community Votes

Total votes cast: 0

Incoming (1)

DNS Name	evil.co

VirusTotal File

maltego.virustotal.File

b99e813023393fd166ed3d053c41fdb987d74d2dec3fd4e4e4535105d605e0f2

Weight	0
MeaningfulName	b99e813023393fd166ed3d053c41fdb987d74d2dec3fd4e4e4535105d605e0f2
File Id	b99e813023393fd166ed3d053c41fdb987d74d2dec3fd4e4e4535105d605e0f2
Names	
File Type	XML
File Type Description	XML
MD5	ab4ca0acf41e8faa2e35b5674f69cbbe
SHA-1	6ef966fbc780b992605eaaaaec916610e6328bcd
SHA-256	b99e813023393fd166ed3d053c41fdb987d74d2dec3fd4e4e4535105d605e0f2
Vhash	
Authentihash	
SSDEEP	6144:Yd0KwZ/Bwrb9Uh/AM5DaR6RbMpP3by6S7EA8xft9X8aJtY2fpUX0u1zcDosrq:YdvwZ/BwrbXP35ZxV9XJJtU0uZ8o+q
Magic	XML document text
File Size	535809
Tags	xml
Capability Tags	
Downloadable	null
Creation Date	
First Submission Date	2021-03-09T18:07:30Z
Last Submission Date	2021-03-09T18:07:30Z
Last Analysis Date	2021-05-25T11:54:12Z
Total Votes - Harmless	0
Total Votes - Malicious	0
Submissions	1
Reputation	0

View on VirusTotal

GUI Url:
https://www.virustotal.com/gui/file/b99e813023393fd166ed3d053c41fdb987d74d2dec3fd4e4e4535105d605e0f2

File Summary

Names	
File Type	xml
File Type Description	XML
Tags	xml
Times Submitted	1

TrID - file type identification tool

File Type	Probability %
Scalable Vector Graphics (var.3)	52.7
Synchronized Multimedia Integration Language	18.1
Generic XML (ASCII)	18.1
HyperText Markup Language	10.9

VirusTotal Analysis Summary	
Aggregate Result	undetected - 48 / 74

VirusTotal Analysis Stats	
Analysis Type	Number of Analysis
Confirmed Timeout	0
Failure	0
Harmless	0
Malicious	10
Suspicious	0
Timeout	0
Type Unsupported	16
Undetected	48
Total	**74**

Community Votes

Total votes cast: 0

Incoming (1)

	DNS Name	www.evil.com

Domain

maltego.Domain

imap.evil.co

Weight	0
Domain Name	imap.evil.co
WHOIS Info	Admin City: REDACTED FOR PRIVACY Admin Country: REDACTED FOR PRIVACY Admin Organization: REDACTED FOR PRIVACY Admin Postal Code: REDACTED FOR PRIVACY Admin State/Province: REDACTED FOR PRIVACY Creation Date: 2019-10-05T17:00:14Z DNSSEC: unsigned Domain Name: evil.co Domain Status: clientDeleteProhibited http://www.icann.org/epp#clientDeleteProhibited Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited Domain Status: clientRenewProhibited http://www.icann.org/epp#clientRenewProhibited Domain Status: clientRenewProhibited https://icann.org/epp#clientRenewProhibited Domain Status: clientTransferProhibited http://www.icann.org/epp#clientTransferProhibited Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Domain Status: clientUpdateProhibited http://www.icann.org/epp#clientUpdateProhibited Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited Name Server: NS1.UNIREGISTRYMARKET.LINK Name Server: NS2.UNIREGISTRYMARKET.LINK Name Server: ns1.uniregistrymarket.link Name Server: ns2.uniregistrymarket.link Registrant City: 1f8f4166599d23ee Registrant Country: US Registrant Email: 44f8172ee385b60bs@ Registrant Email: f651612a2f356ad3s@ Registrant Fax Ext: 1f8f4166599d23ee Registrant Fax: 1f8f4166599d23ee Registrant Name: 1f8f4166599d23ee Registrant Organization: 3432650ec337c945 Registrant Phone Ext: 1f8f4166599d23ee Registrant Phone: 1f8f4166599d23ee Registrant Postal Code: 1f8f4166599d23ee Registrant State/Province: c5117919ef41a795 Registrant Street: 1f8f4166599d23ee Registrar Abuse Contact Email: abuse@godaddy.com Registrar Abuse Contact Phone: +1.4806242505 Registrar IANA ID: 146 Registrar Registration Expiration Date: 2022-10-05T17:00:14Z Registrar URL: http://www.godaddy.com Registrar URL: whois.godaddy.com Registrar WHOIS Server: whois.godaddy.com Registrar: GoDaddy.com, LLC Registry Admin ID: REDACTED FOR PRIVACY Registry Domain ID: D8A750721BA904C4A90CFDA260DBE314E-NSR Registry Expiry Date: 2022-10-05T17:00:14Z Registry Registrant ID: REDACTED FOR PRIVACY Registry Tech ID: REDACTED FOR PRIVACY Tech City: REDACTED FOR PRIVACY Tech Country: REDACTED FOR PRIVACY Tech Organization: REDACTED FOR PRIVACY Tech Postal Code: REDACTED FOR PRIVACY Tech State/Province: REDACTED FOR PRIVACY Updated Date: 2021-06-17T12:14:42Z Updated Date: 2021-06-22T19:14:40Z

VirusTotal Domain Summary

VirusTotal Reputation	0
Tags	

VirusTotal Analysis Summary

Aggregate Result	harmless - 86 / 86

VirusTotal Analysis Stats

Analysis Type	Number of Analysis
Confirmed Timeout	0
Failure	0
Harmless	86
Malicious	0
Suspicious	0
Timeout	0
Type Unsupported	0
Undetected	0
Total	**86**

View on VirusTotal

GUI Url: https://www.virustotal.com/gui/domain/imap.evil.co

Community Votes

Total votes cast: 0

Incoming (1)

DNS Name	evil.co

VirusTotal File

maltego.virustotal.File

01217b1a3f83a64c45533f31f51b12fb56e60b89b079a641e8cdf3e868a612ad

Weight	0
MeaningfulName	01217b1a3f83a64c45533f31f51b12fb56e60b89b079a641e8cdf3e868a612ad
File Id	01217b1a3f83a64c45533f31f51b12fb56e60b89b079a641e8cdf3e868a612ad
Names	
File Type	XML
File Type Description	XML
MD5	0a62fe95394c92ba34e103b44225787e
SHA-1	986a71661272fbc420b94a45d290339ce72b1acd
SHA-256	01217b1a3f83a64c45533f31f51b12fb56e60b89b079a641e8cdf3e868a612ad
Vhash	
Authentihash	
SSDEEP	3072:x+qvLzfMmMPW4jCqTwWl5T4Eg67UZ2xFq93Yjhccrv2QrFDlIBw2Z/q4+FNwPzGg:SDw6T4l2xQ5YjFb2YFDl+bZ/TLeho
Magic	XML document text
File Size	849004
Tags	xml
Capability Tags	
Downloadable	null
Creation Date	
First Submission Date	2021-04-10T20:21:05Z
Last Submission Date	2021-04-10T20:21:05Z
Last Analysis Date	2021-04-10T22:22:59Z
Total Votes - Harmless	0
Total Votes - Malicious	0
Submissions	1
Reputation	0

View on VirusTotal

GUI Url:
https://www.virustotal.com/gui/file/01217b1a3f83a64c45533f31f51b12fb56e60b89b079a641e8cdf3e868a612ad

File Summary

Names	
File Type	xml
File Type Description	XML
Tags	xml
Times Submitted	1

TrID - file type identification tool	
File Type	Probability %
NuGet Specification	32.4
Atom web feed	26.7
wxWindows - wxPython Resource	12.8
Scalable Vector Graphics (var.3)	10.9
Artificial Intelligence Markup Language	10.9

VirusTotal Analysis Summary	
Aggregate Result	undetected - 56 / 73

VirusTotal Analysis Stats	
Analysis Type	Number of Analysis
Confirmed Timeout	0
Failure	0
Harmless	0
Malicious	1
Suspicious	0
Timeout	0
Type Unsupported	16
Undetected	56
Total	**73**

Community Votes

Total votes cast: 0

Incoming (1)

	DNS Name	www.evil.com

Domain

maltego.Domain

imap2.evil.co

Weight	0
Domain Name	imap2.evil.co
WHOIS Info	Admin City: REDACTED FOR PRIVACY Admin Country: REDACTED FOR PRIVACY Admin Organization: REDACTED FOR PRIVACY Admin Postal Code: REDACTED FOR PRIVACY Admin State/Province: REDACTED FOR PRIVACY Creation Date: 2019-10-05T17:00:14Z DNSSEC: unsigned Domain Name: evil.co Domain Status: clientDeleteProhibited http://www.icann.org/epp#clientDeleteProhibited Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited Domain Status: clientRenewProhibited http://www.icann.org/epp#clientRenewProhibited Domain Status: clientRenewProhibited https://icann.org/epp#clientRenewProhibited Domain Status: clientTransferProhibited http://www.icann.org/epp#clientTransferProhibited Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Domain Status: clientUpdateProhibited http://www.icann.org/epp#clientUpdateProhibited Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited Name Server: NS1.UNIREGISTRYMARKET.LINK Name Server: NS2.UNIREGISTRYMARKET.LINK Name Server: ns1.uniregistrymarket.link Name Server: ns2.uniregistrymarket.link Registrant City: 1f8f4166599d23ee Registrant Country: US Registrant Email: 44f8172ee385b60bs@ Registrant Email: f651612a2f356ad3s@ Registrant Fax Ext: 1f8f4166599d23ee Registrant Fax: 1f8f4166599d23ee Registrant Name: 1f8f4166599d23ee Registrant Organization: 3432650ec337c945 Registrant Phone Ext: 1f8f4166599d23ee Registrant Phone: 1f8f4166599d23ee Registrant Postal Code: 1f8f4166599d23ee Registrant State/Province: c5117919ef41a795 Registrant Street: 1f8f4166599d23ee Registrar Abuse Contact Email: abuse@godaddy.com Registrar Abuse Contact Phone: +1.4806242505 Registrar IANA ID: 146 Registrar Registration Expiration Date: 2022-10-05T17:00:14Z Registrar URL: http://www.godaddy.com Registrar URL: whois.godaddy.com Registrar WHOIS Server: whois.godaddy.com Registrar: GoDaddy.com, LLC Registry Admin ID: REDACTED FOR PRIVACY Registry Domain ID: D8A750721BA904C4A90CFDA260DBE314E-NSR Registry Expiry Date: 2022-10-05T17:00:14Z Registry Registrant ID: REDACTED FOR PRIVACY Registry Tech ID: REDACTED FOR PRIVACY Tech City: REDACTED FOR PRIVACY Tech Country: REDACTED FOR PRIVACY Tech Organization: REDACTED FOR PRIVACY Tech Postal Code: REDACTED FOR PRIVACY Tech State/Province: REDACTED FOR PRIVACY Updated Date: 2021-06-17T12:14:42Z Updated Date: 2021-06-22T19:14:40Z

VirusTotal Domain Summary

VirusTotal Reputation	0
Tags	

VirusTotal Analysis Summary

Aggregate Result	harmless - 86 / 86

VirusTotal Analysis Stats

Analysis Type	Number of Analysis
Confirmed Timeout	0
Failure	0
Harmless	86
Malicious	0
Suspicious	0
Timeout	0
Type Unsupported	0
Undetected	0
Total	**86**

View on VirusTotal

GUI Url: https://www.virustotal.com/gui/domain/imap2.evil.co

Community Votes

Total votes cast: 0

Incoming (1)

DNS Name	evil.co

VirusTotal File

maltego.virustotal.File

d8307ef63337fa211962ef4cebdacb240ffd079fdccad3ba2a4e3d1c05553d39

Weight	0
MeaningfulName	d8307ef63337fa211962ef4cebdacb240ffd079fdccad3ba2a4e3d1c05553d39
File Id	d8307ef63337fa211962ef4cebdacb240ffd079fdccad3ba2a4e3d1c05553d39
Names	
File Type	PEEXE
File Type Description	Win32 EXE
MD5	d61845838f05397429f0d2fa357f0965
SHA-1	540ea611bce11d4b2deae4753a65eff1cfb6eadd
SHA-256	d8307ef63337fa211962ef4cebdacb240ffd079fdccad3ba2a4e3d1c05553d39
Vhash	016056655d156561z13z20078z47z72z1dfz
Authentihash	fa9912ab6def07e9cf479a2e7dcdd67af0070c5f1ef97da1878a6f1f81fa6ee0
SSDEEP	24576:V/XZaF/YEX+Mys661SS5rU+QXUKLtfB2br9P6YhAoIlVOZ:V/pM/VyiSS8Uip2bt6wAoIlVc
Magic	PE32 executable for MS Windows (GUI) Intel 80386 32-bit
File Size	1290668
Tags	peexe, invalid-rich-pe-linker-version, overlay, direct-cpu-clock-access, runtime-modules
Capability Tags	
Downloadable	null
Creation Date	2021-02-03T08:07:52Z
First Submission Date	2021-03-27T10:30:06Z
Last Submission Date	2021-03-27T10:30:06Z
Last Analysis Date	2021-04-03T01:23:20Z
Total Votes - Harmless	0
Total Votes - Malicious	0
Submissions	1
Reputation	0

View on VirusTotal

GUI Url:
https://www.virustotal.com/gui/file/d8307ef63337fa211962ef4cebdacb240ffd079fdccad3ba2a4e3d1c05553d39

File Summary

Names	
File Type	peexe
File Type Description	Win32 EXE
Tags	peexe, invalid-rich-pe-linker-version, overlay, direct-cpu-clock-access, runtime-modules
Times Submitted	1

TrID - file type identification tool	
File Type	Probability %
Win64 Executable (generic)	40.3
Win16 NE executable (generic)	19.3
Win32 Executable (generic)	17.2
OS/2 Executable (generic)	7.7
Generic Win/DOS Executable	7.6

VirusTotal Analysis Summary	
Aggregate Result	undetected - 41 / 74

VirusTotal Analysis Stats	
Analysis Type	Number of Analysis
Confirmed Timeout	0
Failure	4
Harmless	0
Malicious	22
Suspicious	0
Timeout	1
Type Unsupported	6
Undetected	41
Total	**74**

Community Votes

Total votes cast: 0

Incoming (1)

DNS Name	www.evil.com

Domain

maltego.Domain

comune.evil.co

Weight	0
Domain Name	comune.evil.co
WHOIS Info	Admin City: REDACTED FOR PRIVACY Admin Country: REDACTED FOR PRIVACY Admin Organization: REDACTED FOR PRIVACY Admin Postal Code: REDACTED FOR PRIVACY Admin State/Province: REDACTED FOR PRIVACY Creation Date: 2019-10-05T17:00:14Z DNSSEC: unsigned Domain Name: evil.co Domain Status: clientDeleteProhibited http://www.icann.org/epp#clientDeleteProhibited Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited Domain Status: clientRenewProhibited http://www.icann.org/epp#clientRenewProhibited Domain Status: clientRenewProhibited https://icann.org/epp#clientRenewProhibited Domain Status: clientTransferProhibited http://www.icann.org/epp#clientTransferProhibited Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Domain Status: clientUpdateProhibited http://www.icann.org/epp#clientUpdateProhibited Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited Name Server: NS1.UNIREGISTRYMARKET.LINK Name Server: NS2.UNIREGISTRYMARKET.LINK Name Server: ns1.uniregistrymarket.link Name Server: ns2.uniregistrymarket.link Registrant City: 1f8f4166599d23ee Registrant Country: US Registrant Email: 44f8172ee385b60bs@ Registrant Email: f651612a2f356ad3s@ Registrant Fax Ext: 1f8f4166599d23ee Registrant Fax: 1f8f4166599d23ee Registrant Name: 1f8f4166599d23ee Registrant Organization: 3432650ec337c945 Registrant Phone Ext: 1f8f4166599d23ee Registrant Phone: 1f8f4166599d23ee Registrant Postal Code: 1f8f4166599d23ee Registrant State/Province: c5117919ef41a795 Registrant Street: 1f8f4166599d23ee Registrar Abuse Contact Email: abuse@godaddy.com Registrar Abuse Contact Phone: +1.4806242505 Registrar IANA ID: 146 Registrar Registration Expiration Date: 2022-10-05T17:00:14Z Registrar URL: http://www.godaddy.com Registrar URL: whois.godaddy.com Registrar WHOIS Server: whois.godaddy.com Registrar: GoDaddy.com, LLC Registry Admin ID: REDACTED FOR PRIVACY Registry Domain ID: D8A750721BA904C4A90CFDA260DBE314E-NSR Registry Expiry Date: 2022-10-05T17:00:14Z Registry Registrant ID: REDACTED FOR PRIVACY Registry Tech ID: REDACTED FOR PRIVACY Tech City: REDACTED FOR PRIVACY Tech Country: REDACTED FOR PRIVACY Tech Organization: REDACTED FOR PRIVACY Tech Postal Code: REDACTED FOR PRIVACY Tech State/Province: REDACTED FOR PRIVACY Updated Date: 2021-06-17T12:14:42Z Updated Date: 2021-06-22T19:14:40Z

VirusTotal Domain Summary

VirusTotal Reputation	0
Tags	

VirusTotal Analysis Summary

Aggregate Result	harmless - 86 / 86

VirusTotal Analysis Stats

Analysis Type	Number of Analysis
Confirmed Timeout	0
Failure	0
Harmless	86
Malicious	0
Suspicious	0
Timeout	0
Type Unsupported	0
Undetected	0
Total	**86**

View on VirusTotal

GUI Url: https://www.virustotal.com/gui/domain/comune.evil.co

Community Votes

Total votes cast: 0

Incoming (1)

DNS Name	evil.co

Domain

maltego.Domain

po.evil.co

Weight	0
Domain Name	po.evil.co
WHOIS Info	Admin City: REDACTED FOR PRIVACY Admin Country: REDACTED FOR PRIVACY Admin Organization: REDACTED FOR PRIVACY Admin Postal Code: REDACTED FOR PRIVACY Admin State/Province: REDACTED FOR PRIVACY Creation Date: 2019-10-05T17:00:14Z DNSSEC: unsigned Domain Name: evil.co Domain Status: clientDeleteProhibited http://www.icann.org/epp#clientDeleteProhibited Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited Domain Status: clientRenewProhibited http://www.icann.org/epp#clientRenewProhibited Domain Status: clientRenewProhibited https://icann.org/epp#clientRenewProhibited Domain Status: clientTransferProhibited http://www.icann.org/epp#clientTransferProhibited Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Domain Status: clientUpdateProhibited http://www.icann.org/epp#clientUpdateProhibited Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited Name Server: NS1.UNIREGISTRYMARKET.LINK Name Server: NS2.UNIREGISTRYMARKET.LINK Name Server: ns1.uniregistrymarket.link Name Server: ns2.uniregistrymarket.link Registrant City: 1f8f4166599d23ee Registrant Country: US Registrant Email: 44f8172ee385b60bs@ Registrant Email: f651612a2f356ad3s@ Registrant Fax Ext: 1f8f4166599d23ee Registrant Fax: 1f8f4166599d23ee Registrant Name: 1f8f4166599d23ee Registrant Organization: 3432650ec337c945 Registrant Phone Ext: 1f8f4166599d23ee Registrant Phone: 1f8f4166599d23ee Registrant Postal Code: 1f8f4166599d23ee Registrant State/Province: c5117919ef41a795 Registrant Street: 1f8f4166599d23ee Registrar Abuse Contact Email: abuse@godaddy.com Registrar Abuse Contact Phone: +1.4806242505 Registrar IANA ID: 146 Registrar Registration Expiration Date: 2022-10-05T17:00:14Z Registrar URL: http://www.godaddy.com Registrar URL: whois.godaddy.com Registrar WHOIS Server: whois.godaddy.com Registrar: GoDaddy.com, LLC Registry Admin ID: REDACTED FOR PRIVACY Registry Domain ID: D8A750721BA904C4A90CFDA260DBE314E-NSR Registry Expiry Date: 2022-10-05T17:00:14Z Registry Registrant ID: REDACTED FOR PRIVACY Registry Tech ID: REDACTED FOR PRIVACY Tech City: REDACTED FOR PRIVACY Tech Country: REDACTED FOR PRIVACY Tech Organization: REDACTED FOR PRIVACY Tech Postal Code: REDACTED FOR PRIVACY Tech State/Province: REDACTED FOR PRIVACY Updated Date: 2021-06-17T12:14:42Z Updated Date: 2021-06-22T19:14:40Z

VirusTotal Domain Summary

VirusTotal Reputation	0
Tags	

VirusTotal Analysis Summary

Aggregate Result	harmless - 86 / 86

VirusTotal Analysis Stats

Analysis Type	Number of Analysis
Confirmed Timeout	0
Failure	0
Harmless	86
Malicious	0
Suspicious	0
Timeout	0
Type Unsupported	0
Undetected	0
Total	**86**

View on VirusTotal

GUI Url: https://www.virustotal.com/gui/domain/po.evil.co

Community Votes

Total votes cast: 0

Incoming (1)

DNS Name evil.co

VirusTotal File

maltego.virustotal.File

check-client.phar

Weight	0
MeaningfulName	check-client.phar
File Id	a71e275aef42948ab4079c2092b047e33e1f1be43de0e72ddba537589e6180cf
Names	check-client.phar
File Type	
File Type Description	unknown
MD5	3cde08bf663564df0833b87a5dd37df6
SHA-1	038a1c62044e07e2b9514bcb15830628b7017522
SHA-256	a71e275aef42948ab4079c2092b047e33e1f1be43de0e72ddba537589e6180cf
Vhash	
Authentihash	
SSDEEP	24576:hydTGWuSqEq0/gBx0tBN3jTpM6FoN5AZ8:gM
Magic	data
File Size	1354163
Tags	
Capability Tags	
Downloadable	null
Creation Date	
First Submission Date	2021-05-18T11:05:51Z
Last Submission Date	2021-05-18T11:05:51Z
Last Analysis Date	2021-05-24T22:46:50Z
Total Votes - Harmless	0
Total Votes - Malicious	0
Submissions	1
Reputation	0

View on VirusTotal

GUI Url:
https://www.virustotal.com/gui/file/a71e275aef42948ab4079c2092b047e33e1f1be43de0e72ddba537589e6180cf

File Summary

Names	check-client.phar
File Type	
File Type Description	unknown
Tags	
Times Submitted	1

TrID - file type identification tool

File Type	Probability %
Timed Text Markup Language	73.7
PHP source	16.3
HyperText Markup Language	9.8

VirusTotal Analysis Summary	
Aggregate Result	undetected - 56 / 73

VirusTotal Analysis Stats	
Analysis Type	Number of Analysis
Confirmed Timeout	0
Failure	0
Harmless	0
Malicious	1
Suspicious	0
Timeout	0
Type Unsupported	16
Undetected	56
Total	**73**

Community Votes

Total votes cast: 0

Incoming (1)

	DNS Name	www.evil.com

VirusTotal File

maltego.virustotal.File

degrees-of-lewdity-rus.tar

Weight	0
MeaningfulName	degrees-of-lewdity-rus.tar
File Id	f20fa0f34568fdeede49b60dc0ed0900f8d6b6ab8e4c916e1213d4241f53922d
Names	degrees-of-lewdity-rus.tar
File Type	TAR
File Type Description	TAR
MD5	05aae10a87dc8957fb4137b17b145af8
SHA-1	ffe91e30f4c9d6ac156c55a8188d347ac7053483
SHA-256	f20fa0f34568fdeede49b60dc0ed0900f8d6b6ab8e4c916e1213d4241f53922d
Vhash	0f020c96555a6c9eb8a130ba146dac55
Authentihash	
SSDEEP	1572864:MspO6vUMiVMm1Rwj1GHKnHJE54Djk1Z5o41k98Epf99qzINUsrVwgPVMbYcyK:MsvvU41ZE54Dja5ol99xSGqgtMbYcr
Magic	POSIX tar archive
File Size	144404480
Tags	tar
Capability Tags	
Downloadable	null
Creation Date	
First Submission Date	2021-08-22T00:43:45Z
Last Submission Date	2021-08-22T00:43:45Z
Last Analysis Date	2021-08-22T03:57:42Z
Total Votes - Harmless	0
Total Votes - Malicious	0
Submissions	1
Reputation	0

View on VirusTotal

GUI Url:
https://www.virustotal.com/gui/file/f20fa0f34568fdeede49b60dc0ed0900f8d6b6ab8e4c916e1213d4241f53922d

File Summary

Names	degrees-of-lewdity-rus.tar
File Type	tar
File Type Description	TAR
Tags	tar
Times Submitted	1

TrID - file type identification tool

File Type	Probability %
TAR - Tape ARchive (POSIX)	100.0

VirusTotal Analysis Summary

Aggregate Result	undetected - 40 / 73

VirusTotal Analysis Stats

Analysis Type	Number of Analysis
Confirmed Timeout	1
Failure	1
Harmless	0
Malicious	1
Suspicious	0
Timeout	15
Type Unsupported	15
Undetected	40
Total	**73**

Community Votes

Total votes cast: 0

Incoming (1)

DNS	DNS Name	www.evil.com

Domain

maltego.Domain

dom.evil.co

Weight	0
Domain Name	dom.evil.co
WHOIS Info	Admin City: REDACTED FOR PRIVACY Admin Country: REDACTED FOR PRIVACY Admin Organization: REDACTED FOR PRIVACY Admin Postal Code: REDACTED FOR PRIVACY Admin State/Province: REDACTED FOR PRIVACY Creation Date: 2019-10-05T17:00:14Z DNSSEC: unsigned Domain Name: evil.co Domain Status: clientDeleteProhibited http://www.icann.org/epp#clientDeleteProhibited Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited Domain Status: clientRenewProhibited http://www.icann.org/epp#clientRenewProhibited Domain Status: clientRenewProhibited https://icann.org/epp#clientRenewProhibited Domain Status: clientTransferProhibited http://www.icann.org/epp#clientTransferProhibited Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Domain Status: clientUpdateProhibited http://www.icann.org/epp#clientUpdateProhibited Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited Name Server: NS1.UNIREGISTRYMARKET.LINK Name Server: NS2.UNIREGISTRYMARKET.LINK Name Server: ns1.uniregistrymarket.link Name Server: ns2.uniregistrymarket.link Registrant City: 1f8f4166599d23ee Registrant Country: US Registrant Email: 44f8172ee385b60bs@ Registrant Email: f651612a2f356ad3s@ Registrant Fax Ext: 1f8f4166599d23ee Registrant Fax: 1f8f4166599d23ee Registrant Name: 1f8f4166599d23ee Registrant Organization: 3432650ec337c945 Registrant Phone Ext: 1f8f4166599d23ee Registrant Phone: 1f8f4166599d23ee Registrant Postal Code: 1f8f4166599d23ee Registrant State/Province: c5117919ef41a795 Registrant Street: 1f8f4166599d23ee Registrar Abuse Contact Email: abuse@godaddy.com Registrar Abuse Contact Phone: +1.4806242505 Registrar IANA ID: 146 Registrar Registration Expiration Date: 2022-10-05T17:00:14Z Registrar URL: http://www.godaddy.com Registrar URL: whois.godaddy.com Registrar WHOIS Server: whois.godaddy.com Registrar: GoDaddy.com, LLC Registry Admin ID: REDACTED FOR PRIVACY Registry Domain ID: D8A750721BA904C4A90CFDA260DBE314E-NSR Registry Expiry Date: 2022-10-05T17:00:14Z Registry Registrant ID: REDACTED FOR PRIVACY Registry Tech ID: REDACTED FOR PRIVACY Tech City: REDACTED FOR PRIVACY Tech Country: REDACTED FOR PRIVACY Tech Organization: REDACTED FOR PRIVACY Tech Postal Code: REDACTED FOR PRIVACY Tech State/Province: REDACTED FOR PRIVACY Updated Date: 2021-06-17T12:14:42Z Updated Date: 2021-06-22T19:14:40Z

VirusTotal Domain Summary

VirusTotal Reputation	0
Tags	

VirusTotal Analysis Summary

Aggregate Result	harmless - 86 / 86

VirusTotal Analysis Stats

Analysis Type	Number of Analysis
Confirmed Timeout	0
Failure	0
Harmless	86
Malicious	0
Suspicious	0
Timeout	0
Type Unsupported	0
Undetected	0
Total	**86**

View on VirusTotal

GUI Url: https://www.virustotal.com/gui/domain/dom.evil.co

Community Votes

Total votes cast: 0

Incoming (1)

DNS Name	evil.co

VirusTotal File

maltego.virustotal.File

ib_logfile2 - Copy

Weight	0
MeaningfulName	ib_logfile2 - Copy
File Id	3ba37146b6c5acc8c2c00fb48e23fdcfd440cd93ec99ecf2feec28df8c7dc4ab
Names	ib_logfile2 - Copy, ib_logfile2
File Type	
File Type Description	unknown
MD5	11d671fb9027912b0d81d7fcbcab8ac3
SHA-1	3a0500b1463aa4870302ca04e57f75d383ca4650
SHA-256	3ba37146b6c5acc8c2c00fb48e23fdcfd440cd93ec99ecf2feec28df8c7dc4ab
Vhash	
Authentihash	
SSDEEP	1572864:m5CGej/q/ZpAqYycM3RM9rJb6J7qlgGfwyuHOFRXOObUjBnqJh+:m59diycMzwOObMqJh+
Magic	data
File Size	314572800
Tags	exploit, cve-2014-0276
Capability Tags	
Downloadable	null
Creation Date	
First Submission Date	2019-12-09T10:58:16Z
Last Submission Date	2019-12-09T12:33:04Z
Last Analysis Date	2021-07-09T16:49:18Z
Total Votes - Harmless	0
Total Votes - Malicious	0
Submissions	2
Reputation	0

View on VirusTotal

GUI Url:
https://www.virustotal.com/gui/file/3ba37146b6c5acc8c2c00fb48e23fdcfd440cd93ec99ecf2feec28df8c7dc4ab

File Summary

Names	ib_logfile2 - Copy, ib_logfile2
File Type	
File Type Description	unknown
Tags	exploit, cve-2014-0276
Times Submitted	2

TrID - file type identification tool

File Type	Probability %
MacBinary 1	50.7
Adobe PhotoShop Brush	49.2

VirusTotal Analysis Summary

Aggregate Result	undetected - 55 / 76

VirusTotal Analysis Stats

Analysis Type	Number of Analysis
Confirmed Timeout	0
Failure	1
Harmless	0
Malicious	4
Suspicious	0
Timeout	0
Type Unsupported	16
Undetected	55
Total	**76**

Community Votes

Total votes cast: 0

Incoming (1)

DNS Name	www.evil.com

VirusTotal File

maltego.virustotal.File

StackOverflowData.csv

Weight	0
MeaningfulName	StackOverflowData.csv
File Id	0c6bfe150dc7b4f08de4df5f649c3754afbe483ab4fa11f7043d9a9b00b253b5
Names	StackOverflowData.csv
File Type	JAVASCRIPT
File Type Description	JavaScript
MD5	a41959675422af4de8576413026dc698
SHA-1	70660a18b3cdcee41aa5068880281247cdb938fe
SHA-256	0c6bfe150dc7b4f08de4df5f649c3754afbe483ab4fa11f7043d9a9b00b253b5
Vhash	ef5b0b32218d996c754d5e7a566788bf
Authentihash	
SSDEEP	49152:dQHwAybfOPJc7uT/TP6FopjvbX+eANVylOwptLgmgkEx7q:SwTFejzyRq
Magic	UTF-8 Unicode C++ program text, with very long lines, with CRLF, LF line terminators
File Size	4681686
Tags	javascript
Capability Tags	
Downloadable	null
Creation Date	
First Submission Date	2021-10-01T15:25Z
Last Submission Date	2021-10-01T15:25Z
Last Analysis Date	2021-10-02T16:35:56Z
Total Votes - Harmless	0
Total Votes - Malicious	0
Submissions	1
Reputation	0

View on VirusTotal

GUI Url:
https://www.virustotal.com/gui/file/0c6bfe150dc7b4f08de4df5f649c3754afbe483ab4fa11f7043d9a9b00b253b5

File Summary

Names	StackOverflowData.csv
File Type	javascript
File Type Description	JavaScript
Tags	javascript
Times Submitted	1

TrID - file type identification tool

File Type	Probability %
file seems to be plain text/ASCII	0.0

VirusTotal Analysis Summary

Aggregate Result	undetected - 53 / 71

VirusTotal Analysis Stats

Analysis Type	Number of Analysis
Confirmed Timeout	0
Failure	0
Harmless	0
Malicious	4
Suspicious	0
Timeout	0
Type Unsupported	14
Undetected	53
Total	**71**

Community Votes

Total votes cast: 0

Incoming (1)

DNS Name	www.evil.com

A Record

maltego.ARecord

w3snoop.com

Weight	0
IPv4 Address	35.168.41.214
Time to Live (TTL)	0
DNS Name	w3snoop.com
Shodan Last Update	2020-03-02T19:17:23.392203+00:00

Incoming (1)

DNS Name	w3snoop.com

A Record

maltego.ARecord

w3snoop.com

Weight	0
IPv4 Address	52.4.142.59
Time to Live (TTL)	0
DNS Name	w3snoop.com
Shodan Last Update	2020-02-03T02:49:58.465930+00:00

Incoming (1)

DNS Name	w3snoop.com

A Record

maltego.ARecord

w3snoop.com

Weight	0
IPv4 Address	34.230.210.117
Time to Live (TTL)	0
DNS Name	w3snoop.com
Shodan Last Update	2019-04-20T09:26:29.720736+00:00

Incoming (1)

DNS Name	w3snoop.com

A Record

maltego.ARecord

w3snoop.com

Weight	0
IPv4 Address	52.77.33.135
Time to Live (TTL)	0
DNS Name	w3snoop.com
Shodan Last Update	2020-01-21T14:08:32.027048+00:00

Incoming (1)

DNS Name	w3snoop.com

A Record

maltego.ARecord

w3snoop.com

Weight	0
IPv4 Address	35.153.250.12
Time to Live (TTL)	0
DNS Name	w3snoop.com
Shodan Last Update	2019-12-24T02:45:01.408715+00:00

Incoming (1)

DNS Name	w3snoop.com

A Record

maltego.ARecord

w3snoop.com

Weight	0
IPv4 Address	52.52.40.206
Time to Live (TTL)	0
DNS Name	w3snoop.com
Shodan Last Update	2019-05-20T06:10:45.583536+00:00

Incoming (1)

DNS Name	w3snoop.com

A Record

maltego.ARecord

w3snoop.com

Weight	0
IPv4 Address	34.237.101.58
Time to Live (TTL)	0
DNS Name	w3snoop.com
Shodan Last Update	2019-04-16T03:37:45.905666+00:00

Incoming (1)

DNS Name	w3snoop.com

Email Address

maltego.EmailAddress

eig-noc@endurance.com

Weight	100
Email Address	eig-noc@endurance.com

Incoming (1)

IPv4 Address	66.96.146.129

A Record

maltego.ARecord

w3snoop.com

Weight	0
IPv4 Address	54.156.9.246
Time to Live (TTL)	0
DNS Name	w3snoop.com
Shodan Last Update	2020-04-06T18:38:45.351457+00:00

Incoming (1)

DNS Name	w3snoop.com

VirusTotal File

maltego.virustotal.File

prefs-2.js

Weight	0
MeaningfulName	prefs-2.js
File Id	96aa12b18255db551b7a8e86ec999222e2945069bdad71dc35ac63fbb2593766
Names	prefs-2.js
File Type	C
File Type Description	C
MD5	c4363f03293a2ed8ee7dd7d39318a0e0
SHA-1	25b5c5fc0a4fb7e4cb0ad65cab65a24e0028c422
SHA-256	96aa12b18255db551b7a8e86ec999222e2945069bdad71dc35ac63fbb2593766
Vhash	
Authentihash	
SSDEEP	1536:ul781tw1iWuSBfAdIftevmbKmNYiDRfPcFS7xvv8wdku1:u/6tvOpMu1
Magic	UTF-8 Unicode C program text, with very long lines, with CRLF line terminators
File Size	110227
Tags	c
Capability Tags	
Downloadable	null
Creation Date	
First Submission Date	2017-12-09T02:42:45Z
Last Submission Date	2017-12-09T02:42:45Z
Last Analysis Date	2018-09-09T14:10:45Z
Total Votes - Harmless	0
Total Votes - Malicious	0
Submissions	1
Reputation	0

View on VirusTotal

GUI Url:
https://www.virustotal.com/gui/file/96aa12b18255db551b7a8e86ec999222e2945069bdad71dc35ac63fbb2593766

File Summary

Names	prefs-2.js
File Type	c
File Type Description	C
Tags	c
Times Submitted	1

TrID - file type identification tool	
File Type	Probability %
OpenVPN profile (with rem)	100.0

VirusTotal Analysis Summary	
Aggregate Result	undetected - 58 / 70

VirusTotal Analysis Stats	
Analysis Type	Number of Analysis
Confirmed Timeout	0
Failure	0
Harmless	0
Malicious	0
Suspicious	0
Timeout	0
Type Unsupported	12
Undetected	58
Total	**70**

Community Votes

Total votes cast: 0

Incoming (1)

DNS Name	w3snoop.com

VirusTotal File

maltego.virustotal.File

deccab.exe

Weight	0
MeaningfulName	deccab.exe
File Id	211560ab26cf48c0d80c16cee64aa936c9ce3df92f7d4e35aec2cf6a671d72f3
Names	deccab, deccab.exe, 24851077
File Type	PEEXE
File Type Description	Win32 EXE
MD5	4c83533ee8528311f65a2392caccaf86
SHA-1	e3c26632aebd92dcf0141c5b67f653c5eda285e1
SHA-256	211560ab26cf48c0d80c16cee64aa936c9ce3df92f7d4e35aec2cf6a671d72f3
Vhash	046046655d151az3529=z
Authentihash	38a532a7d7d6677c6e19a3fc8899755468666b24e1f64e064396ff709fac629a
SSDEEP	98304:k01kmQl2iR4MdgKG8Yx/p1xUJEg0Jff4P:k6kmqNplYf1aJEjJIP
Magic	PE32 executable for MS Windows (GUI) Intel 80386 32-bit
File Size	4000784
Tags	peexe, overlay
Capability Tags	
Downloadable	null
Creation Date	2016-07-11T10:18:50Z
First Submission Date	2019-05-12T17:39:20Z
Last Submission Date	2019-05-12T17:39:20Z
Last Analysis Date	2019-06-10T09:09:10Z
Total Votes - Harmless	0
Total Votes - Malicious	0
Submissions	1
Reputation	0

View on VirusTotal

GUI Url:
https://www.virustotal.com/gui/file/211560ab26cf48c0d80c16cee64aa936c9ce3df92f7d4e35aec2cf6a671d72f3

File Summary

Names	deccab, deccab.exe, 24851077
File Type	peexe
File Type Description	Win32 EXE
Tags	peexe, overlay
Times Submitted	1

TrID - file type identification tool	
File Type	Probability %
Win32 Executable MS Visual C++ (generic)	33.7
Win64 Executable (generic)	29.8
Microsoft Visual C++ compiled executable (generic)	17.8
Win32 Dynamic Link Library (generic)	7.1
Win32 Executable (generic)	4.8

VirusTotal Analysis Summary	
Aggregate Result	undetected - 70 / 71

VirusTotal Analysis Stats	
Analysis Type	Number of Analysis
Confirmed Timeout	0
Failure	0
Harmless	0
Malicious	0
Suspicious	0
Timeout	0
Type Unsupported	1
Undetected	70
Total	**71**

Community Votes

Total votes cast: 0

Incoming (1)

	DNS Name	w3snoop.com

VirusTotal File

maltego.virustotal.File

Speed Booster [Android].xlsx

Weight	0
MeaningfulName	Speed Booster [Android].xlsx
File Id	ae5a3cd7c6edb95105b3c4e425c6e1a301446c303960d452bead1a8ae4b37882
Names	Speed Booster [Android].xlsx
File Type	XLSX
File Type Description	Office Open XML Spreadsheet
MD5	e79c1746e25c68348d011f3442e278bc
SHA-1	0cee99b29b7d6df4fc1c761c76817aeb42237351
SHA-256	ae5a3cd7c6edb95105b3c4e425c6e1a301446c303960d452bead1a8ae4b37882
Vhash	5f32346cd3cad731a88f1f4ed42be743
Authentihash	
SSDEEP	24576:HlLhDab6axAAaqaxj892O3PC7gwZx/+mA0iI1BmdOIAqTpIh7Jqy3E9:HT2b6axA1lj8jdOIZVny38
Magic	Zip archive data, at least v2.0 to extract
File Size	1127411
Tags	xlsx
Capability Tags	
Downloadable	null
Creation Date	
First Submission Date	2017-10-03T00:33:39Z
Last Submission Date	2017-10-03T00:33:39Z
Last Analysis Date	2017-11-02T19:29:39Z
Total Votes - Harmless	0
Total Votes - Malicious	0
Submissions	2
Reputation	0

View on VirusTotal

GUI Url:
https://www.virustotal.com/gui/file/ae5a3cd7c6edb95105b3c4e425c6e1a301446c303960d452bead1a8ae4b37882

File Summary

Names	Speed Booster [Android].xlsx
File Type	xlsx
File Type Description	Office Open XML Spreadsheet
Tags	xlsx
Times Submitted	2

TrID - file type identification tool	
File Type	Probability %
Excel Microsoft Office Open XML Format document	61.2
Open Packaging Conventions container	31.5
ZIP compressed archive	7.2

VirusTotal Analysis Summary	
Aggregate Result	undetected - 61 / 71

VirusTotal Analysis Stats	
Analysis Type	Number of Analysis
Confirmed Timeout	0
Failure	0
Harmless	0
Malicious	0
Suspicious	0
Timeout	0
Type Unsupported	10
Undetected	61
Total	**71**

Community Votes

Total votes cast: 0

Incoming (1)

	DNS Name	w3snoop.com

VirusTotal File

maltego.virustotal.File

places.sqlite

Weight	0
MeaningfulName	places.sqlite
File Id	f169d376181cec17a01767b22b4fa9d4b3f62df203149627969a4b161bfa55d7
Names	places.sqlite
File Type	
File Type Description	unknown
MD5	94088dc8dc447c82d3dcb5879bc27e60
SHA-1	aff1cef892df925e7e85c9d5ce122bf30871cac5
SHA-256	f169d376181cec17a01767b22b4fa9d4b3f62df203149627969a4b161bfa55d7
Vhash	
Authentihash	
SSDEEP	24576:xvTJ289q66hu6m9rBC1HGYrPovw6JL6IxPx:FJMU6m9Q1Zovw6JLpxP
Magic	SQLite 3.x database, user version 26
File Size	10485760
Tags	
Capability Tags	
Downloadable	null
Creation Date	
First Submission Date	2017-02-10T04:05:15Z
Last Submission Date	2018-03-12T10:09:28Z
Last Analysis Date	2020-12-20T02:10:08Z
Total Votes - Harmless	0
Total Votes - Malicious	0
Submissions	2
Reputation	0

View on VirusTotal

GUI Url:
https://www.virustotal.com/gui/file/f169d376181cec17a01767b22b4fa9d4b3f62df203149627969a4b161bfa55d7

File Summary

Names	places.sqlite
File Type	
File Type Description	unknown
Tags	
Times Submitted	2

TrID - file type identification tool

File Type	Probability %
SQLite 3.x database	100.0

VirusTotal Analysis Summary

Aggregate Result	undetected - 60 / 76

VirusTotal Analysis Stats

Analysis Type	Number of Analysis
Confirmed Timeout	0
Failure	0
Harmless	0
Malicious	0
Suspicious	0
Timeout	0
Type Unsupported	16
Undetected	60
Total	**76**

Community Votes

Total votes cast: 0

Incoming (1)

DNS Name	w3snoop.com

VirusTotal File

maltego.virustotal.File

4646-apk.apk

Weight	0
MeaningfulName	4646-apk.apk
File Id	e6cd4aa07adefff0cf483ef80c49e3503fbad724eb85075b8e4699a7012aa07b
Names	4646-apk.apk, moc.study.AllinOneInternetkiJankari.apk
File Type	ANDROID
File Type Description	Android
MD5	87151b97b0e8a391c314aa6d4857f2b1
SHA-1	5166aea4e030cc2a7b449542366d7fce443c6180
SHA-256	e6cd4aa07adefff0cf483ef80c49e3503fbad724eb85075b8e4699a7012aa07b
Vhash	7728012f0283849f0287a3e72ff56a2a
Authentihash	
SSDEEP	12288:pLtomcnWxKadIekkEp0HswOtT1mW1Zcv17VeAnqpSYZrlEl/CpKVCkgc:3orW8adIe9mtr1Zs1sAnBYBlP/lCkf
Magic	Zip archive data, at least v2.0 to extract
File Size	1562285
Tags	apk, android
Capability Tags	
Downloadable	null
Creation Date	
First Submission Date	2018-08-31T06:55:21Z
Last Submission Date	2021-04-17T21:52:11Z
Last Analysis Date	2021-04-17T23:53:43Z
Total Votes - Harmless	0
Total Votes - Malicious	0
Submissions	5
Reputation	0

View on VirusTotal

GUI Url:
https://www.virustotal.com/gui/file/e6cd4aa07adefff0cf483ef80c49e3503fbad724eb85075b8e4699a7012aa07b

File Summary

Names	4646-apk.apk, moc.study.AllinOneInternetkiJankari.apk
File Type	android
File Type Description	Android
Tags	apk, android
Times Submitted	5

TrID - file type identification tool

File Type	Probability %
Android Package	57.0
Java Archive	20.0
Sweet Home 3D design (generic)	15.5
ZIP compressed archive	5.9
PrintFox/Pagefox bitmap (640x800)	1.4

VirusTotal Analysis Summary

Aggregate Result	undetected - 61 / 73

VirusTotal Analysis Stats

Analysis Type	Number of Analysis
Confirmed Timeout	0
Failure	0
Harmless	0
Malicious	1
Suspicious	0
Timeout	0
Type Unsupported	11
Undetected	61
Total	**73**

Community Votes

Total votes cast: 0

Incoming (1)

DNS Name	w3snoop.com

Person

maltego.Person

OrgTechName

Weight	37
Full Name	OrgTechName
First Names	
Surname	

Info

Relevance:	0.371864
Count:	1

Incoming (1)

IPv4 Address	66.96.146.129

Person

maltego.Person

OrgNOCName

Weight	37
Full Name	OrgNOCName
First Names	
Surname	

Info

Relevance:	0.376018
Count:	1

Incoming (1)

IPv4 Address	66.96.146.129

Person

maltego.Person

OrgName

Weight	38
Full Name	OrgName
First Names	
Surname	

Info

Relevance:	0.389883
Count:	1

Incoming (1)

IPv4 Address	66.96.146.129

Email Address

maltego.EmailAddress

eig-net-team@endurance.com

Weight	100
Email Address	eig-net-team@endurance.com

Incoming (1)

IPv4 Address	66.96.146.129

Phone Number

maltego.PhoneNumber

+1 877 659 6181

Weight	100
Phone Number	+1 877 659 6181
Country Code	
City Code	
Area Code	
Last Digits	

Incoming (1)

IPv4 Address	66.96.146.129

Location

maltego.Location

Burlington

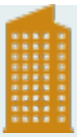
Weight	41
Name	Burlington
Country	
City	
Street Address	
Area	
Area Code	
Country Code	
Longitude	0.0
Latitude	0.0

Info

Relevance:	0.411051
Count:	1

Incoming (1)

IPv4 Address	66.96.146.129



Company

maltego.Company

Endurance International Group

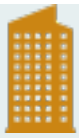
Weight	78
Name	Endurance International Group

Info

Relevance:	0.781732
Count:	2

Incoming (1)

IPv4 Address	66.96.146.129



Company

maltego.Company

EIG Network Operations

Weight	88
Name	EIG Network Operations

Info

Relevance:	0.88388
Count:	2

Incoming (1)

IPv4 Address	66.96.146.129

Snapshot

maltego.wayback.Snapshot

1999 Feb 03: http://evil.com:80/

Weight	1626382
Timestamp	19990203102243
Description	1999 Feb 03: http://evil.com:80/
Web Archive URL	https://web.archive.org/web/19990203102243/http://evil.com:80/
Original URL	http://evil.com:80/
DateTime	03 Feb 1999 10:22:43 +0000
HTTP Status	200
Short title	
URL	https://web.archive.org/web/19990203102243if_/http://evil.com:80/
Title	https://web.archive.org/web/19990203102243if_/http://evil.com:80/

Entity Data

Archived Page URL	https://web.archive.org/web/19990203102243if_/http://evil.com:80/
Web Archive URL	https://web.archive.org/web/19990203102243/http://evil.com:80/
Snapshot DateTime	03 Feb 1999 10:22:43 +0000
Original URL	http://evil.com:80/

Incoming (1)

Domain	evil.com

VirusTotal File

maltego.virustotal.File

9038431d73550aedf97d341faef1025c.virus

Weight	0
MeaningfulName	9038431d73550aedf97d341faef1025c.virus
File Id	dabf447e17bec4397c07c0782438d12d19eaaee09738c1095df4343b4906e10b
Names	9038431d73550aedf97d341faef1025c.virus
File Type	PEEXE
File Type Description	Win32 EXE
MD5	9038431d73550aedf97d341faef1025c
SHA-1	52b93015ced351b36ba87ebb6026edb686ffaf86
SHA-256	dabf447e17bec4397c07c0782438d12d19eaaee09738c1095df4343b4906e10b
Vhash	066056655d1c0510d043z8003d7z47z62z3ffz
Authentihash	27f38a3fd3d3c488ab9c9fbdaddf44df96a0fa73415245f6d308cc8b6700dc33
SSDEEP	196608:mT5mPKwy9tVUIDB9lAiwdSUmgeqP922CN1QORmaQM2:ybDlKSUxP82A1QONQM2
Magic	PE32 executable for MS Windows (GUI) Intel 80386 32-bit
File Size	6470077
Tags	nsis, peexe, overlay
Capability Tags	
Downloadable	null
Creation Date	2018-01-30T03:57:45Z
First Submission Date	2018-10-27T17:46:28Z
Last Submission Date	2018-10-27T17:46:28Z
Last Analysis Date	2021-10-09T07:28:11Z
Total Votes - Harmless	0
Total Votes - Malicious	0
Submissions	1
Reputation	0

View on VirusTotal

GUI Url:
https://www.virustotal.com/gui/file/dabf447e17bec4397c07c0782438d12d19eaaee09738c1095df4343b4906e10b

File Summary

Names	9038431d73550aedf97d341faef1025c.virus
File Type	peexe
File Type Description	Win32 EXE
Tags	nsis, peexe, overlay
Times Submitted	1

TrID - file type identification tool	
File Type	Probability %
NSIS - Nullsoft Scriptable Install System	92.9
Win32 Executable MS Visual C++ (generic)	3.4
Win64 Executable (generic)	1.1
Win32 Dynamic Link Library (generic)	0.7
Win16 NE executable (generic)	0.5

VirusTotal Analysis Summary	
Aggregate Result	malicious - 46 / 74

VirusTotal Analysis Stats	
Analysis Type	Number of Analysis
Confirmed Timeout	0
Failure	0
Harmless	0
Malicious	46
Suspicious	0
Timeout	0
Type Unsupported	5
Undetected	23
Total	**74**

Community Votes

Total votes cast: 0

Incoming (1)

	DNS Name	evil.com

Snapshot

maltego.wayback.Snapshot

1996 Dec 29: http://www.evil.com:80/

Weight	523016
Timestamp	19961229045648
Description	1996 Dec 29: http://www.evil.com:80/
Web Archive URL	https://web.archive.org/web/19961229045648/http://www.evil.com:80/
Original URL	http://www.evil.com:80/
DateTime	29 Dec 1996 04:56:48 +0000
HTTP Status	200
Short title	
URL	https://web.archive.org/web/19961229045648if_/http://www.evil.com:80/
Title	https://web.archive.org/web/19961229045648if_/http://www.evil.com:80/

Entity Data

Archived Page URL	https://web.archive.org/web/19961229045648if_/http://www.evil.com:80/
Web Archive URL	https://web.archive.org/web/19961229045648/http://www.evil.com:80/
Snapshot DateTime	29 Dec 1996 04:56:48 +0000
Original URL	http://www.evil.com:80/

Incoming (1)

Domain	evil.com

VirusTotal File

maltego.virustotal.File

15-bro-x32[1].exe

Weight	0
MeaningfulName	15-bro-x32[1].exe
File Id	ccb1f6be23be5f898f26eefb5d92cf940552c3383bd6896a6e519c131826ce00
Names	15-bro-x32[1].exe, 15-bro-x32.exe
File Type	PEEXE
File Type Description	Win32 EXE
MD5	962aeb518be347599495dcc5ab7db004
SHA-1	50d06b24abbd84443970b97e6829c09ff9187d3f
SHA-256	ccb1f6be23be5f898f26eefb5d92cf940552c3383bd6896a6e519c131826ce00
Vhash	026086655d151d1d151562c8zc8bz33z301001d031z38z2
Authentihash	8dbf28310b2f1c445cd80db27739c96e6e672314728bd552670110529a24d0fd
SSDEEP	49152:jgl7n8t0Cj72fsjgf+DJTGVh1s5QNLqXmN5:Yu9j7Ef+Y31CQNLCmN5
Magic	PE32 executable for MS Windows (GUI) Intel 80386 32-bit
File Size	2594528
Tags	peexe, signed, overlay
Capability Tags	
Downloadable	null
Creation Date	2018-07-24T17:24:30Z
First Submission Date	2021-09-15T22:59:19Z
Last Submission Date	2021-10-07T12:56:01Z
Last Analysis Date	2021-10-07T14:57:42Z
Total Votes - Harmless	0
Total Votes - Malicious	0
Submissions	6
Reputation	0

View on VirusTotal

GUI Url:
https://www.virustotal.com/gui/file/ccb1f6be23be5f898f26eefb5d92cf940552c3383bd6896a6e519c131826ce00

File Summary

Names	15-bro-x32[1].exe, 15-bro-x32.exe
File Type	peexe
File Type Description	Win32 EXE
Tags	peexe, signed, overlay
Times Submitted	6

TrID - file type identification tool

File Type	Probability %
Win32 Executable (generic)	42.7
OS/2 Executable (generic)	19.2
Generic Win/DOS Executable	19.0
DOS Executable Generic	18.9

VirusTotal Analysis Summary	
Aggregate Result	undetected - 67 / 73

VirusTotal Analysis Stats	
Analysis Type	Number of Analysis
Confirmed Timeout	0
Failure	0
Harmless	0
Malicious	1
Suspicious	0
Timeout	0
Type Unsupported	5
Undetected	67
Total	**73**

Community Votes

Total votes cast: 0

Incoming (1)

DNS Name	evil.com

Snapshot

maltego.wayback.Snapshot

1997 Feb 04: http://www.evil.com:80/

Weight	576027
Timestamp	19970204002710
Description	1997 Feb 04: http://www.evil.com:80/
Web Archive URL	https://web.archive.org/web/19970204002710/http://www.evil.com:80/
Original URL	http://www.evil.com:80/
DateTime	04 Feb 1997 00:27:10 +0000
HTTP Status	200
Short title	
URL	https://web.archive.org/web/19970204002710if_/http://www.evil.com:80/
Title	https://web.archive.org/web/19970204002710if_/http://www.evil.com:80/

Entity Data

Archived Page URL	https://web.archive.org/web/19970204002710if_/http://www.evil.com:80/
Web Archive URL	https://web.archive.org/web/19970204002710/http://www.evil.com:80/
Snapshot DateTime	04 Feb 1997 00:27:10 +0000
Original URL	http://www.evil.com:80/

Incoming (1)

Domain	evil.com

VirusTotal File

maltego.virustotal.File

Солодушкин_С_И_Разработка_программных_комплексов_на_языке_JavaScript.pdf

Weight	0
MeaningfulName	Солодушкин_С_И_Разработка_программных_комплексов_на_языке_JavaScript.pdf
File Id	035a5cf5b5b6e22ed640a34e656635548c8568e3bc34975a749d7c416636d353
Names	Солодушкин_С_И_Разработка_программных_комплексов_на_языке_JavaScript.pdf
File Type	PDF
File Type Description	PDF
MD5	6a7690827126e361376bf8e31d50d7f2
SHA-1	1a8ac15886f672b99d819b3670705942da6e00f8
SHA-256	035a5cf5b5b6e22ed640a34e656635548c8568e3bc34975a749d7c416636d353
Vhash	943a05649ade8a43adc184212b66c5176
Authentihash	
SSDEEP	393216:T5tpJAqJqQ+4IE/aB2+3bCi7mztUy4o0/XFale/fZq147+6DgWxUKvOlYn7kB:9tAqL+thBF3blGmoiVao/lmWakMi7kB
Magic	PDF document, version 1.3
File Size	20276375
Tags	pdf, autoaction, direct-cpu-clock-access, checks-user-input, detect-debug-environment, runtime-modules
Capability Tags	
Downloadable	null
Creation Date	2020-07-31T13:41:30Z
First Submission Date	2021-10-09T07:27:08Z
Last Submission Date	2021-10-09T07:27:08Z
Last Analysis Date	2021-10-10T08:40:58Z
Total Votes - Harmless	0
Total Votes - Malicious	0
Submissions	1
Reputation	0

View on VirusTotal

GUI Url:
https://www.virustotal.com/gui/file/035a5cf5b5b6e22ed640a34e656635548c8568e3bc34975a749d7c416636d353

File Summary

Names	_____JavaScript.pdf
File Type	pdf
File Type Description	PDF
Tags	pdf, autoaction, direct-cpu-clock-access, checks-user-input, detect-debug-environment, runtime-modules
Times Submitted	1

TrID - file type identification tool

File Type	Probability %
Adobe Portable Document Format	100.0

VirusTotal Analysis Summary

Aggregate Result	undetected - 59 / 72

VirusTotal Analysis Stats

Analysis Type	Number of Analysis
Confirmed Timeout	0
Failure	0
Harmless	0
Malicious	1
Suspicious	0
Timeout	0
Type Unsupported	12
Undetected	59
Total	**72**

Community Votes

Total votes cast: 0

Incoming (1)

DNS Name	evil.com

VirusTotal File

maltego.virustotal.File

SMServer_x32_Setup.exe

Weight	0
MeaningfulName	SMServer_x32_Setup.exe
File Id	19a9068af92894968f6f300dbff20107c4da99a02ad4c7ef3e0f030ccd15a3b6
Names	SMServer_x32_Setup, SMServer_x32_Setup.exe, 855472
File Type	PEEXE
File Type Description	Win32 EXE
MD5	a89dce381e18b6f9d86524f222de9067
SHA-1	3e6b242dd09b7a4b2949bac278bc3fb3052824cf
SHA-256	19a9068af92894968f6f300dbff20107c4da99a02ad4c7ef3e0f030ccd15a3b6
Vhash	018056651d15155270d020023009e6z120f5z804008e03dz
Authentihash	f59684e7a184d5b943ac1ca26d34b3765f124e424b87f0d8952b4047cd3e92dc
SSDEEP	3145728:IzP+NdF1Xq5/+oIDHowy01R3gK+mgCUNHCpXGmCmI3QbFO:NveYDoC1R347mWmCmIAbc
Magic	PE32 executable for MS Windows (GUI) Intel 80386 32-bit
File Size	106197720
Tags	peexe, signed, overlay
Capability Tags	
Downloadable	null
Creation Date	2015-10-21T08:05:29Z
First Submission Date	2016-05-28T05:06:48Z
Last Submission Date	2016-05-28T05:06:48Z
Last Analysis Date	2021-10-08T06:05:44Z
Total Votes - Harmless	0
Total Votes - Malicious	0
Submissions	1
Reputation	0

View on VirusTotal

GUI Url:
https://www.virustotal.com/gui/file/19a9068af92894968f6f300dbff20107c4da99a02ad4c7ef3e0f030ccd15a3b6

File Summary

Names	SMServer_x32_Setup, SMServer_x32_Setup.exe, 855472
File Type	peexe
File Type Description	Win32 EXE
Tags	peexe, signed, overlay
Times Submitted	1

TrID - file type identification tool

File Type	Probability %
Windows Control Panel Item (generic)	46.4
Windows ActiveX control	27.4
InstallShield setup	10.1
Win32 EXE PECompact compressed (generic)	9.7
Win64 Executable (generic)	2.4

VirusTotal Analysis Summary

Aggregate Result	undetected - 63 / 73

VirusTotal Analysis Stats

Analysis Type	Number of Analysis
Confirmed Timeout	0
Failure	0
Harmless	0
Malicious	2
Suspicious	0
Timeout	0
Type Unsupported	8
Undetected	63
Total	**73**

Community Votes

Total votes cast: 0

Incoming (1)

DNS	DNS Name	evil.com

VirusTotal File

maltego.virustotal.File

SMServer_x32_Setup.exe

Weight	0
MeaningfulName	SMServer_x32_Setup.exe
File Id	0d8324319dae838ed2a11672854d2e18baeeaa870ebed560a58c39d23fd90b9a
Names	SMServer_x32_Setup, SMServer_x32_Setup.exe, 828191
File Type	PEEXE
File Type Description	Win32 EXE
MD5	e4cd8dd09cf676f1126503fb4a1dd4b5
SHA-1	097917282f5eaa0f8677af39e80a44e0af78e1a9
SHA-256	0d8324319dae838ed2a11672854d2e18baeeaa870ebed560a58c39d23fd90b9a
Vhash	018056651d15155270d020023009e6z120f5z804008e03dz
Authentihash	984b6aa9691c135adfb97101d8c61b6d333f843389fff92560380376c95f6efa
SSDEEP	3145728:MzmrJakk7gathy01R3gK+mgCUNHCpXGmCmI3QbFj:XJEJL1R347mWmCmIAbZ
Magic	PE32 executable for MS Windows (GUI) Intel 80386 32-bit
File Size	104481272
Tags	peexe, signed, overlay
Capability Tags	
Downloadable	null
Creation Date	2015-10-21T08:05:29Z
First Submission Date	2016-04-02T02:58:21Z
Last Submission Date	2016-04-02T02:58:21Z
Last Analysis Date	2021-10-10T07:26:14Z
Total Votes - Harmless	0
Total Votes - Malicious	0
Submissions	1
Reputation	0

View on VirusTotal

GUI Url:
https://www.virustotal.com/gui/file/0d8324319dae838ed2a11672854d2e18baeeaa870ebed560a58c39d23fd90b9a

File Summary

Names	SMServer_x32_Setup, SMServer_x32_Setup.exe, 828191
File Type	peexe
File Type Description	Win32 EXE
Tags	peexe, signed, overlay
Times Submitted	1

TrID - file type identification tool

File Type	Probability %
Windows Control Panel Item (generic)	46.4
Windows ActiveX control	27.4
InstallShield setup	10.1
Win32 EXE PECompact compressed (generic)	9.7
Win64 Executable (generic)	2.4

VirusTotal Analysis Summary

Aggregate Result	undetected - 55 / 73

VirusTotal Analysis Stats

Analysis Type	Number of Analysis
Confirmed Timeout	1
Failure	0
Harmless	0
Malicious	3
Suspicious	0
Timeout	7
Type Unsupported	7
Undetected	55
Total	**73**

Community Votes

Total votes cast: 0

Incoming (1)

DNS	DNS Name	evil.com

VirusTotal File

maltego.virustotal.File

ddd7d622dc5517e202383bc7d02fb333ceac8b6f4b9c4bceef96a302b732297b

Weight	0
MeaningfulName	ddd7d622dc5517e202383bc7d02fb333ceac8b6f4b9c4bceef96a302b732297b
File Id	ddd7d622dc5517e202383bc7d02fb333ceac8b6f4b9c4bceef96a302b732297b
Names	
File Type	PEEXE
File Type Description	Win32 EXE
MD5	6f79991a3d6e04864582257a7bc7c9ca
SHA-1	84dbd826b54962d2ca112a23604d5c99fe9e503e
SHA-256	ddd7d622dc5517e202383bc7d02fb333ceac8b6f4b9c4bceef96a302b732297b
Vhash	066056655d5c05109043z8003b7z47z62z3e03dz
Authentihash	f2691f36351c61005676348584b20a5e0a1ef7963012af090e9ba298193f0819
SSDEEP	196608:uT5mPKwy9tVUIDB9lAiwdSUmgeqP922CN1QORmaQq:6bDlKSUxP82A1QONQq
Magic	PE32 executable for MS Windows (GUI) Intel 80386 32-bit
File Size	6309545
Tags	peexe, overlay
Capability Tags	
Downloadable	null
Creation Date	2009-12-05T22:50:52Z
First Submission Date	2018-09-23T10:48:05Z
Last Submission Date	2018-09-23T10:48:05Z
Last Analysis Date	2021-10-10T07:42:33Z
Total Votes - Harmless	0
Total Votes - Malicious	0
Submissions	1
Reputation	0

View on VirusTotal

GUI Url:
https://www.virustotal.com/gui/file/ddd7d622dc5517e202383bc7d02fb333ceac8b6f4b9c4bceef96a302b732297b

File Summary

Names	
File Type	peexe
File Type Description	Win32 EXE
Tags	peexe, overlay
Times Submitted	1

TrID - file type identification tool	
File Type	Probability %
NSIS - Nullsoft Scriptable Install System	91.3
Win32 Executable MS Visual C++ (generic)	3.3
Microsoft Visual C++ compiled executable (generic)	1.7
Win64 Executable (generic)	1.1
Win32 Dynamic Link Library (generic)	0.7

VirusTotal Analysis Summary	
Aggregate Result	malicious - 49 / 74

VirusTotal Analysis Stats	
Analysis Type	Number of Analysis
Confirmed Timeout	1
Failure	0
Harmless	0
Malicious	49
Suspicious	0
Timeout	0
Type Unsupported	5
Undetected	19
Total	**74**

Community Votes

Total votes cast: 0

Incoming (1)

	DNS Name	evil.com

VirusTotal File

maltego.virustotal.File

ebcd1eb0db969353c12284a3c36f958ff9ab6a9a1a113ea8a89cad0cefbf10f3

Weight	0
MeaningfulName	ebcd1eb0db969353c12284a3c36f958ff9ab6a9a1a113ea8a89cad0cefbf10f3
File Id	ebcd1eb0db969353c12284a3c36f958ff9ab6a9a1a113ea8a89cad0cefbf10f3
Names	1181801910DA045D7D5B33530ADD25BA
File Type	ANDROID
File Type Description	Android
MD5	1181801910da045d7d5b33530add25ba
SHA-1	a1f01f9e4b54ef23e36146eb0684f1140933895d
SHA-256	ebcd1eb0db969353c12284a3c36f958ff9ab6a9a1a113ea8a89cad0cefbf10f3
Vhash	fb2b00ce67a00676b7a3a3782fd48bb1
Authentihash	
SSDEEP	196608:pe10of5hdg5Q1q4ADNNg3FPeOH0CSoir+qmjdulJ7xhq1m27IftOFm5G/L/Tj3SH:U10gFq5hNqjNqm5uLf2EfQs5G/L/n3e
Magic	Zip archive data, at least v2.0 to extract
File Size	23623534
Tags	obfuscated, reflection, apk, runtime-modules, crypto, telephony, clipboard, android
Capability Tags	
Downloadable	null
Creation Date	
First Submission Date	2021-10-10T06:48:04Z
Last Submission Date	2021-10-10T06:48:04Z
Last Analysis Date	2021-10-10T08:51:30Z
Total Votes - Harmless	0
Total Votes - Malicious	0
Submissions	1
Reputation	0

View on VirusTotal

GUI Url:
https://www.virustotal.com/gui/file/ebcd1eb0db969353c12284a3c36f958ff9ab6a9a1a113ea8a89cad0cefbf10f3

File Summary

Names	1181801910DA045D7D5B33530ADD25BA
File Type	android
File Type Description	Android
Tags	obfuscated, reflection, apk, runtime-modules, crypto, telephony, clipboard, android
Times Submitted	1

TrID - file type identification tool	
File Type	Probability %
Android Package	32.4
SPSS Extension	25.3
Opera Widget	11.8
Java Archive	11.3
Sweet Home 3D design (generic)	8.8

VirusTotal Analysis Summary	
Aggregate Result	undetected - 60 / 73

VirusTotal Analysis Stats	
Analysis Type	Number of Analysis
Confirmed Timeout	0
Failure	0
Harmless	0
Malicious	2
Suspicious	0
Timeout	0
Type Unsupported	11
Undetected	60
Total	**73**

Community Votes

Total votes cast: 0

Incoming (1)

	DNS Name	evil.com

Snapshot

maltego.wayback.Snapshot

1998 Dec 12: http://www.evil.com:80/

Weight	1549608
Timestamp	19981212024814
Description	1998 Dec 12: http://www.evil.com:80/
Web Archive URL	https://web.archive.org/web/19981212024814/http://www.evil.com:80/
Original URL	http://www.evil.com:80/
DateTime	12 Dec 1998 02:48:14 +0000
HTTP Status	200
Short title	
URL	https://web.archive.org/web/19981212024814if_/http://www.evil.com:80/
Title	https://web.archive.org/web/19981212024814if_/http://www.evil.com:80/

Entity Data

Archived Page URL	https://web.archive.org/web/19981212024814if_/http://www.evil.com:80/
Web Archive URL	https://web.archive.org/web/19981212024814/http://www.evil.com:80/
Snapshot DateTime	12 Dec 1998 02:48:14 +0000
Original URL	http://www.evil.com:80/

Incoming (1)

Domain	evil.com

Snapshot

maltego.wayback.Snapshot

1998 Dec 05: http://www.evil.com:80/

Weight	1540712
Timestamp	19981205223243
Description	1998 Dec 05: http://www.evil.com:80/
Web Archive URL	https://web.archive.org/web/19981205223243/http://www.evil.com:80/
Original URL	http://www.evil.com:80/
DateTime	05 Dec 1998 22:32:43 +0000
HTTP Status	200
Short title	
URL	https://web.archive.org/web/19981205223243if_/http://www.evil.com:80/
Title	https://web.archive.org/web/19981205223243if_/http://www.evil.com:80/

Entity Data

Archived Page URL	https://web.archive.org/web/19981205223243if_/http://www.evil.com:80/
Web Archive URL	https://web.archive.org/web/19981205223243/http://www.evil.com:80/
Snapshot DateTime	05 Dec 1998 22:32:43 +0000
Original URL	http://www.evil.com:80/

Incoming (1)

Domain	evil.com

Snapshot

maltego.wayback.Snapshot

1999 Feb 02: http://www.evil.com:80/

Weight	1625026
Timestamp	19990202114649
Description	1999 Feb 02: http://www.evil.com:80/
Web Archive URL	https://web.archive.org/web/19990202114649/http://www.evil.com:80/
Original URL	http://www.evil.com:80/
DateTime	02 Feb 1999 11:46:49 +0000
HTTP Status	200
Short title	
URL	https://web.archive.org/web/19990202114649if_/http://www.evil.com:80/
Title	https://web.archive.org/web/19990202114649if_/http://www.evil.com:80/

Entity Data

Archived Page URL	https://web.archive.org/web/19990202114649if_/http://www.evil.com:80/
Web Archive URL	https://web.archive.org/web/19990202114649/http://www.evil.com:80/
Snapshot DateTime	02 Feb 1999 11:46:49 +0000
Original URL	http://www.evil.com:80/

Incoming (1)

Domain	evil.com

Domain

maltego.Domain

apitwitter.w3snoop.com

Weight	0
Domain Name	apitwitter.w3snoop.com
WHOIS Info	Admin City: Tempe Admin Country: US Admin Email: c9b5a1cf1d0c3764s@domainsbyproxy.com Admin Organization: Domains By Proxy, LLC Admin Postal Code: 85284 Admin State/Province: Arizona Creation Date: 2011-06-05T21:04:22Z Creation Date: 2011-06-06T02:04:22Z DNSSEC: unsigned Domain Name: W3SNOOP.COM Domain Status: clientDeleteProhibited http://www.icann.org/epp#clientDeleteProhibited Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited Domain Status: clientRenewProhibited http://www.icann.org/epp#clientRenewProhibited Domain Status: clientRenewProhibited https://icann.org/epp#clientRenewProhibited Domain Status: clientTransferProhibited http://www.icann.org/epp#clientTransferProhibited Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Domain Status: clientUpdateProhibited http://www.icann.org/epp#clientUpdateProhibited Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited Name Server: INDRI.EZOICNS.COM Name Server: SAOLA.EZOICNS.COM Registrant City: a7319ae5e6c95df5 Registrant Country: US Registrant Email: c9b5a1cf1d0c3764s@domainsbyproxy.com Registrant Fax Ext: 3432650ec337c945 Registrant Fax: 9fad764be0c7e95d Registrant Name: 80315b2e6ac1a801 Registrant Organization: b46a98a26fe2fd9f Registrant Phone Ext: 3432650ec337c945 Registrant Phone: d5f66d3a005b000d Registrant Postal Code: 052e5bd148f904f9 Registrant State/Province: 30bdd2917a604c83 Registrant Street: 037792fd5a6fe619 Registrant Street: d733533b6a6c0c21 Registrar Abuse Contact Email: abuse@godaddy.com Registrar Abuse Contact Phone: +1.4806242505 Registrar Abuse Contact Phone: 480-624-2505 Registrar IANA ID: 146 Registrar Registration Expiration Date: 2023-06-05T21:04:22Z Registrar URL: http://www.godaddy.com Registrar WHOIS Server: whois.godaddy.com Registrar: GoDaddy.com, LLC Registry Admin ID: Not Available From Registry Registry Domain ID: 1660071767_DOMAIN_COM-VRSN Registry Expiry Date: 2023-06-06T02:04:22Z Registry Registrant ID: Not Available From Registry Registry Tech ID: Not Available From Registry Tech City: Tempe Tech Country: US Tech Email: c9b5a1cf1d0c3764s@domainsbyproxy.com Tech Organization: Domains By Proxy, LLC Tech Postal Code: 85284 Tech State/Province: Arizona Updated Date: 2020-02-09T21:49:40Z Updated Date: 2020-02-10T04:49:41Z

VirusTotal Domain Summary

VirusTotal Reputation	0
Tags	

VirusTotal Analysis Summary	
Aggregate Result	harmless - 86 / 86

VirusTotal Analysis Stats	
Analysis Type	Number of Analysis
Confirmed Timeout	0
Failure	0
Harmless	86
Malicious	0
Suspicious	0
Timeout	0
Type Unsupported	0
Undetected	0
Total	**86**

View on VirusTotal

GUI Url: https://www.virustotal.com/gui/domain/apitwitter.w3snoop.com

Community Votes

Total votes cast: 0

Incoming (1)

	DNS Name	w3snoop.com

Snapshot

maltego.wayback.Snapshot

1997 Oct 14: http://www.evil.com:80/

Weight	939149
Timestamp	19971014042913
Description	1997 Oct 14: http://www.evil.com:80/
Web Archive URL	https://web.archive.org/web/19971014042913/http://www.evil.com:80/
Original URL	http://www.evil.com:80/
DateTime	14 Oct 1997 04:29:13 +0000
HTTP Status	200
Short title	
URL	https://web.archive.org/web/19971014042913if_/http://www.evil.com:80/
Title	https://web.archive.org/web/19971014042913if_/http://www.evil.com:80/

Entity Data	
Archived Page URL	https://web.archive.org/web/19971014042913if_/http://www.evil.com:80/
Web Archive URL	https://web.archive.org/web/19971014042913/http://www.evil.com:80/
Snapshot DateTime	14 Oct 1997 04:29:13 +0000
Original URL	http://www.evil.com:80/

Incoming (1)	
Domain	evil.com

Snapshot

maltego.wayback.Snapshot

1999 Jan 25: http://evil.com:80/

Weight	1613336
Timestamp	19990125085642
Description	1999 Jan 25: http://evil.com:80/
Web Archive URL	https://web.archive.org/web/19990125085642/http://evil.com:80/
Original URL	http://evil.com:80/
DateTime	25 Jan 1999 08:56:42 +0000
HTTP Status	200
Short title	
URL	https://web.archive.org/web/19990125085642if_/http://evil.com:80/
Title	https://web.archive.org/web/19990125085642if_/http://evil.com:80/

Entity Data	
Archived Page URL	https://web.archive.org/web/19990125085642if_/http://evil.com:80/
Web Archive URL	https://web.archive.org/web/19990125085642/http://evil.com:80/
Snapshot DateTime	25 Jan 1999 08:56:42 +0000
Original URL	http://evil.com:80/

Incoming (1)	
Domain	evil.com

Snapshot

maltego.wayback.Snapshot

1999 Jan 25: http://www.evil.com:80/

Weight	1613392
Timestamp	19990125095200
Description	1999 Jan 25: http://www.evil.com:80/
Web Archive URL	https://web.archive.org/web/19990125095200/http://www.evil.com:80/
Original URL	http://www.evil.com:80/
DateTime	25 Jan 1999 09:52:00 +0000
HTTP Status	200
Short title	
URL	https://web.archive.org/web/19990125095200if_/http://www.evil.com:80/
Title	https://web.archive.org/web/19990125095200if_/http://www.evil.com:80/

Entity Data

Archived Page URL	https://web.archive.org/web/19990125095200if_/http://www.evil.com:80/
Web Archive URL	https://web.archive.org/web/19990125095200/http://www.evil.com:80/
Snapshot DateTime	25 Jan 1999 09:52:00 +0000
Original URL	http://www.evil.com:80/

Incoming (1)

Domain	evil.com

VirusTotal File

maltego.virustotal.File

VpnSetup.exe

Weight	0
MeaningfulName	VpnSetup.exe
File Id	e4d8615b5e864ceb85968e83d69e6d16d12298c5e7557da420c967e73f1be679
Names	VpnSetup.exe
File Type	PEEXE
File Type Description	Win32 EXE
MD5	057b03dceac4867dc3c5551f95caa609
SHA-1	66c4a8a40e3cbad15ea928b396a0cb14e26806b8
SHA-256	e4d8615b5e864ceb85968e83d69e6d16d12298c5e7557da420c967e73f1be679
Vhash	28603675651200732311380922
Authentihash	e6bb6b20ed2c68c3c4a99fc33ec67ae99b04ea9fface7564b6ee711e6125091a
SSDEEP	196608:Hki7Gv6snkMyT/T5mPKwy9tVUIDB9lxz6V8zgeQvnR/ka22CJUORmuX1:Hki7G5VyT3bDlxuPvlkJ25OVl
Magic	PE32 executable for MS Windows (GUI) Intel 80386 Mono/.Net assembly
File Size	8280064
Tags	peexe, runtime-modules, assembly, direct-cpu-clock-access, detect-debug-environment
Capability Tags	
Downloadable	null
Creation Date	2021-05-05T10:27:43Z
First Submission Date	2021-05-05T19:55:15Z
Last Submission Date	2021-05-05T19:55:15Z
Last Analysis Date	2021-10-03T08:07:57Z
Total Votes - Harmless	0
Total Votes - Malicious	0
Submissions	1
Reputation	0

View on VirusTotal

GUI Url:
https://www.virustotal.com/gui/file/e4d8615b5e864ceb85968e83d69e6d16d12298c5e7557da420c967e73f1be679

File Summary

Names	VpnSetup.exe
File Type	peexe
File Type Description	Win32 EXE
Tags	peexe, runtime-modules, assembly, direct-cpu-clock-access, detect-debug-environment
Times Submitted	1

TrID - file type identification tool

File Type	Probability %
NSIS - Nullsoft Scriptable Install System	70.9
Windows Control Panel Item (generic)	16.5
Generic CIL Executable (.NET, Mono, etc.)	6.1
InstallShield setup	3.6
Win64 Executable (generic)	0.8

VirusTotal Analysis Summary

Aggregate Result	undetected - 59 / 70

VirusTotal Analysis Stats

Analysis Type	Number of Analysis
Confirmed Timeout	1
Failure	1
Harmless	0
Malicious	3
Suspicious	0
Timeout	1
Type Unsupported	5
Undetected	59
Total	**70**

Community Votes

Total votes cast: 0

Incoming (1)

DNS Name	evil.com

VirusTotal File

maltego.virustotal.File

15-bro-x32.exe

Weight	0
MeaningfulName	15-bro-x32.exe
File Id	597bc9282c227fc08fa6738a0a70d0e9113edc17982962b8e6cd6f0a3d3c9f0f
Names	15-bro-x32.exe
File Type	PEEXE
File Type Description	Win32 EXE
MD5	2e971746fb158593fa5b29e0656b9b60
SHA-1	1637aa453b349cbc45bcae8b9cd37b9166df0297
SHA-256	597bc9282c227fc08fa6738a0a70d0e9113edc17982962b8e6cd6f0a3d3c9f0f
Vhash	026086655d151d1d151562c8zc8bz33z301001d031z38z2
Authentihash	1dc62df1a060985c6dab6b00e25e13e6e1994e4d7a599afef6d941d2b65cad9f
SSDEEP	49152:rgl7n8t0Cj72fsjgf+DJTGVg4d5fEbqXmNG:gu9j7Ef+Ye43fEbCmNG
Magic	PE32 executable for MS Windows (GUI) Intel 80386 32-bit
File Size	2594528
Tags	peexe, signed, overlay
Capability Tags	
Downloadable	null
Creation Date	2018-07-24T17:24:30Z
First Submission Date	2021-08-30T14:18:04Z
Last Submission Date	2021-08-30T14:18:04Z
Last Analysis Date	2021-10-03T16:55:07Z
Total Votes - Harmless	0
Total Votes - Malicious	0
Submissions	1
Reputation	0

View on VirusTotal

GUI Url:
https://www.virustotal.com/gui/file/597bc9282c227fc08fa6738a0a70d0e9113edc17982962b8e6cd6f0a3d3c9f0f

File Summary

Names	15-bro-x32.exe
File Type	peexe
File Type Description	Win32 EXE
Tags	peexe, signed, overlay
Times Submitted	1

TrID - file type identification tool

File Type	Probability %
Win32 Executable (generic)	42.7
OS/2 Executable (generic)	19.2
Generic Win/DOS Executable	19.0
DOS Executable Generic	18.9

VirusTotal Analysis Summary	
Aggregate Result	undetected - 66 / 73

VirusTotal Analysis Stats	
Analysis Type	Number of Analysis
Confirmed Timeout	0
Failure	1
Harmless	0
Malicious	1
Suspicious	0
Timeout	0
Type Unsupported	5
Undetected	66
Total	**73**

Community Votes

Total votes cast: 0

Incoming (1)

	DNS Name	evil.com

VirusTotal File

maltego.virustotal.File

VpnSetup.exe

Weight	0
MeaningfulName	VpnSetup.exe
File Id	f9f7fe45c4ed2522cc78c1b803ce752fb8b2d58a36db34f1eb5857e74d8ae888
Names	VpnSetup.exe, c0cc5cc963cc4830800d3e4631ad2053cae49275.exe, InvinciBull 2.15.11.22431.exe, InvinciBull.exe
File Type	PEEXE
File Type Description	Win32 EXE
MD5	1326ab0be31e3bdae2e9b8c333505a0c
SHA-1	c0cc5cc963cc4830800d3e4631ad2053cae49275
SHA-256	f9f7fe45c4ed2522cc78c1b803ce752fb8b2d58a36db34f1eb5857e74d8ae888
Vhash	0760566d55557560e013z1005214kz1e03dz
Authentihash	1724a7bad20582b8a303d7ebcce08e48ea16befc97bd959cc766892ce2062ed3
SSDEEP	196608:kyX60bMXrYWtmR/1xxhtfZiAb777WbxGFIFdMKrLt6cVudQFZ1lq2:epXcxig7XoTdzLwc0QG2
Magic	PE32 executable for MS Windows (GUI) Intel 80386 32-bit
File Size	7767008
Tags	peexe, overlay, runtime-modules, signed, detect-debug-environment, direct-cpu-clock-access, checks-disk-space, persistence
Capability Tags	
Downloadable	null
Creation Date	2018-01-01T04:48:28Z
First Submission Date	2021-05-05T16:29:03Z
Last Submission Date	2021-05-05T16:29:03Z
Last Analysis Date	2021-10-03T08:06:41Z
Total Votes - Harmless	0
Total Votes - Malicious	0
Submissions	1
Reputation	0

View on VirusTotal

GUI Url:
https://www.virustotal.com/gui/file/f9f7fe45c4ed2522cc78c1b803ce752fb8b2d58a36db34f1eb5857e74d8ae888

File Summary

Names	VpnSetup.exe, c0cc5cc963cc4830800d3e4631ad2053cae49275.exe, InvinciBull 2.15.11.22431.exe, InvinciBull.exe
File Type	peexe
File Type Description	Win32 EXE
Tags	peexe, overlay, runtime-modules, signed, detect-debug-environment, direct-cpu-clock-access, checks-disk-space, persistence
Times Submitted	1

TrID - file type identification tool	
File Type	Probability %
Windows Control Panel Item (generic)	61.4
InstallShield setup	13.4
Win32 Executable MS Visual C++ (generic)	9.7
Microsoft Visual C++ compiled executable (generic)	5.1
Win64 Executable (generic)	3.2

VirusTotal Analysis Summary	
Aggregate Result	undetected - 65 / 73

VirusTotal Analysis Stats	
Analysis Type	Number of Analysis
Confirmed Timeout	1
Failure	0
Harmless	0
Malicious	2
Suspicious	0
Timeout	0
Type Unsupported	5
Undetected	65
Total	**73**

Community Votes

Total votes cast: 0

Incoming (1)

	DNS Name	evil.com

VirusTotal File

maltego.virustotal.File

BlackBelt Privacy PostFF57 10.2021.10.1.exe

Weight	0
MeaningfulName	BlackBelt Privacy PostFF57 10.2021.10.1.exe
File Id	f5a50a1ef1367a28d6ea8dc0f61a268100c608b981ae15a526ba28937f524ba4
Names	BlackBelt Privacy PostFF57 10.2021.10.1.exe, BlackBelt%20Privacy%20PostFF57%2010.2021.10.1.exe, downloads.sourceforge.net, netcologne.dl.sourceforge.net
File Type	PEEXE
File Type Description	Win32 EXE
MD5	34fc72b036adda52a0cfeec7f7cf3027
SHA-1	7ef44021f97f63a6f961984074dc326981bf18cb
SHA-256	f5a50a1ef1367a28d6ea8dc0f61a268100c608b981ae15a526ba28937f524ba4
Vhash	0370866d1c0d1c051505105016z1c9z5bz1fz
Authentihash	8b0808d53155f922a21293cb729b0d4e04066ea1ebd9c668c819a2dd624cfa99
SSDEEP	393216:/6Ra7WSR/NgizycKLeuSiJIxMx2AaL//ak6wQhSnAVqXLTFt1uq:/6Ra7WUlgQuqKuxi0//ak6xZqX3Psq
Magic	PE32 executable for MS Windows (GUI) Intel 80386 32-bit
File Size	30094623
Tags	peexe, overlay, runtime-modules, detect-debug-environment, calls-wmi, direct-cpu-clock-access, persistence
Capability Tags	
Downloadable	null
Creation Date	1992-06-19T22:22:17Z
First Submission Date	2021-10-05T23:09:07Z
Last Submission Date	2021-10-06T23:35:55Z
Last Analysis Date	2021-10-11T04:37:29Z
Total Votes - Harmless	0
Total Votes - Malicious	0
Submissions	5
Reputation	0

View on VirusTotal

GUI Url:
https://www.virustotal.com/gui/file/f5a50a1ef1367a28d6ea8dc0f61a268100c608b981ae15a526ba28937f524ba4

File Summary

Names	BlackBelt Privacy PostFF57 10.2021.10.1.exe, BlackBelt%20Privacy%20PostFF57%2010.2021.10.1.exe, downloads.sourceforge.net, netcologne.dl.sourceforge.net
File Type	peexe
File Type Description	Win32 EXE
Tags	peexe, overlay, runtime-modules, detect-debug-environment, calls-wmi, direct-cpu-clock-access, persistence
Times Submitted	5

TrID - file type identification tool	
File Type	Probability %
Inno Setup installer	70.2
Win32 Executable Delphi generic	9.0
Windows screen saver	8.3
Win32 Dynamic Link Library (generic)	4.2
Win32 Executable (generic)	2.8

VirusTotal Analysis Summary	
Aggregate Result	undetected - 58 / 71

VirusTotal Analysis Stats	
Analysis Type	Number of Analysis
Confirmed Timeout	0
Failure	0
Harmless	0
Malicious	7
Suspicious	0
Timeout	0
Type Unsupported	6
Undetected	58
Total	**71**

Community Votes

Total votes cast: 0

Incoming (1)

	DNS Name	evil.com

VirusTotal File

maltego.virustotal.File

Release NDD NFS-e Core_6103_26290.exe

Weight	0
MeaningfulName	Release NDD NFS-e Core_6103_26290.exe
File Id	f6c51a3fb750f2839a38b84c73e4242139459f7679d42f37287b6cc303849146
Names	Release NDD NFS-e Core_6103_26290.exe
File Type	PEEXE
File Type Description	Win32 EXE
MD5	85a2ddc747777b7e14695bb09cdd7052
SHA-1	a83d1bd2b3136095925a51e5164a4e7a16f4dd95
SHA-256	f6c51a3fb750f2839a38b84c73e4242139459f7679d42f37287b6cc303849146
Vhash	057056655d5c05109043z8003b7z47z62z3e03dz
Authentihash	80e7b99405d838f359409d2ff786ddc883f1a9e69c6353dc353ab8d178ec36df
SSDEEP	1572864:zOMVASu/gJBI11UPnBu4F/vyUt5Pmz94XxbVkyK:yAASu/gJBgUPISvyw53XxbOyK
Magic	PE32 executable for MS Windows (GUI) Intel 80386 32-bit
File Size	53034859
Tags	peexe, overlay, direct-cpu-clock-access, runtime-modules
Capability Tags	
Downloadable	null
Creation Date	2009-12-05T22:50:52Z
First Submission Date	2021-10-05T18:37:01Z
Last Submission Date	2021-10-05T18:37:01Z
Last Analysis Date	2021-10-06T19:45:59Z
Total Votes - Harmless	0
Total Votes - Malicious	0
Submissions	1
Reputation	0

View on VirusTotal

GUI Url:
https://www.virustotal.com/gui/file/f6c51a3fb750f2839a38b84c73e4242139459f7679d42f37287b6cc303849146

File Summary

Names	Release NDD NFS-e Core_6103_26290.exe
File Type	peexe
File Type Description	Win32 EXE
Tags	peexe, overlay, direct-cpu-clock-access, runtime-modules
Times Submitted	1

TrID - file type identification tool	
File Type	Probability %
NSIS - Nullsoft Scriptable Install System	92.9
Win32 Executable MS Visual C++ (generic)	3.4
Win64 Executable (generic)	1.1
Win32 Dynamic Link Library (generic)	0.7
Win16 NE executable (generic)	0.5

VirusTotal Analysis Summary	
Aggregate Result	undetected - 60 / 71

VirusTotal Analysis Stats	
Analysis Type	Number of Analysis
Confirmed Timeout	0
Failure	0
Harmless	0
Malicious	1
Suspicious	0
Timeout	2
Type Unsupported	8
Undetected	60
Total	**71**

Community Votes

Total votes cast: 0

Incoming (1)

	DNS Name	evil.com

Snapshot

maltego.wayback.Snapshot

2000 Jun 21: http://www.evil.com:80/

Weight	2351657
Timestamp	20000621021710
Description	2000 Jun 21: http://www.evil.com:80/
Web Archive URL	https://web.archive.org/web/20000621021710/http://www.evil.com:80/
Original URL	http://www.evil.com:80/
DateTime	21 Jun 2000 02:17:10 +0000
HTTP Status	200
Short title	
URL	https://web.archive.org/web/20000621021710if_/http://www.evil.com:80/
Title	https://web.archive.org/web/20000621021710if_/http://www.evil.com:80/

Entity Data

Archived Page URL	https://web.archive.org/web/20000621021710if_/http://www.evil.com:80/
Web Archive URL	https://web.archive.org/web/20000621021710/http://www.evil.com:80/
Snapshot DateTime	21 Jun 2000 02:17:10 +0000
Original URL	http://www.evil.com:80/

Incoming (1)

Domain	evil.com

IPv4 Address

maltego.IPv4Address

69.172.201.153

Weight	0
IP Address	69.172.201.153
Internal	false
Date Resolved	2020-02-03T06:30:54Z
Resolver	VirusTotal

Incoming (1)

DNS Name	evil.co

Snapshot

maltego.wayback.Snapshot

2000 Apr 07: http://www.evil.com:80/

Weight	2244013
Timestamp	20000407081324
Description	2000 Apr 07: http://www.evil.com:80/
Web Archive URL	https://web.archive.org/web/20000407081324/http://www.evil.com:80/
Original URL	http://www.evil.com:80/
DateTime	07 Apr 2000 08:13:24 +0000
HTTP Status	200
Short title	
URL	https://web.archive.org/web/20000407081324if_/http://www.evil.com:80/
Title	https://web.archive.org/web/20000407081324if_/http://www.evil.com:80/

Entity Data

Archived Page URL	https://web.archive.org/web/20000407081324if_/http://www.evil.com:80/
Web Archive URL	https://web.archive.org/web/20000407081324/http://www.evil.com:80/
Snapshot DateTime	07 Apr 2000 08:13:24 +0000
Original URL	http://www.evil.com:80/

Incoming (1)

Domain	evil.com

WHOIS Record

maltego.WHOISRecord

www.evil.com

Weight	0
Name	www.evil.com
WHOIS Info	Name Server: NS1.VERIO.COM | NS2.VERIO.COM Registrar IANA ID: 2 Registrar Abuse Contact Phone: +1.8003337680 DNSSEC: unsigned Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited | clientTransferProhibited https://icann.org/epp#clientTransferProhibited | clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited Creation Date: 1995-04-10T04:00:00Z Registrar URL: http://networksolutions.com Registrar WHOIS Server: whois.networksolutions.com Updated Date: 2018-12-04T14:57:04Z Registrar: Network Solutions, LLC Domain Name: EVIL.COM Registrar Abuse Contact Email: abuse@web.com Registry Domain ID: 1040763_DOMAIN_COM-VRSN Registry Expiry Date: 2020-04-11T04:00:00Z
Registry Domain ID	1040763_DOMAIN_COM-VRSN
Domain Name	EVIL.COM
Created Date	1995-04-10T04:00:00Z
Registry Expiry Date	2020-04-11T04:00:00Z
Updated Date	2018-12-04T14:57:04Z
Transfer Date	
Nameservers	NS1.VERIO.COM | NS2.VERIO.COM
Name Server IP Addresses	
Mantainer	
Created By	
Updated By	
DNSSEC	unsigned
Domain Status	clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited | clientTransferProhibited https://icann.org/epp#clientTransferProhibited | clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
ENS AuthId	
Registry Registrant ID	
Registrant Name	
Registrant Organization	
Registrant Address	
Registrant Street	
Registrant City	
Registrant State/Province	
Registrant Country	
Registrant Country Code	
Registrant Postal Code	
Registrant Phone	
Registrant Phone Ext	
Registrant Fax	
Registrant Fax Ext	
Registrant Email	
Admin ID	
Admin ID	
Admin Name	
Admin Organization	
Admin Address	
Admin Street	
Admin City	

Admin City	
Admin State/Province	
Admin Country	
Admin Country Code	
Admin Postal Code	
Admin Phone	
Admin Phone Ext	
Admin Fax	
Admin Fax Ext	
Admin Email	
Tech ID	
Tech Name	
Tech Organization	
Tech Address	
Tech City	
Tech State/Province	
Tech Country	
Tech Postal Code	
Tech Phone	
Tech Phone Ext	
Tech Fax	
Tech Fax Ext	
Tech Email	
Registrar ID	
Registrar IANA ID	2
Registrar	Network Solutions, LLC
Registrar Registration Expiration Date	
Registrar URL	http://networksolutions.com
Registrar WHOIS Server	whois.networksolutions.com
Registrar Status	
Registrar Address	
Registrar City	
Registrar State/Province	
Registrar Country	
Registrar Postal Code	
Registrar Phone	
Registrar Fax	
Registrar Fax Ext	
Registrar Email	
Registrar Abuse Contact Email	abuse@web.com
Registrar Abuse Contact Phone	+1.8003337680
Sponsoring Registrar	

Whois Information	
Name Server	NS1.VERIO.COM | NS2.VERIO.COM
Registrar IANA ID	2
Registrar Abuse Contact Phone	+1.8003337680
DNSSEC	unsigned
Domain Status	clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited | clientTransferProhibited https://icann.org/epp#clientTransferProhibited | clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
Creation Date	1995-04-10T04:00:00Z
Registrar URL	http://networksolutions.com
Registrar WHOIS Server	whois.networksolutions.com
Updated Date	2018-12-04T14:57:04Z
Registrar	Network Solutions, LLC
Domain Name	EVIL.COM
Registrar Abuse Contact Email	abuse@web.com
Registry Domain ID	1040763_DOMAIN_COM-VRSN
Registry Expiry Date	2020-04-11T04:00:00Z

Incoming (1)	
DNS Name	www.evil.com

Snapshot

maltego.wayback.Snapshot

2000 Oct 17: http://www.evil.com:80/

Weight	2522314
Timestamp	20001017143438
Description	2000 Oct 17: http://www.evil.com:80/
Web Archive URL	https://web.archive.org/web/20001017143438/http://www.evil.com:80/
Original URL	http://www.evil.com:80/
DateTime	17 Oct 2000 14:34:38 +0000
HTTP Status	200
Short title	
URL	https://web.archive.org/web/20001017143438if_/http://www.evil.com:80/
Title	https://web.archive.org/web/20001017143438if_/http://www.evil.com:80/

Entity Data	
Archived Page URL	https://web.archive.org/web/20001017143438if_/http://www.evil.com:80/
Web Archive URL	https://web.archive.org/web/20001017143438/http://www.evil.com:80/
Snapshot DateTime	17 Oct 2000 14:34:38 +0000
Original URL	http://www.evil.com:80/

Incoming (1)	
Domain	evil.com

WHOIS Record

maltego.WHOISRecord

www.evil.com

Weight	0
Name	www.evil.com
WHOIS Info	Name Server: NS1.VERIO.COM | NS2.VERIO.COM Registrar IANA ID: 2 Registrar Abuse Contact Phone: +1.8003337680 DNSSEC: unsigned Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited | clientTransferProhibited https://icann.org/epp#clientTransferProhibited | clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited Creation Date: 1995-04-10T04:00:00Z Registrar URL: http://networksolutions.com Registrar WHOIS Server: whois.networksolutions.com Updated Date: 2019-12-17T16:17:59Z Registrar: Network Solutions, LLC Domain Name: EVIL.COM Registrar Abuse Contact Email: abuse@web.com Registry Domain ID: 1040763_DOMAIN_COM-VRSN Registry Expiry Date: 2023-04-11T04:00:00Z
Registry Domain ID	1040763_DOMAIN_COM-VRSN
Domain Name	EVIL.COM
Created Date	1995-04-10T04:00:00Z
Registry Expiry Date	2023-04-11T04:00:00Z
Updated Date	2019-12-17T16:17:59Z
Transfer Date	
Nameservers	NS1.VERIO.COM | NS2.VERIO.COM
Name Server IP Addresses	
Mantainer	
Created By	
Updated By	
DNSSEC	unsigned
Domain Status	clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited | clientTransferProhibited https://icann.org/epp#clientTransferProhibited | clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
ENS AuthId	
Registry Registrant ID	
Registrant Name	
Registrant Organization	
Registrant Address	
Registrant Street	
Registrant City	
Registrant State/Province	
Registrant Country	
Registrant Country Code	
Registrant Postal Code	
Registrant Phone	
Registrant Phone Ext	
Registrant Fax	
Registrant Fax Ext	
Registrant Email	
Admin ID	
Admin ID	
Admin Name	
Admin Organization	
Admin Address	
Admin Street	
Admin City	

Admin City	
Admin State/Province	
Admin Country	
Admin Country Code	
Admin Postal Code	
Admin Phone	
Admin Phone Ext	
Admin Fax	
Admin Fax Ext	
Admin Email	
Tech ID	
Tech Name	
Tech Organization	
Tech Address	
Tech City	
Tech State/Province	
Tech Country	
Tech Postal Code	
Tech Phone	
Tech Phone Ext	
Tech Fax	
Tech Fax Ext	
Tech Email	
Registrar ID	
Registrar IANA ID	2
Registrar	Network Solutions, LLC
Registrar Registration Expiration Date	
Registrar URL	http://networksolutions.com
Registrar WHOIS Server	whois.networksolutions.com
Registrar Status	
Registrar Address	
Registrar City	
Registrar State/Province	
Registrar Country	
Registrar Postal Code	
Registrar Phone	
Registrar Fax	
Registrar Fax Ext	
Registrar Email	
Registrar Abuse Contact Email	abuse@web.com
Registrar Abuse Contact Phone	+1.8003337680
Sponsoring Registrar	

Whois Information	
Name Server	NS1.VERIO.COM | NS2.VERIO.COM
Registrar IANA ID	2
Registrar Abuse Contact Phone	+1.8003337680
DNSSEC	unsigned
Domain Status	clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited | clientTransferProhibited https://icann.org/epp#clientTransferProhibited | clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
Creation Date	1995-04-10T04:00:00Z
Registrar URL	http://networksolutions.com
Registrar WHOIS Server	whois.networksolutions.com
Updated Date	2019-12-17T16:17:59Z
Registrar	Network Solutions, LLC
Domain Name	EVIL.COM
Registrar Abuse Contact Email	abuse@web.com
Registry Domain ID	1040763_DOMAIN_COM-VRSN
Registry Expiry Date	2023-04-11T04:00:00Z

Incoming (1)	
DNS Name	www.evil.com

Snapshot

maltego.wayback.Snapshot

2000 Jun 21: http://www.evil.com:80/

Weight	2351778
Timestamp	20000621041818
Description	2000 Jun 21: http://www.evil.com:80/
Web Archive URL	https://web.archive.org/web/20000621041818/http://www.evil.com:80/
Original URL	http://www.evil.com:80/
DateTime	21 Jun 2000 04:18:18 +0000
HTTP Status	200
Short title	
URL	https://web.archive.org/web/20000621041818if_/http://www.evil.com:80/
Title	https://web.archive.org/web/20000621041818if_/http://www.evil.com:80/

Entity Data	
Archived Page URL	https://web.archive.org/web/20000621041818if_/http://www.evil.com:80/
Web Archive URL	https://web.archive.org/web/20000621041818/http://www.evil.com:80/
Snapshot DateTime	21 Jun 2000 04:18:18 +0000
Original URL	http://www.evil.com:80/

Incoming (1)	
Domain	evil.com

WHOIS Record

maltego.WHOISRecord

www.evil.com

Weight	0
Name	www.evil.com
WHOIS Info	Tech Email: 7599906c332e348as@networksolutionsprivateregistration.com Registrant Postal Code: ecc83fcbe503dd84 Admin Country: US Registrant Organization: 3432650ec337c945 Registrant Name: 8792ba892fc41135 Registrar Registration Expiration Date: 2020-04-11T04:00:00Z Registrant Fax: 3432650ec337c945 Registrar IANA ID: 2 DNSSEC: unsigned Creation Date: 1995-04-10T04:00:00Z Updated Date: 2017-12-20T05:26:25Z | 2018-12-04T14:57:04Z Admin City: Jacksonville Tech Country: US Tech Postal Code: 32256 Registrant Email: 269cfbd588b9739bs@networksolutionsprivateregistration.com Admin Postal Code: 32256 Admin State/Province: FL Admin Email: 269cfbd588b9739bs@networksolutionsprivateregistration.com Registrar URL: http://networksolutions.com Registrant City: 55985aaef9d91102 Registrar: Network Solutions, LLC Registrant Fax Ext: 3432650ec337c945 Registrant State/Province: 6eb233f5a5adbed8 Registry Domain ID: 1040763_DOMAIN_COM-VRSN Registrant Phone: 40171cfbdb8fe780 Tech City: Jacksonville Registry Expiry Date: 2020-04-11T04:00:00Z Name Server: NS1.VERIO.COM | NS2.VERIO.COM Registrar Abuse Contact Phone: +1.8003337680 Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited | clientTransferProhibited https://icann.org/epp#clientTransferProhibited | clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited Registrant Phone Ext: 3432650ec337c945 Registrar WHOIS Server: whois.networksolutions.com Registrant Street: 8f73e9118a9c558c Registrar Abuse Contact Email: abuse@web.com Registrant Country: US Tech State/Province: FL Domain Name: EVIL.COM
Registry Domain ID	1040763_DOMAIN_COM-VRSN
Domain Name	EVIL.COM
Created Date	1995-04-10T04:00:00Z
Registry Expiry Date	2020-04-11T04:00:00Z
Updated Date	2017-12-20T05:26:25Z | 2018-12-04T14:57:04Z
Transfer Date	
Nameservers	NS1.VERIO.COM | NS2.VERIO.COM
Name Server IP Addresses	
Mantainer	
Created By	
Updated By	
DNSSEC	unsigned
Domain Status	clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited | clientTransferProhibited https://icann.org/epp#clientTransferProhibited | clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
ENS AuthId	
Registry Registrant ID	
Registrant Name	8792ba892fc41135
Registrant Organization	3432650ec337c945
Registrant Address	
Registrant Street	8f73e9118a9c558c
Registrant City	55985aaef9d91102

Registrant State/Province	6eb233f5a5adbed8
Registrant Country	US
Registrant Country Code	
Registrant Postal Code	ecc83fcbe503dd84
Registrant Phone	40171cfbdb8fe780
Registrant Phone Ext	3432650ec337c945
Registrant Fax	3432650ec337c945
Registrant Fax Ext	3432650ec337c945
Registrant Email	269cfbd588b9739bs@networksolutionsprivateregistration.com
Admin ID	
Admin ID	
Admin Name	
Admin Organization	
Admin Address	
Admin Street	
Admin City	Jacksonville
Admin State/Province	FL
Admin Country	US
Admin Country Code	
Admin Postal Code	32256
Admin Phone	
Admin Phone Ext	
Admin Fax	
Admin Fax Ext	
Admin Email	269cfbd588b9739bs@networksolutionsprivateregistration.com
Tech ID	
Tech Name	
Tech Organization	
Tech Address	
Tech City	Jacksonville
Tech State/Province	FL
Tech Country	US
Tech Postal Code	32256
Tech Phone	
Tech Phone Ext	
Tech Fax	
Tech Fax Ext	
Tech Email	7599906c332e348as@networksolutionsprivateregistration.com
Registrar ID	
Registrar IANA ID	2
Registrar	Network Solutions, LLC
Registrar Registration Expiration Date	2020-04-11T04:00:00Z
Registrar URL	http://networksolutions.com
Registrar WHOIS Server	whois.networksolutions.com
Registrar Status	
Registrar Address	
Registrar City	
Registrar State/Province	
Registrar Country	
Registrar Postal Code	

Registrar Postal Code	
Registrar Phone	
Registrar Fax	
Registrar Fax Ext	
Registrar Email	
Registrar Abuse Contact Email	abuse@web.com
Registrar Abuse Contact Phone	+1.8003337680
Sponsoring Registrar	

Whois Information

Tech Email	7599906c332e348as@networksolutionsprivateregistration.com
Registrant Postal Code	ecc83fcbe503dd84
Admin Country	US
Registrant Organization	3432650ec337c945
Registrant Name	8792ba892fc41135
Registrar Registration Expiration Date	2020-04-11T04:00:00Z
Registrant Fax	3432650ec337c945
Registrar IANA ID	2
DNSSEC	unsigned
Creation Date	1995-04-10T04:00:00Z
Updated Date	2017-12-20T05:26:25Z | 2018-12-04T14:57:04Z
Admin City	Jacksonville
Tech Country	US
Tech Postal Code	32256
Registrant Email	269cfbd588b9739bs@networksolutionsprivateregistration.com
Admin Postal Code	32256
Admin State/Province	FL
Admin Email	269cfbd588b9739bs@networksolutionsprivateregistration.com
Registrar URL	http://networksolutions.com
Registrant City	55985aaef9d91102
Registrar	Network Solutions, LLC
Registrant Fax Ext	3432650ec337c945
Registrant State/Province	6eb233f5a5adbed8
Registry Domain ID	1040763_DOMAIN_COM-VRSN
Registrant Phone	40171cfbdb8fe780
Tech City	Jacksonville
Registry Expiry Date	2020-04-11T04:00:00Z
Name Server	NS1.VERIO.COM | NS2.VERIO.COM
Registrar Abuse Contact Phone	+1.8003337680

Domain Status	clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited | clientTransferProhibited https://icann.org/epp#clientTransferProhibited | clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
Registrant Phone Ext	3432650ec337c945
Registrar WHOIS Server	whois.networksolutions.com
Registrant Street	8f73e9118a9c558c
Registrar Abuse Contact Email	abuse@web.com
Registrant Country	US
Tech State/Province	FL
Domain Name	EVIL.COM

Incoming (1)

DNS Name	www.evil.com

Snapshot

maltego.wayback.Snapshot

2000 May 11: http://www.evil.com:80/

Weight	2293442
Timestamp	20000511160231
Description	2000 May 11: http://www.evil.com:80/
Web Archive URL	https://web.archive.org/web/20000511160231/http://www.evil.com:80/
Original URL	http://www.evil.com:80/
DateTime	11 May 2000 16:02:31 +0000
HTTP Status	200
Short title	
URL	https://web.archive.org/web/20000511160231if_/http://www.evil.com:80/
Title	https://web.archive.org/web/20000511160231if_/http://www.evil.com:80/

Entity Data

Archived Page URL	https://web.archive.org/web/20000511160231if_/http://www.evil.com:80/
Web Archive URL	https://web.archive.org/web/20000511160231/http://www.evil.com:80/
Snapshot DateTime	11 May 2000 16:02:31 +0000
Original URL	http://www.evil.com:80/

Incoming (1)

Domain	evil.com

Snapshot

maltego.wayback.Snapshot

2000 Jun 21: http://www.evil.com:80/

Weight	2351645
Timestamp	20000621020527
Description	2000 Jun 21: http://www.evil.com:80/
Web Archive URL	https://web.archive.org/web/20000621020527/http://www.evil.com:80/
Original URL	http://www.evil.com:80/
DateTime	21 Jun 2000 02:05:27 +0000
HTTP Status	200
Short title	
URL	https://web.archive.org/web/20000621020527if_/http://www.evil.com:80/
Title	https://web.archive.org/web/20000621020527if_/http://www.evil.com:80/

Entity Data

Archived Page URL	https://web.archive.org/web/20000621020527if_/http://www.evil.com:80/
Web Archive URL	https://web.archive.org/web/20000621020527/http://www.evil.com:80/
Snapshot DateTime	21 Jun 2000 02:05:27 +0000
Original URL	http://www.evil.com:80/

Incoming (1)

Domain	evil.com

WHOIS Record

maltego.WHOISRecord

www.evil.com

Weight	0
Name	www.evil.com
WHOIS Info	Tech Email: 4477a7cde58c09eas@networksolutionsprivateregistration.com Registrant Postal Code: ecc83fcbe503dd84 Admin Country: US Registrant Organization: 3432650ec337c945 Registrant Name: 8792ba892fc41135 Registrar Registration Expiration Date: 2023-04-11T04:00:00Z Registrant Fax: 3432650ec337c945 Registrar IANA ID: 2 DNSSEC: unsigned Creation Date: 1995-04-10T04:00:00Z Updated Date: 2019-12-17T16:17:59Z | 2019-12-17T16:51:42Z Admin City: Jacksonville Tech Country: US Tech Postal Code: 32256 Registrant Email: 34a8e9bbb60a230cs@networksolutionsprivateregistration.com Admin Postal Code: 32256 Admin State/Province: FL Admin Email: 34a8e9bbb60a230cs@networksolutionsprivateregistration.com Registrar URL: http://networksolutions.com Registrant City: 55985aaef9d91102 Registrar: Network Solutions, LLC Registrant Fax Ext: 3432650ec337c945 Registrant State/Province: 6eb233f5a5adbed8 Registry Domain ID: 1040763_DOMAIN_COM-VRSN Registrant Phone: 40171cfbdb8fe780 Tech City: Jacksonville Registry Expiry Date: 2023-04-11T04:00:00Z Name Server: NS1.VERIO.COM | NS2.VERIO.COM Registrar Abuse Contact Phone: +1.8003337680 Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited | clientTransferProhibited https://icann.org/epp#clientTransferProhibited | clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited Registrant Phone Ext: 3432650ec337c945 Registrar WHOIS Server: whois.networksolutions.com Registrant Street: 8f73e9118a9c558c Registrar Abuse Contact Email: abuse@web.com Registrant Country: US Tech State/Province: FL Domain Name: EVIL.COM
Registry Domain ID	1040763_DOMAIN_COM-VRSN
Domain Name	EVIL.COM
Created Date	1995-04-10T04:00:00Z
Registry Expiry Date	2023-04-11T04:00:00Z
Updated Date	2019-12-17T16:17:59Z | 2019-12-17T16:51:42Z
Transfer Date	
Nameservers	NS1.VERIO.COM | NS2.VERIO.COM
Name Server IP Addresses	
Mantainer	
Created By	
Updated By	
DNSSEC	unsigned
Domain Status	clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited | clientTransferProhibited https://icann.org/epp#clientTransferProhibited | clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
ENS AuthId	
Registry Registrant ID	
Registrant Name	8792ba892fc41135
Registrant Organization	3432650ec337c945
Registrant Address	
Registrant Street	8f73e9118a9c558c
Registrant City	55985aaef9d91102

Registrant State/Province	6eb233f5a5adbed8
Registrant Country	US
Registrant Country Code	
Registrant Postal Code	ecc83fcbe503dd84
Registrant Phone	40171cfbdb8fe780
Registrant Phone Ext	3432650ec337c945
Registrant Fax	3432650ec337c945
Registrant Fax Ext	3432650ec337c945
Registrant Email	34a8e9bbb60a230cs@networksolutionsprivateregistration.com
Admin ID	
Admin ID	
Admin Name	
Admin Organization	
Admin Address	
Admin Street	
Admin City	Jacksonville
Admin State/Province	FL
Admin Country	US
Admin Country Code	
Admin Postal Code	32256
Admin Phone	
Admin Phone Ext	
Admin Fax	
Admin Fax Ext	
Admin Email	34a8e9bbb60a230cs@networksolutionsprivateregistration.com
Tech ID	
Tech Name	
Tech Organization	
Tech Address	
Tech City	Jacksonville
Tech State/Province	FL
Tech Country	US
Tech Postal Code	32256
Tech Phone	
Tech Phone Ext	
Tech Fax	
Tech Fax Ext	
Tech Email	4477a7cde58c09eas@networksolutionsprivateregistration.com
Registrar ID	
Registrar IANA ID	2
Registrar	Network Solutions, LLC
Registrar Registration Expiration Date	2023-04-11T04:00:00Z
Registrar URL	http://networksolutions.com
Registrar WHOIS Server	whois.networksolutions.com
Registrar Status	
Registrar Address	
Registrar City	
Registrar State/Province	
Registrar Country	
Registrar Postal Code	

Registrar Postal Code	
Registrar Phone	
Registrar Fax	
Registrar Fax Ext	
Registrar Email	
Registrar Abuse Contact Email	abuse@web.com
Registrar Abuse Contact Phone	+1.8003337680
Sponsoring Registrar	

Whois Information

Tech Email	4477a7cde58c09eas@networksolutionsprivateregistration.com
Registrant Postal Code	ecc83fcbe503dd84
Admin Country	US
Registrant Organization	3432650ec337c945
Registrant Name	8792ba892fc41135
Registrar Registration Expiration Date	2023-04-11T04:00:00Z
Registrant Fax	3432650ec337c945
Registrar IANA ID	2
DNSSEC	unsigned
Creation Date	1995-04-10T04:00:00Z
Updated Date	2019-12-17T16:17:59Z | 2019-12-17T16:51:42Z
Admin City	Jacksonville
Tech Country	US
Tech Postal Code	32256
Registrant Email	34a8e9bbb60a230cs@networksolutionsprivateregistration.com
Admin Postal Code	32256
Admin State/Province	FL
Admin Email	34a8e9bbb60a230cs@networksolutionsprivateregistration.com
Registrar URL	http://networksolutions.com
Registrant City	55985aaef9d91102
Registrar	Network Solutions, LLC
Registrant Fax Ext	3432650ec337c945
Registrant State/Province	6eb233f5a5adbed8
Registry Domain ID	1040763_DOMAIN_COM-VRSN
Registrant Phone	40171cfbdb8fe780
Tech City	Jacksonville
Registry Expiry Date	2023-04-11T04:00:00Z
Name Server	NS1.VERIO.COM | NS2.VERIO.COM
Registrar Abuse Contact Phone	+1.8003337680

Domain Status	clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited | clientTransferProhibited https://icann.org/epp#clientTransferProhibited | clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
Registrant Phone Ext	3432650ec337c945
Registrar WHOIS Server	whois.networksolutions.com
Registrant Street	8f73e9118a9c558c
Registrar Abuse Contact Email	abuse@web.com
Registrant Country	US
Tech State/Province	FL
Domain Name	EVIL.COM

Incoming (1)

DNS Name	www.evil.com

WHOIS Record

maltego.WHOISRecord

evil.co

Weight	0
Name	evil.co
WHOIS Info	Registrant Postal Code: 3432650ec337c945 DNSSEC: unsigned Registrant Organization: 3432650ec337c945 Registrant Name: 3432650ec337c945 Registry Domain ID: D8A750721BA904C4A90CFDA260DBE314E-NSR Registrar IANA ID: 1387 Creation Date: 2019-10-05T17:00:14Z Updated Date: 2019-10-10T17:01:29Z Registrant Email: f651612a2f356ad3s@ Registrar URL: www.1api.net Registrant City: 3432650ec337c945 Registrar: 1API GmbH Registrant Fax Ext: 3432650ec337c945 Registrant State/Province: b5ccaeb3c805e2cb Registrant Fax: 3432650ec337c945 Registrant Phone: 3432650ec337c945 Registry Expiry Date: 2020-10-05T17:00:14Z Name Server: ns1.uniregistrymarket.link | ns2.uniregistrymarket.link Registrar Abuse Contact Phone: +49.68416984200 Domain Status: ok https://icann.org/epp#ok Registrant Phone Ext: 3432650ec337c945 Registrar WHOIS Server: whois.1api.net Registrant Street: 3432650ec337c945 Registrar Abuse Contact Email: abuse@1api.net Registrant Country: US Domain Name: evil.co
Registry Domain ID	D8A750721BA904C4A90CFDA260DBE314E-NSR
Domain Name	evil.co
Created Date	2019-10-05T17:00:14Z
Registry Expiry Date	2020-10-05T17:00:14Z
Updated Date	2019-10-10T17:01:29Z
Transfer Date	
Nameservers	ns1.uniregistrymarket.link | ns2.uniregistrymarket.link
Name Server IP Addresses	
Mantainer	
Created By	
Updated By	
DNSSEC	unsigned
Domain Status	ok https://icann.org/epp#ok
ENS AuthId	
Registry Registrant ID	
Registrant Name	3432650ec337c945
Registrant Organization	3432650ec337c945
Registrant Address	
Registrant Street	3432650ec337c945
Registrant City	3432650ec337c945
Registrant State/Province	b5ccaeb3c805e2cb
Registrant Country	US
Registrant Country Code	
Registrant Postal Code	3432650ec337c945
Registrant Phone	3432650ec337c945
Registrant Phone Ext	3432650ec337c945
Registrant Fax	3432650ec337c945
Registrant Fax Ext	3432650ec337c945
Registrant Email	f651612a2f356ad3s@
Admin ID	
Admin ID	

Admin Name	
Admin Organization	
Admin Address	
Admin Street	
Admin City	
Admin State/Province	
Admin Country	
Admin Country Code	
Admin Postal Code	
Admin Phone	
Admin Phone Ext	
Admin Fax	
Admin Fax Ext	
Admin Email	
Tech ID	
Tech Name	
Tech Organization	
Tech Address	
Tech City	
Tech State/Province	
Tech Country	
Tech Postal Code	
Tech Phone	
Tech Phone Ext	
Tech Fax	
Tech Fax Ext	
Tech Email	
Registrar ID	
Registrar IANA ID	1387
Registrar	1API GmbH
Registrar Registration Expiration Date	
Registrar URL	www.1api.net
Registrar WHOIS Server	whois.1api.net
Registrar Status	
Registrar Address	
Registrar City	
Registrar State/Province	
Registrar Country	
Registrar Postal Code	
Registrar Phone	
Registrar Fax	
Registrar Fax Ext	
Registrar Email	
Registrar Abuse Contact Email	abuse@1api.net
Registrar Abuse Contact Phone	+49.68416984200
Sponsoring Registrar	

Whois Information	
Registrant Postal Code	3432650ec337c945
DNSSEC	unsigned
Registrant Organization	3432650ec337c945
Registrant Name	3432650ec337c945
Registry Domain ID	D8A750721BA904C4A90CFDA260DBE314E-NSR
Registrar IANA ID	1387
Creation Date	2019-10-05T17:00:14Z
Updated Date	2019-10-10T17:01:29Z
Registrant Email	f651612a2f356ad3s@
Registrar URL	www.1api.net
Registrant City	3432650ec337c945
Registrar	1API GmbH
Registrant Fax Ext	3432650ec337c945
Registrant State/Province	b5ccaeb3c805e2cb
Registrant Fax	3432650ec337c945
Registrant Phone	3432650ec337c945
Registry Expiry Date	2020-10-05T17:00:14Z
Name Server	ns1.uniregistrymarket.link | ns2.uniregistrymarket.link
Registrar Abuse Contact Phone	+49.68416984200
Domain Status	ok https://icann.org/epp#ok
Registrant Phone Ext	3432650ec337c945
Registrar WHOIS Server	whois.1api.net
Registrant Street	3432650ec337c945
Registrar Abuse Contact Email	abuse@1api.net
Registrant Country	US
Domain Name	evil.co

Incoming (1)	
DNS Name	evil.co

WHOIS Record

maltego.WHOISRecord

evil.co

Weight	0
Name	evil.co
WHOIS Info	Registrant Postal Code: 1f8f4166599d23ee DNSSEC: unsigned Registrant Organization: 3432650ec337c945 Registrant Name: 1f8f4166599d23ee Admin Organization: REDACTED FOR PRIVACY Registrar Registration Expiration Date: 2022-10-05T17:00:14Z Registrant Fax: 1f8f4166599d23ee Tech Organization: REDACTED FOR PRIVACY Registrar IANA ID: 146 Admin Country: REDACTED FOR PRIVACY Creation Date: 2019-10-05T17:00:14Z Updated Date: 2021-06-17T12:14:42Z | 2021-06-22T19:14:40Z Admin City: REDACTED FOR PRIVACY Tech Country: REDACTED FOR PRIVACY Registry Admin ID: REDACTED FOR PRIVACY Tech Postal Code: REDACTED FOR PRIVACY Registrant Email: 44f8172ee385b60bs@ | f651612a2f356ad3s@ Admin Postal Code: REDACTED FOR PRIVACY Admin State/Province: REDACTED FOR PRIVACY Registrar URL: http://www.godaddy.com | whois.godaddy.com Registry Tech ID: REDACTED FOR PRIVACY Registry Registrant ID: REDACTED FOR PRIVACY Registrant City: 1f8f4166599d23ee Registrar: GoDaddy.com, LLC Registrant Fax Ext: 1f8f4166599d23ee Registrant State/Province: c5117919ef41a795 Registry Domain ID: D8A750721BA904C4A90CFDA260DBE314E-NSR Registrant Phone: 1f8f4166599d23ee Tech City: REDACTED FOR PRIVACY Registry Expiry Date: 2022-10-05T17:00:14Z Name Server: NS1.UNIREGISTRYMARKET.LINK | NS2.UNIREGISTRYMARKET.LINK | ns1.uniregistrymarket.link | ns2.uniregistrymarket.link Registrar Abuse Contact Phone: +1.4806242505 Domain Status: clientDeleteProhibited http://www.icann.org/epp#clientDeleteProhibited | clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited | clientRenewProhibited http://www.icann.org/epp#clientRenewProhibited | clientRenewProhibited https://icann.org/epp#clientRenewProhibited | clientTransferProhibited http://www.icann.org/epp#clientTransferProhibited | clientTransferProhibited https://icann.org/epp#clientTransferProhibited | clientUpdateProhibited http://www.icann.org/epp#clientUpdateProhibited | clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited Registrant Phone Ext: 1f8f4166599d23ee Registrar WHOIS Server: whois.godaddy.com Registrant Street: 1f8f4166599d23ee Registrar Abuse Contact Email: abuse@godaddy.com Registrant Country: US Tech State/Province: REDACTED FOR PRIVACY Domain Name: evil.co
Registry Domain ID	D8A750721BA904C4A90CFDA260DBE314E-NSR
Domain Name	evil.co
Created Date	2019-10-05T17:00:14Z
Registry Expiry Date	2022-10-05T17:00:14Z
Updated Date	2021-06-17T12:14:42Z | 2021-06-22T19:14:40Z
Transfer Date	
Nameservers	NS1.UNIREGISTRYMARKET.LINK | NS2.UNIREGISTRYMARKET.LINK | ns1.uniregistrymarket.link | ns2.uniregistrymarket.link
Name Server IP Addresses	
Mantainer	
Created By	
Updated By	
DNSSEC	unsigned

Domain Status	clientDeleteProhibited http://www.icann.org/epp#clientDeleteProhibited | clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited | clientRenewProhibited http://www.icann.org/epp#clientRenewProhibited | clientRenewProhibited https://icann.org/epp#clientRenewProhibited | clientTransferProhibited http://www.icann.org/epp#clientTransferProhibited | clientTransferProhibited https://icann.org/epp#clientTransferProhibited | clientUpdateProhibited http://www.icann.org/epp#clientUpdateProhibited | clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
ENS AuthId	
Registry Registrant ID	REDACTED FOR PRIVACY
Registrant Name	1f8f4166599d23ee
Registrant Organization	3432650ec337c945
Registrant Address	
Registrant Street	1f8f4166599d23ee
Registrant City	1f8f4166599d23ee
Registrant State/Province	c5117919ef41a795
Registrant Country	US
Registrant Country Code	
Registrant Postal Code	1f8f4166599d23ee
Registrant Phone	1f8f4166599d23ee
Registrant Phone Ext	1f8f4166599d23ee
Registrant Fax	1f8f4166599d23ee
Registrant Fax Ext	1f8f4166599d23ee
Registrant Email	44f8172ee385b60bs@ | f651612a2f356ad3s@
Admin ID	
Admin ID	REDACTED FOR PRIVACY
Admin Name	
Admin Organization	REDACTED FOR PRIVACY
Admin Address	
Admin Street	
Admin City	REDACTED FOR PRIVACY
Admin State/Province	REDACTED FOR PRIVACY
Admin Country	REDACTED FOR PRIVACY
Admin Country Code	
Admin Postal Code	REDACTED FOR PRIVACY
Admin Phone	
Admin Phone Ext	
Admin Fax	
Admin Fax Ext	
Admin Email	
Tech ID	REDACTED FOR PRIVACY
Tech Name	
Tech Organization	REDACTED FOR PRIVACY
Tech Address	
Tech City	REDACTED FOR PRIVACY
Tech State/Province	REDACTED FOR PRIVACY
Tech Country	REDACTED FOR PRIVACY
Tech Postal Code	REDACTED FOR PRIVACY
Tech Phone	
Tech Phone Ext	
Tech Fax	
Tech Fax Ext	
Tech Email	

Tech Email	
Registrar ID	
Registrar IANA ID	146
Registrar	GoDaddy.com, LLC
Registrar Registration Expiration Date	2022-10-05T17:00:14Z
Registrar URL	http://www.godaddy.com | whois.godaddy.com
Registrar WHOIS Server	whois.godaddy.com
Registrar Status	
Registrar Address	
Registrar City	
Registrar State/Province	
Registrar Country	
Registrar Postal Code	
Registrar Phone	
Registrar Fax	
Registrar Fax Ext	
Registrar Email	
Registrar Abuse Contact Email	abuse@godaddy.com
Registrar Abuse Contact Phone	+1.4806242505
Sponsoring Registrar	

Whois Information

Registrant Postal Code	1f8f4166599d23ee
DNSSEC	unsigned
Registrant Organization	3432650ec337c945
Registrant Name	1f8f4166599d23ee
Admin Organization	REDACTED FOR PRIVACY
Registrar Registration Expiration Date	2022-10-05T17:00:14Z
Registrant Fax	1f8f4166599d23ee
Tech Organization	REDACTED FOR PRIVACY
Registrar IANA ID	146
Admin Country	REDACTED FOR PRIVACY
Creation Date	2019-10-05T17:00:14Z
Updated Date	2021-06-17T12:14:42Z | 2021-06-22T19:14:40Z
Admin City	REDACTED FOR PRIVACY
Tech Country	REDACTED FOR PRIVACY
Registry Admin ID	REDACTED FOR PRIVACY
Tech Postal Code	REDACTED FOR PRIVACY
Registrant Email	44f8172ee385b60bs@ | f651612a2f356ad3s@
Admin Postal Code	REDACTED FOR PRIVACY
Admin State/Province	REDACTED FOR PRIVACY
Registrar URL	http://www.godaddy.com | whois.godaddy.com
Registry Tech ID	REDACTED FOR PRIVACY
Registry Registrant ID	REDACTED FOR PRIVACY
Registrant City	1f8f4166599d23ee
Registrar	GoDaddy.com, LLC
Registrant Fax Ext	1f8f4166599d23ee
Registrant State/Province	c5117919ef41a795
Registry Domain ID	D8A750721BA904C4A90CFDA260DBE314E-NSR
Registrant Phone	1f8f4166599d23ee
Tech City	REDACTED FOR PRIVACY
Registry Expiry Date	2022-10-05T17:00:14Z

Name Server	NS1.UNIREGISTRYMARKET.LINK | NS2.UNIREGISTRYMARKET.LINK | ns1.uniregistrymarket.link | ns2.uniregistrymarket.link
Registrar Abuse Contact Phone	+1.4806242505
Domain Status	clientDeleteProhibited http://www.icann.org/epp#clientDeleteProhibited | clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited | clientRenewProhibited http://www.icann.org/epp#clientRenewProhibited | clientRenewProhibited https://icann.org/epp#clientRenewProhibited | clientTransferProhibited http://www.icann.org/epp#clientTransferProhibited | clientTransferProhibited https://icann.org/epp#clientTransferProhibited | clientUpdateProhibited http://www.icann.org/epp#clientUpdateProhibited | clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
Registrant Phone Ext	1f8f4166599d23ee
Registrar WHOIS Server	whois.godaddy.com
Registrant Street	1f8f4166599d23ee
Registrar Abuse Contact Email	abuse@godaddy.com
Registrant Country	US
Tech State/Province	REDACTED FOR PRIVACY
Domain Name	evil.co

Incoming (1)

	DNS Name	evil.co

WHOIS Record

maltego.WHOISRecord

evil.co

Weight	0
Name	evil.co
WHOIS Info	Registrant Postal Code: 1f8f4166599d23ee DNSSEC: unsigned Registrant Organization: 3432650ec337c945 Registrant Name: 1f8f4166599d23ee Admin Organization: REDACTED FOR PRIVACY Registrant Fax: 1f8f4166599d23ee Tech Organization: REDACTED FOR PRIVACY Registrar IANA ID: 146 Admin Country: REDACTED FOR PRIVACY Creation Date: 2019-10-05T17:00:14Z Updated Date: 2020-09-27T15:06:02Z Admin City: REDACTED FOR PRIVACY Tech Country: REDACTED FOR PRIVACY Registry Admin ID: REDACTED FOR PRIVACY Tech Postal Code: REDACTED FOR PRIVACY Registrant Email: f651612a2f356ad3s@ Admin Postal Code: REDACTED FOR PRIVACY Admin State/Province: REDACTED FOR PRIVACY Registrar URL: whois.godaddy.com Registry Tech ID: REDACTED FOR PRIVACY Registry Registrant ID: REDACTED FOR PRIVACY Registrant City: 1f8f4166599d23ee Registrar: GoDaddy.com, LLC Registrant Fax Ext: 1f8f4166599d23ee Registrant State/Province: c5117919ef41a795 Registry Domain ID: D8A750721BA904C4A90CFDA260DBE314E-NSR Registrant Phone: 1f8f4166599d23ee Tech City: REDACTED FOR PRIVACY Registry Expiry Date: 2021-10-05T17:00:14Z Name Server: ns1.uniregistrymarket.link | ns2.uniregistrymarket.link Registrar Abuse Contact Phone: +1.4806242505 Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited | clientRenewProhibited https://icann.org/epp#clientRenewProhibited | clientTransferProhibited https://icann.org/epp#clientTransferProhibited | clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited Registrant Phone Ext: 1f8f4166599d23ee Registrar WHOIS Server: whois.godaddy.com Registrant Street: 1f8f4166599d23ee Registrar Abuse Contact Email: abuse@godaddy.com Registrant Country: US Tech State/Province: REDACTED FOR PRIVACY Domain Name: evil.co
Registry Domain ID	D8A750721BA904C4A90CFDA260DBE314E-NSR
Domain Name	evil.co
Created Date	2019-10-05T17:00:14Z
Registry Expiry Date	2021-10-05T17:00:14Z
Updated Date	2020-09-27T15:06:02Z
Transfer Date	
Nameservers	ns1.uniregistrymarket.link | ns2.uniregistrymarket.link
Name Server IP Addresses	
Mantainer	
Created By	
Updated By	
DNSSEC	unsigned
Domain Status	clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited | clientRenewProhibited https://icann.org/epp#clientRenewProhibited | clientTransferProhibited https://icann.org/epp#clientTransferProhibited | clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
ENS AuthId	
Registry Registrant ID	REDACTED FOR PRIVACY
Registrant Name	1f8f4166599d23ee
Registrant Organization	3432650ec337c945
Registrant Address	

Registrant Street	1f8f4166599d23ee
Registrant City	1f8f4166599d23ee
Registrant State/Province	c5117919ef41a795
Registrant Country	US
Registrant Country Code	
Registrant Postal Code	1f8f4166599d23ee
Registrant Phone	1f8f4166599d23ee
Registrant Phone Ext	1f8f4166599d23ee
Registrant Fax	1f8f4166599d23ee
Registrant Fax Ext	1f8f4166599d23ee
Registrant Email	f651612a2f356ad3s@
Admin ID	
Admin ID	REDACTED FOR PRIVACY
Admin Name	
Admin Organization	REDACTED FOR PRIVACY
Admin Address	
Admin Street	
Admin City	REDACTED FOR PRIVACY
Admin State/Province	REDACTED FOR PRIVACY
Admin Country	REDACTED FOR PRIVACY
Admin Country Code	
Admin Postal Code	REDACTED FOR PRIVACY
Admin Phone	
Admin Phone Ext	
Admin Fax	
Admin Fax Ext	
Admin Email	
Tech ID	REDACTED FOR PRIVACY
Tech Name	
Tech Organization	REDACTED FOR PRIVACY
Tech Address	
Tech City	REDACTED FOR PRIVACY
Tech State/Province	REDACTED FOR PRIVACY
Tech Country	REDACTED FOR PRIVACY
Tech Postal Code	REDACTED FOR PRIVACY
Tech Phone	
Tech Phone Ext	
Tech Fax	
Tech Fax Ext	
Tech Email	
Registrar ID	
Registrar IANA ID	146
Registrar	GoDaddy.com, LLC
Registrar Registration Expiration Date	
Registrar URL	whois.godaddy.com
Registrar WHOIS Server	whois.godaddy.com
Registrar Status	
Registrar Address	
Registrar City	
Registrar State/Province	

Registrar State/Province	
Registrar Country	
Registrar Postal Code	
Registrar Phone	
Registrar Fax	
Registrar Fax Ext	
Registrar Email	
Registrar Abuse Contact Email	abuse@godaddy.com
Registrar Abuse Contact Phone	+1.4806242505
Sponsoring Registrar	

Whois Information

Registrant Postal Code	1f8f4166599d23ee
DNSSEC	unsigned
Registrant Organization	3432650ec337c945
Registrant Name	1f8f4166599d23ee
Admin Organization	REDACTED FOR PRIVACY
Registrant Fax	1f8f4166599d23ee
Tech Organization	REDACTED FOR PRIVACY
Registrar IANA ID	146
Admin Country	REDACTED FOR PRIVACY
Creation Date	2019-10-05T17:00:14Z
Updated Date	2020-09-27T15:06:02Z
Admin City	REDACTED FOR PRIVACY
Tech Country	REDACTED FOR PRIVACY
Registry Admin ID	REDACTED FOR PRIVACY
Tech Postal Code	REDACTED FOR PRIVACY
Registrant Email	f651612a2f356ad3s@
Admin Postal Code	REDACTED FOR PRIVACY
Admin State/Province	REDACTED FOR PRIVACY
Registrar URL	whois.godaddy.com
Registry Tech ID	REDACTED FOR PRIVACY
Registry Registrant ID	REDACTED FOR PRIVACY
Registrant City	1f8f4166599d23ee
Registrar	GoDaddy.com, LLC
Registrant Fax Ext	1f8f4166599d23ee
Registrant State/Province	c5117919ef41a795
Registry Domain ID	D8A750721BA904C4A90CFDA260DBE314E-NSR
Registrant Phone	1f8f4166599d23ee
Tech City	REDACTED FOR PRIVACY
Registry Expiry Date	2021-10-05T17:00:14Z
Name Server	ns1.uniregistrymarket.link | ns2.uniregistrymarket.link

Name Server	ns1.uniregistrymarket.link | ns2.uniregistrymarket.link
Registrar Abuse Contact Phone	+1.4806242505
Domain Status	clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited | clientRenewProhibited https://icann.org/epp#clientRenewProhibited | clientTransferProhibited https://icann.org/epp#clientTransferProhibited | clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
Registrant Phone Ext	1f8f4166599d23ee
Registrar WHOIS Server	whois.godaddy.com
Registrant Street	1f8f4166599d23ee
Registrar Abuse Contact Email	abuse@godaddy.com
Registrant Country	US
Tech State/Province	REDACTED FOR PRIVACY
Domain Name	evil.co

Incoming (1)

	DNS Name	evil.co

WHOIS Record

maltego.WHOISRecord

apitwitter.com.w3snoop.com

Weight	0
Name	apitwitter.com.w3snoop.com
WHOIS Info	Tech Email: c9b5a1cf1d0c3764s@domainsbyproxy.com Registrant Postal Code: b9448b1c75ff534d Admin Country: US Registrant Organization: b46a98a26fe2fd9f Registrant Name: 80315b2e6ac1a801 Admin Organization: Domains By Proxy, LLC Registrar Registration Expiration Date: 2023-06-06T02:04:22Z Registrant Fax: 9fad764be0c7e95d Tech Organization: Domains By Proxy, LLC Registrar IANA ID: 146 DNSSEC: unsigned Creation Date: 2011-06-06T02:04:22Z Updated Date: 2020-02-10T04:49:39Z | 2020-02-10T04:49:41Z Admin City: Scottsdale Tech Country: US Registry Admin ID: Not Available From Registry Tech Postal Code: 85260 Registrant Email: c9b5a1cf1d0c3764s@domainsbyproxy.com Admin Postal Code: 85260 Admin State/Province: Arizona Admin Email: c9b5a1cf1d0c3764s@domainsbyproxy.com Registrar URL: http://www.godaddy.com Registry Tech ID: Not Available From Registry Registry Registrant ID: Not Available From Registry Registrant City: 373f4980ad3d2d01 Registrar: GoDaddy.com, LLC Registrant Fax Ext: 3432650ec337c945 Registrant State/Province: 30bdd2917a604c83 Registry Domain ID: 1660071767_DOMAIN_COM-VRSN Registrant Phone: d5f66d3a005b000d Tech City: Scottsdale Registry Expiry Date: 2023-06-06T02:04:22Z Name Server: INDRI.EZOICNS.COM | SAOLA.EZOICNS.COM Registrar Abuse Contact Phone: +1.4806242505 | 480-624-2505 Domain Status: clientDeleteProhibited http://www.icann.org/epp#clientDeleteProhibited | clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited | clientRenewProhibited http://www.icann.org/epp#clientRenewProhibited | clientRenewProhibited https://icann.org/epp#clientRenewProhibited | clientTransferProhibited http://www.icann.org/epp#clientTransferProhibited | clientTransferProhibited https://icann.org/epp#clientTransferProhibited | clientUpdateProhibited http://www.icann.org/epp#clientUpdateProhibited | clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited Registrant Phone Ext: 3432650ec337c945 Registrar WHOIS Server: whois.godaddy.com Registrant Street: 037792fd5a6fe619 | f38c0adea706dbc3 Registrar Abuse Contact Email: abuse@godaddy.com Registrant Country: US Tech State/Province: Arizona Domain Name: W3SNOOP.COM
Registry Domain ID	1660071767_DOMAIN_COM-VRSN
Domain Name	W3SNOOP.COM
Created Date	2011-06-06T02:04:22Z
Registry Expiry Date	2023-06-06T02:04:22Z
Updated Date	2020-02-10T04:49:39Z | 2020-02-10T04:49:41Z
Transfer Date	
Nameservers	INDRI.EZOICNS.COM | SAOLA.EZOICNS.COM
Name Server IP Addresses	
Mantainer	
Created By	
Updated By	
DNSSEC	unsigned

Domain Status	clientDeleteProhibited http://www.icann.org/epp#clientDeleteProhibited | clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited | clientRenewProhibited http://www.icann.org/epp#clientRenewProhibited | clientRenewProhibited https://icann.org/epp#clientRenewProhibited | clientTransferProhibited http://www.icann.org/epp#clientTransferProhibited | clientTransferProhibited https://icann.org/epp#clientTransferProhibited | clientUpdateProhibited http://www.icann.org/epp#clientUpdateProhibited | clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
ENS AuthId	
Registry Registrant ID	Not Available From Registry
Registrant Name	80315b2e6ac1a801
Registrant Organization	b46a98a26fe2fd9f
Registrant Address	
Registrant Street	037792fd5a6fe619 | f38c0adea706dbc3
Registrant City	373f4980ad3d2d01
Registrant State/Province	30bdd2917a604c83
Registrant Country	US
Registrant Country Code	
Registrant Postal Code	b9448b1c75ff534d
Registrant Phone	d5f66d3a005b000d
Registrant Phone Ext	3432650ec337c945
Registrant Fax	9fad764be0c7e95d
Registrant Fax Ext	3432650ec337c945
Registrant Email	c9b5a1cf1d0c3764s@domainsbyproxy.com
Admin ID	
Admin ID	Not Available From Registry
Admin Name	
Admin Organization	Domains By Proxy, LLC
Admin Address	
Admin Street	
Admin City	Scottsdale
Admin State/Province	Arizona
Admin Country	US
Admin Country Code	
Admin Postal Code	85260
Admin Phone	
Admin Phone Ext	
Admin Fax	
Admin Fax Ext	
Admin Email	c9b5a1cf1d0c3764s@domainsbyproxy.com
Tech ID	Not Available From Registry
Tech Name	
Tech Organization	Domains By Proxy, LLC
Tech Address	
Tech City	Scottsdale
Tech State/Province	Arizona
Tech Country	US
Tech Postal Code	85260
Tech Phone	
Tech Phone Ext	
Tech Fax	
Tech Fax Ext	
Tech Email	c9b5a1cf1d0c3764s@domainsbyproxy.com

Tech Email	c9b5a1cf1d0c3764s@domainsbyproxy.com
Registrar ID	
Registrar IANA ID	146
Registrar	GoDaddy.com, LLC
Registrar Registration Expiration Date	2023-06-06T02:04:22Z
Registrar URL	http://www.godaddy.com
Registrar WHOIS Server	whois.godaddy.com
Registrar Status	
Registrar Address	
Registrar City	
Registrar State/Province	
Registrar Country	
Registrar Postal Code	
Registrar Phone	
Registrar Fax	
Registrar Fax Ext	
Registrar Email	
Registrar Abuse Contact Email	abuse@godaddy.com
Registrar Abuse Contact Phone	+1.4806242505 | 480-624-2505
Sponsoring Registrar	

Whois Information

Tech Email	c9b5a1cf1d0c3764s@domainsbyproxy.com
Registrant Postal Code	b9448b1c75ff534d
Admin Country	US
Registrant Organization	b46a98a26fe2fd9f
Registrant Name	80315b2e6ac1a801
Admin Organization	Domains By Proxy, LLC
Registrar Registration Expiration Date	2023-06-06T02:04:22Z
Registrant Fax	9fad764be0c7e95d
Tech Organization	Domains By Proxy, LLC
Registrar IANA ID	146
DNSSEC	unsigned
Creation Date	2011-06-06T02:04:22Z
Updated Date	2020-02-10T04:49:39Z | 2020-02-10T04:49:41Z
Admin City	Scottsdale
Tech Country	US
Registry Admin ID	Not Available From Registry
Tech Postal Code	85260
Registrant Email	c9b5a1cf1d0c3764s@domainsbyproxy.com
Admin Postal Code	85260
Admin State/Province	Arizona
Admin Email	c9b5a1cf1d0c3764s@domainsbyproxy.com
Registrar URL	http://www.godaddy.com
Registry Tech ID	Not Available From Registry
Registry Registrant ID	Not Available From Registry
Registrant City	373f4980ad3d2d01
Registrar	GoDaddy.com, LLC
Registrant Fax Ext	3432650ec337c945
Registrant State/Province	30bdd2917a604c83
Registry Domain ID	1660071767_DOMAIN_COM-VRSN
Registrant Phone	d5f66d3a005b000d
Tech City	Scottsdale

Registry Expiry Date	2023-06-06T02:04:22Z
Name Server	INDRI.EZOICNS.COM | SAOLA.EZOICNS.COM
Registrar Abuse Contact Phone	+1.4806242505 | 480-624-2505
Domain Status	clientDeleteProhibited http://www.icann.org/epp#clientDeleteProhibited | clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited | clientRenewProhibited http://www.icann.org/epp#clientRenewProhibited | clientRenewProhibited https://icann.org/epp#clientRenewProhibited | clientTransferProhibited http://www.icann.org/epp#clientTransferProhibited | clientTransferProhibited https://icann.org/epp#clientTransferProhibited | clientUpdateProhibited http://www.icann.org/epp#clientUpdateProhibited | clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
Registrant Phone Ext	3432650ec337c945
Registrar WHOIS Server	whois.godaddy.com
Registrant Street	037792fd5a6fe619 | f38c0adea706dbc3
Registrar Abuse Contact Email	abuse@godaddy.com
Registrant Country	US
Tech State/Province	Arizona
Domain Name	W3SNOOP.COM

Incoming (1)

DNS Name	apitwitter.com.w3snoop.com

IPv4 Address

maltego.IPv4Address

91.195.240.126

Weight	0
IP Address	91.195.240.126
Internal	false
Date Resolved	2019-04-21T13:31:12Z
Resolver	VirusTotal

Incoming (1)

DNS Name	evil.co

IPv4 Address

maltego.IPv4Address

72.52.4.119

Weight	0
IP Address	72.52.4.119
Internal	false
Date Resolved	2016-06-17T00:00Z
Resolver	VirusTotal

Incoming (1)

DNS Name	evil.co

WHOIS Record

maltego.WHOISRecord

w3snoop.com

Weight	0
Name	w3snoop.com
WHOIS Info	Tech Email: c9b5a1cf1d0c3764s@domainsbyproxy.com Registrant Postal Code: b9448b1c75ff534d Admin Country: US Registrant Organization: b46a98a26fe2fd9f Registrant Name: 80315b2e6ac1a801 Admin Organization: Domains By Proxy, LLC Registrar Registration Expiration Date: 2021-06-06T02:04:22Z Registry Domain ID: 1660071767_DOMAIN_COM-VRSN Tech Organization: Domains By Proxy, LLC Registrar IANA ID: 146 DNSSEC: unsigned Creation Date: 2011-06-06T02:04:22Z Updated Date: 2018-12-11T01:55:27Z | 2018-12-11T01:55:29Z Admin City: Scottsdale Tech Country: US Registry Admin ID: Not Available From Registry Tech Postal Code: 85260 Registrant Email: c9b5a1cf1d0c3764s@domainsbyproxy.com Admin Postal Code: 85260 Admin State/Province: Arizona Admin Email: c9b5a1cf1d0c3764s@domainsbyproxy.com Registrar URL: http://www.godaddy.com Registry Tech ID: Not Available From Registry Registry Registrant ID: Not Available From Registry Registrant City: 373f4980ad3d2d01 Registrar: GoDaddy.com, LLC Registrant Fax Ext: 3432650ec337c945 Registrant State/Province: 30bdd2917a604c83 Registrant Fax: 9fad764be0c7e95d Registrant Phone: d5f66d3a005b000d Tech City: Scottsdale Registry Expiry Date: 2021-06-06T02:04:22Z Name Server: INDRI.EZOICNS.COM | SAOLA.EZOICNS.COM Registrar Abuse Contact Phone: +1.4806242505 | 480-624-2505 Domain Status: clientDeleteProhibited http://www.icann.org/epp#clientDeleteProhibited | clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited | clientRenewProhibited http://www.icann.org/epp#clientRenewProhibited | clientRenewProhibited https://icann.org/epp#clientRenewProhibited | clientTransferProhibited http://www.icann.org/epp#clientTransferProhibited | clientTransferProhibited https://icann.org/epp#clientTransferProhibited | clientUpdateProhibited http://www.icann.org/epp#clientUpdateProhibited | clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited Registrant Phone Ext: 3432650ec337c945 Registrar WHOIS Server: whois.godaddy.com Registrant Street: 037792fd5a6fe619 | f38c0adea706dbc3 Registrar Abuse Contact Email: abuse@godaddy.com Registrant Country: US Tech State/Province: Arizona Domain Name: W3SNOOP.COM
Registry Domain ID	1660071767_DOMAIN_COM-VRSN
Domain Name	W3SNOOP.COM
Created Date	2011-06-06T02:04:22Z
Registry Expiry Date	2021-06-06T02:04:22Z
Updated Date	2018-12-11T01:55:27Z | 2018-12-11T01:55:29Z
Transfer Date	
Nameservers	INDRI.EZOICNS.COM | SAOLA.EZOICNS.COM
Name Server IP Addresses	
Mantainer	
Created By	
Updated By	
DNSSEC	unsigned

Domain Status	clientDeleteProhibited http://www.icann.org/epp#clientDeleteProhibited | clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited | clientRenewProhibited http://www.icann.org/epp#clientRenewProhibited | clientRenewProhibited https://icann.org/epp#clientRenewProhibited | clientTransferProhibited http://www.icann.org/epp#clientTransferProhibited | clientTransferProhibited https://icann.org/epp#clientTransferProhibited | clientUpdateProhibited http://www.icann.org/epp#clientUpdateProhibited | clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
ENS AuthId	
Registry Registrant ID	Not Available From Registry
Registrant Name	80315b2e6ac1a801
Registrant Organization	b46a98a26fe2fd9f
Registrant Address	
Registrant Street	037792fd5a6fe619 | f38c0adea706dbc3
Registrant City	373f4980ad3d2d01
Registrant State/Province	30bdd2917a604c83
Registrant Country	US
Registrant Country Code	
Registrant Postal Code	b9448b1c75ff534d
Registrant Phone	d5f66d3a005b000d
Registrant Phone Ext	3432650ec337c945
Registrant Fax	9fad764be0c7e95d
Registrant Fax Ext	3432650ec337c945
Registrant Email	c9b5a1cf1d0c3764s@domainsbyproxy.com
Admin ID	
Admin ID	Not Available From Registry
Admin Name	
Admin Organization	Domains By Proxy, LLC
Admin Address	
Admin Street	
Admin City	Scottsdale
Admin State/Province	Arizona
Admin Country	US
Admin Country Code	
Admin Postal Code	85260
Admin Phone	
Admin Phone Ext	
Admin Fax	
Admin Fax Ext	
Admin Email	c9b5a1cf1d0c3764s@domainsbyproxy.com
Tech ID	Not Available From Registry
Tech Name	
Tech Organization	Domains By Proxy, LLC
Tech Address	
Tech City	Scottsdale
Tech State/Province	Arizona
Tech Country	US
Tech Postal Code	85260
Tech Phone	
Tech Phone Ext	
Tech Fax	
Tech Fax Ext	
Tech Email	c9b5a1cf1d0c3764s@domainsbyproxy.com

Tech Email	c9b5a1cf1d0c3764s@domainsbyproxy.com
Registrar ID	
Registrar IANA ID	146
Registrar	GoDaddy.com, LLC
Registrar Registration Expiration Date	2021-06-06T02:04:22Z
Registrar URL	http://www.godaddy.com
Registrar WHOIS Server	whois.godaddy.com
Registrar Status	
Registrar Address	
Registrar City	
Registrar State/Province	
Registrar Country	
Registrar Postal Code	
Registrar Phone	
Registrar Fax	
Registrar Fax Ext	
Registrar Email	
Registrar Abuse Contact Email	abuse@godaddy.com
Registrar Abuse Contact Phone	+1.4806242505 | 480-624-2505
Sponsoring Registrar	

Whois Information

Tech Email	c9b5a1cf1d0c3764s@domainsbyproxy.com
Registrant Postal Code	b9448b1c75ff534d
Admin Country	US
Registrant Organization	b46a98a26fe2fd9f
Registrant Name	80315b2e6ac1a801
Admin Organization	Domains By Proxy, LLC
Registrar Registration Expiration Date	2021-06-06T02:04:22Z
Registry Domain ID	1660071767_DOMAIN_COM-VRSN
Tech Organization	Domains By Proxy, LLC
Registrar IANA ID	146
DNSSEC	unsigned
Creation Date	2011-06-06T02:04:22Z
Updated Date	2018-12-11T01:55:27Z | 2018-12-11T01:55:29Z
Admin City	Scottsdale
Tech Country	US
Registry Admin ID	Not Available From Registry
Tech Postal Code	85260
Registrant Email	c9b5a1cf1d0c3764s@domainsbyproxy.com
Admin Postal Code	85260
Admin State/Province	Arizona
Admin Email	c9b5a1cf1d0c3764s@domainsbyproxy.com
Registrar URL	http://www.godaddy.com
Registry Tech ID	Not Available From Registry
Registry Registrant ID	Not Available From Registry
Registrant City	373f4980ad3d2d01
Registrar	GoDaddy.com, LLC
Registrant Fax Ext	3432650ec337c945
Registrant State/Province	30bdd2917a604c83
Registrant Fax	9fad764be0c7e95d
Registrant Phone	d5f66d3a005b000d
Tech City	Scottsdale

Registry Expiry Date	2021-06-06T02:04:22Z
Name Server	INDRI.EZOICNS.COM | SAOLA.EZOICNS.COM
Registrar Abuse Contact Phone	+1.4806242505 | 480-624-2505
Domain Status	clientDeleteProhibited http://www.icann.org/epp#clientDeleteProhibited | clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited | clientRenewProhibited http://www.icann.org/epp#clientRenewProhibited | clientRenewProhibited https://icann.org/epp#clientRenewProhibited | clientTransferProhibited http://www.icann.org/epp#clientTransferProhibited | clientTransferProhibited https://icann.org/epp#clientTransferProhibited | clientUpdateProhibited http://www.icann.org/epp#clientUpdateProhibited | clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
Registrant Phone Ext	3432650ec337c945
Registrar WHOIS Server	whois.godaddy.com
Registrant Street	037792fd5a6fe619 | f38c0adea706dbc3
Registrar Abuse Contact Email	abuse@godaddy.com
Registrant Country	US
Tech State/Province	Arizona
Domain Name	W3SNOOP.COM

Whois Information

Tech Email	c9b5a1cf1d0c3764s@domainsbyproxy.com
Registrant Postal Code	b9448b1c75ff534d
Admin Country	US
Registrant Organization	b46a98a26fe2fd9f
Registrant Name	80315b2e6ac1a801
Admin Organization	Domains By Proxy, LLC
Registrar Registration Expiration Date	2021-06-06T02:04:22Z
Registrant Fax	9fad764be0c7e95d
Tech Organization	Domains By Proxy, LLC
Registrar IANA ID	146
DNSSEC	unsigned
Creation Date	2011-06-06T02:04:22Z
Updated Date	2018-12-11T01:55:27Z | 2018-12-11T01:55:29Z
Admin City	Scottsdale
Tech Country	US
Registry Admin ID	Not Available From Registry
Tech Postal Code	85260
Registrant Email	c9b5a1cf1d0c3764s@domainsbyproxy.com
Admin Postal Code	85260
Admin State/Province	Arizona
Admin Email	c9b5a1cf1d0c3764s@domainsbyproxy.com
Registrar URL	http://www.godaddy.com
Registry Tech ID	Not Available From Registry
Registry Registrant ID	Not Available From Registry
Registrant City	373f4980ad3d2d01
Registrar	GoDaddy.com, LLC
Registrant Fax Ext	3432650ec337c945
Registrant State/Province	30bdd2917a604c83
Registry Domain ID	1660071767_DOMAIN_COM-VRSN
Registrant Phone	d5f66d3a005b000d
Tech City	Scottsdale

Registry Expiry Date	2021-06-06T02:04:22Z
Name Server	INDRI.EZOICNS.COM | SAOLA.EZOICNS.COM
Registrar Abuse Contact Phone	+1.4806242505 | 480-624-2505
Domain Status	clientDeleteProhibited http://www.icann.org/epp#clientDeleteProhibited | clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited | clientRenewProhibited http://www.icann.org/epp#clientRenewProhibited | clientRenewProhibited https://icann.org/epp#clientRenewProhibited | clientTransferProhibited http://www.icann.org/epp#clientTransferProhibited | clientTransferProhibited https://icann.org/epp#clientTransferProhibited | clientUpdateProhibited http://www.icann.org/epp#clientUpdateProhibited | clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
Registrant Phone Ext	3432650ec337c945
Registrar WHOIS Server	whois.godaddy.com
Registrant Street	037792fd5a6fe619 | f38c0adea706dbc3
Registrar Abuse Contact Email	abuse@godaddy.com
Registrant Country	US
Tech State/Province	Arizona
Domain Name	W3SNOOP.COM

Incoming (1)

	DNS Name	w3snoop.com

WHOIS Record

maltego.WHOISRecord

w3snoop.com

Weight	0
Name	w3snoop.com
WHOIS Info	Name Server: INDRI.EZOICNS.COM | SAOLA.EZOICNS.COM Registrar IANA ID: 146 Registrar Abuse Contact Phone: 480-624-2505 DNSSEC: unsigned Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited | clientRenewProhibited https://icann.org/epp#clientRenewProhibited | clientTransferProhibited https://icann.org/epp#clientTransferProhibited | clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited Creation Date: 2011-06-06T02:04:22Z Registrar URL: http://www.godaddy.com Registrar WHOIS Server: whois.godaddy.com Updated Date: 2020-02-10T04:49:41Z Registrar: GoDaddy.com, LLC Domain Name: W3SNOOP.COM Registrar Abuse Contact Email: abuse@godaddy.com Registry Domain ID: 1660071767_DOMAIN_COM-VRSN Registry Expiry Date: 2023-06-06T02:04:22Z
Registry Domain ID	1660071767_DOMAIN_COM-VRSN
Domain Name	W3SNOOP.COM
Created Date	2011-06-06T02:04:22Z
Registry Expiry Date	2023-06-06T02:04:22Z
Updated Date	2020-02-10T04:49:41Z
Transfer Date	
Nameservers	INDRI.EZOICNS.COM | SAOLA.EZOICNS.COM
Name Server IP Addresses	
Mantainer	
Created By	
Updated By	
DNSSEC	unsigned
Domain Status	clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited | clientRenewProhibited https://icann.org/epp#clientRenewProhibited | clientTransferProhibited https://icann.org/epp#clientTransferProhibited | clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
ENS AuthId	
Registry Registrant ID	
Registrant Name	
Registrant Organization	
Registrant Address	
Registrant Street	
Registrant City	
Registrant State/Province	
Registrant Country	
Registrant Country Code	
Registrant Postal Code	
Registrant Phone	
Registrant Phone Ext	
Registrant Fax	
Registrant Fax Ext	
Registrant Email	
Admin ID	
Admin ID	
Admin Name	
Admin Organization	
Admin Address	

Admin Street	
Admin City	
Admin State/Province	
Admin Country	
Admin Country Code	
Admin Postal Code	
Admin Phone	
Admin Phone Ext	
Admin Fax	
Admin Fax Ext	
Admin Email	
Tech ID	
Tech Name	
Tech Organization	
Tech Address	
Tech City	
Tech State/Province	
Tech Country	
Tech Postal Code	
Tech Phone	
Tech Phone Ext	
Tech Fax	
Tech Fax Ext	
Tech Email	
Registrar ID	
Registrar IANA ID	146
Registrar	GoDaddy.com, LLC
Registrar Registration Expiration Date	
Registrar URL	http://www.godaddy.com
Registrar WHOIS Server	whois.godaddy.com
Registrar Status	
Registrar Address	
Registrar City	
Registrar State/Province	
Registrar Country	
Registrar Postal Code	
Registrar Phone	
Registrar Fax	
Registrar Fax Ext	
Registrar Email	
Registrar Abuse Contact Email	abuse@godaddy.com
Registrar Abuse Contact Phone	480-624-2505
Sponsoring Registrar	

Whois Information	
Name Server	INDRI.EZOICNS.COM | SAOLA.EZOICNS.COM
Registrar IANA ID	146
Registrar Abuse Contact Phone	480-624-2505
DNSSEC	unsigned
Domain Status	clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited | clientRenewProhibited https://icann.org/epp#clientRenewProhibited | clientTransferProhibited https://icann.org/epp#clientTransferProhibited | clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
Creation Date	2011-06-06T02:04:22Z
Registrar URL	http://www.godaddy.com
Registrar WHOIS Server	whois.godaddy.com
Updated Date	2020-02-10T04:49:41Z
Registrar	GoDaddy.com, LLC
Domain Name	W3SNOOP.COM
Registrar Abuse Contact Email	abuse@godaddy.com
Registry Domain ID	1660071767_DOMAIN_COM-VRSN
Registry Expiry Date	2023-06-06T02:04:22Z

Incoming (1)		
	DNS Name	w3snoop.com

WHOIS Record

maltego.WHOISRecord

w3snoop.com

Weight	0
Name	w3snoop.com
WHOIS Info	Tech Email: c9b5a1cf1d0c3764s@domainsbyproxy.com Registrant Postal Code: b9448b1c75ff534d Admin Country: US Registrant Organization: b46a98a26fe2fd9f Registrant Name: 80315b2e6ac1a801 Admin Organization: Domains By Proxy, LLC Registrar Registration Expiration Date: 2023-06-06T02:04:22Z Registrant Fax: 9fad764be0c7e95d Tech Organization: Domains By Proxy, LLC Registrar IANA ID: 146 DNSSEC: unsigned Creation Date: 2011-06-06T02:04:22Z Updated Date: 2020-02-10T04:49:39Z | 2020-02-10T04:49:41Z Admin City: Scottsdale Tech Country: US Registry Admin ID: Not Available From Registry Tech Postal Code: 85260 Registrant Email: c9b5a1cf1d0c3764s@domainsbyproxy.com Admin Postal Code: 85260 Admin State/Province: Arizona Admin Email: c9b5a1cf1d0c3764s@domainsbyproxy.com Registrar URL: http://www.godaddy.com Registry Tech ID: Not Available From Registry Registry Registrant ID: Not Available From Registry Registrant City: 373f4980ad3d2d01 Registrar: GoDaddy.com, LLC Registrant Fax Ext: 3432650ec337c945 Registrant State/Province: 30bdd2917a604c83 Registry Domain ID: 1660071767_DOMAIN_COM-VRSN Registrant Phone: d5f66d3a005b000d Tech City: Scottsdale Registry Expiry Date: 2023-06-06T02:04:22Z Name Server: INDRI.EZOICNS.COM | SAOLA.EZOICNS.COM Registrar Abuse Contact Phone: +1.4806242505 | 480-624-2505 Domain Status: clientDeleteProhibited http://www.icann.org/epp#clientDeleteProhibited | clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited | clientRenewProhibited http://www.icann.org/epp#clientRenewProhibited | clientRenewProhibited https://icann.org/epp#clientRenewProhibited | clientTransferProhibited http://www.icann.org/epp#clientTransferProhibited | clientTransferProhibited https://icann.org/epp#clientTransferProhibited | clientUpdateProhibited http://www.icann.org/epp#clientUpdateProhibited | clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited Registrant Phone Ext: 3432650ec337c945 Registrar WHOIS Server: whois.godaddy.com Registrant Street: 037792fd5a6fe619 | f38c0adea706dbc3 Registrar Abuse Contact Email: abuse@godaddy.com Registrant Country: US Tech State/Province: Arizona Domain Name: W3SNOOP.COM
Registry Domain ID	1660071767_DOMAIN_COM-VRSN
Domain Name	W3SNOOP.COM
Created Date	2011-06-06T02:04:22Z
Registry Expiry Date	2023-06-06T02:04:22Z
Updated Date	2020-02-10T04:49:39Z | 2020-02-10T04:49:41Z
Transfer Date	
Nameservers	INDRI.EZOICNS.COM | SAOLA.EZOICNS.COM
Name Server IP Addresses	
Mantainer	
Created By	
Updated By	
DNSSEC	unsigned

Domain Status	clientDeleteProhibited http://www.icann.org/epp#clientDeleteProhibited | clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited | clientRenewProhibited http://www.icann.org/epp#clientRenewProhibited | clientRenewProhibited https://icann.org/epp#clientRenewProhibited | clientTransferProhibited http://www.icann.org/epp#clientTransferProhibited | clientTransferProhibited https://icann.org/epp#clientTransferProhibited | clientUpdateProhibited http://www.icann.org/epp#clientUpdateProhibited | clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
ENS AuthId	
Registry Registrant ID	Not Available From Registry
Registrant Name	80315b2e6ac1a801
Registrant Organization	b46a98a26fe2fd9f
Registrant Address	
Registrant Street	037792fd5a6fe619 | f38c0adea706dbc3
Registrant City	373f4980ad3d2d01
Registrant State/Province	30bdd2917a604c83
Registrant Country	US
Registrant Country Code	
Registrant Postal Code	b9448b1c75ff534d
Registrant Phone	d5f66d3a005b000d
Registrant Phone Ext	3432650ec337c945
Registrant Fax	9fad764be0c7e95d
Registrant Fax Ext	3432650ec337c945
Registrant Email	c9b5a1cf1d0c3764s@domainsbyproxy.com
Admin ID	
Admin ID	Not Available From Registry
Admin Name	
Admin Organization	Domains By Proxy, LLC
Admin Address	
Admin Street	
Admin City	Scottsdale
Admin State/Province	Arizona
Admin Country	US
Admin Country Code	
Admin Postal Code	85260
Admin Phone	
Admin Phone Ext	
Admin Fax	
Admin Fax Ext	
Admin Email	c9b5a1cf1d0c3764s@domainsbyproxy.com
Tech ID	Not Available From Registry
Tech Name	
Tech Organization	Domains By Proxy, LLC
Tech Address	
Tech City	Scottsdale
Tech State/Province	Arizona
Tech Country	US
Tech Postal Code	85260
Tech Phone	
Tech Phone Ext	
Tech Fax	
Tech Fax Ext	
Tech Email	c9b5a1cf1d0c3764s@domainsbyproxy.com

Tech Email	c9b5a1cf1d0c3764s@domainsbyproxy.com
Registrar ID	
Registrar IANA ID	146
Registrar	GoDaddy.com, LLC
Registrar Registration Expiration Date	2023-06-06T02:04:22Z
Registrar URL	http://www.godaddy.com
Registrar WHOIS Server	whois.godaddy.com
Registrar Status	
Registrar Address	
Registrar City	
Registrar State/Province	
Registrar Country	
Registrar Postal Code	
Registrar Phone	
Registrar Fax	
Registrar Fax Ext	
Registrar Email	
Registrar Abuse Contact Email	abuse@godaddy.com
Registrar Abuse Contact Phone	+1.4806242505 | 480-624-2505
Sponsoring Registrar	

Whois Information

Tech Email	c9b5a1cf1d0c3764s@domainsbyproxy.com
Registrant Postal Code	b9448b1c75ff534d
Admin Country	US
Registrant Organization	b46a98a26fe2fd9f
Registrant Name	80315b2e6ac1a801
Admin Organization	Domains By Proxy, LLC
Registrar Registration Expiration Date	2023-06-06T02:04:22Z
Registrant Fax	9fad764be0c7e95d
Tech Organization	Domains By Proxy, LLC
Registrar IANA ID	146
DNSSEC	unsigned
Creation Date	2011-06-06T02:04:22Z
Updated Date	2020-02-10T04:49:39Z | 2020-02-10T04:49:41Z
Admin City	Scottsdale
Tech Country	US
Registry Admin ID	Not Available From Registry
Tech Postal Code	85260
Registrant Email	c9b5a1cf1d0c3764s@domainsbyproxy.com
Admin Postal Code	85260
Admin State/Province	Arizona
Admin Email	c9b5a1cf1d0c3764s@domainsbyproxy.com
Registrar URL	http://www.godaddy.com
Registry Tech ID	Not Available From Registry
Registry Registrant ID	Not Available From Registry
Registrant City	373f4980ad3d2d01
Registrar	GoDaddy.com, LLC
Registrant Fax Ext	3432650ec337c945
Registrant State/Province	30bdd2917a604c83
Registry Domain ID	1660071767_DOMAIN_COM-VRSN
Registrant Phone	d5f66d3a005b000d
Tech City	Scottsdale

Registry Expiry Date	2023-06-06T02:04:22Z
Name Server	INDRI.EZOICNS.COM | SAOLA.EZOICNS.COM
Registrar Abuse Contact Phone	+1.4806242505 | 480-624-2505
Domain Status	clientDeleteProhibited http://www.icann.org/epp#clientDeleteProhibited | clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited | clientRenewProhibited http://www.icann.org/epp#clientRenewProhibited | clientRenewProhibited https://icann.org/epp#clientRenewProhibited | clientTransferProhibited http://www.icann.org/epp#clientTransferProhibited | clientTransferProhibited https://icann.org/epp#clientTransferProhibited | clientUpdateProhibited http://www.icann.org/epp#clientUpdateProhibited | clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
Registrant Phone Ext	3432650ec337c945
Registrar WHOIS Server	whois.godaddy.com
Registrant Street	037792fd5a6fe619 | f38c0adea706dbc3
Registrar Abuse Contact Email	abuse@godaddy.com
Registrant Country	US
Tech State/Province	Arizona
Domain Name	W3SNOOP.COM

Incoming (1)

DNS Name	w3snoop.com

IPv4 Address

maltego.IPv4Address

3.224.0.0

Weight	43
IP Address	3.224.0.0
Internal	false

Info

Relevance:	0.433512
Count:	1

Incoming (1)

IPv4 Address	3.234.104.255

IPv4 Address

maltego.IPv4Address

3.128.0.0

Weight	43
IP Address	3.128.0.0
Internal	false

Info

Relevance:	0.433512
Count:	1

Incoming (1)

IPv4 Address	3.234.104.255

IPv4 Address

maltego.IPv4Address

3.255.255.255

Weight	43
IP Address	3.255.255.255
Internal	false

Info

Relevance:	0.433512
Count:	1

Incoming (1)

IPv4 Address	3.234.104.255

IPv4 Address

maltego.IPv4Address

3.239.255.255

Weight	43
IP Address	3.239.255.255
Internal	false

Info

Relevance:	0.433512
Count:	1

Incoming (1)

IPv4 Address	3.234.104.255

A Record

maltego.ARecord

com.evil.co

Weight	0
IPv4 Address	52.128.23.153
Time to Live (TTL)	0
DNS Name	com.evil.co
Time To Live	3600
Type	A

Incoming (1)

DNS Name	com.evil.co

IPv4 Address

maltego.IPv4Address

18.156.95.187

Weight	0
IP Address	18.156.95.187
Internal	false
Date Resolved	2020-08-21T02:56:28Z
Resolver	VirusTotal

Incoming (1)

DNS Name	w3snoop.com

WHOIS Record

maltego.WHOISRecord

evil.com

Weight	0
Name	evil.com
WHOIS Info	Tech Email: 33c9a077fda0e4b4s@networksolutionsprivateregistration.com Registrant Postal Code: ecc83fcbe503dd84 Admin Country: US Registrant Organization: 3432650ec337c945 Registrant Name: 8792ba892fc41135 Registrar Registration Expiration Date: 2020-04-11T04:00:00Z Registrant Fax: 3432650ec337c945 Registrar IANA ID: 2 DNSSEC: unsigned Creation Date: 1995-04-10T04:00:00Z Updated Date: 2017-12-20T05:26:25Z | 2018-12-04T14:57:04Z Admin City: Jacksonville Tech Country: US Tech Postal Code: 32256 Registrant Email: 893a4025c10bd989s@networksolutionsprivateregistration.com Admin Postal Code: 32256 Admin State/Province: FL Admin Email: 893a4025c10bd989s@networksolutionsprivateregistration.com Registrar URL: http://networksolutions.com Registrant City: 55985aaef9d91102 Registrar: Network Solutions, LLC Registrant Fax Ext: 3432650ec337c945 Registrant State/Province: 6eb233f5a5adbed8 Registry Domain ID: 1040763_DOMAIN_COM-VRSN Registrant Phone: 40171cfbdb8fe780 Tech City: Jacksonville Registry Expiry Date: 2020-04-11T04:00:00Z Name Server: NS1.VERIO.COM | NS2.VERIO.COM Registrar Abuse Contact Phone: +1.8003337680 Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited | clientTransferProhibited https://icann.org/epp#clientTransferProhibited | clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited Registrant Phone Ext: 3432650ec337c945 Registrar WHOIS Server: whois.networksolutions.com Registrant Street: 8f73e9118a9c558c Registrar Abuse Contact Email: abuse@web.com Registrant Country: US Tech State/Province: FL Domain Name: EVIL.COM
Registry Domain ID	1040763_DOMAIN_COM-VRSN
Domain Name	EVIL.COM
Created Date	1995-04-10T04:00:00Z
Registry Expiry Date	2020-04-11T04:00:00Z
Updated Date	2017-12-20T05:26:25Z | 2018-12-04T14:57:04Z
Transfer Date	
Nameservers	NS1.VERIO.COM | NS2.VERIO.COM
Name Server IP Addresses	
Mantainer	
Created By	
Updated By	
DNSSEC	unsigned
Domain Status	clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited | clientTransferProhibited https://icann.org/epp#clientTransferProhibited | clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
ENS AuthId	
Registry Registrant ID	
Registrant Name	8792ba892fc41135
Registrant Organization	3432650ec337c945
Registrant Address	
Registrant Street	8f73e9118a9c558c
Registrant City	55985aaef9d91102

Registrant State/Province	6eb233f5a5adbed8
Registrant Country	US
Registrant Country Code	
Registrant Postal Code	ecc83fcbe503dd84
Registrant Phone	40171cfbdb8fe780
Registrant Phone Ext	3432650ec337c945
Registrant Fax	3432650ec337c945
Registrant Fax Ext	3432650ec337c945
Registrant Email	893a4025c10bd989s@networksolutionsprivateregistration.com
Admin ID	
Admin ID	
Admin Name	
Admin Organization	
Admin Address	
Admin Street	
Admin City	Jacksonville
Admin State/Province	FL
Admin Country	US
Admin Country Code	
Admin Postal Code	32256
Admin Phone	
Admin Phone Ext	
Admin Fax	
Admin Fax Ext	
Admin Email	893a4025c10bd989s@networksolutionsprivateregistration.com
Tech ID	
Tech Name	
Tech Organization	
Tech Address	
Tech City	Jacksonville
Tech State/Province	FL
Tech Country	US
Tech Postal Code	32256
Tech Phone	
Tech Phone Ext	
Tech Fax	
Tech Fax Ext	
Tech Email	33c9a077fda0e4b4s@networksolutionsprivateregistration.com
Registrar ID	
Registrar IANA ID	2
Registrar	Network Solutions, LLC
Registrar Registration Expiration Date	2020-04-11T04:00:00Z
Registrar URL	http://networksolutions.com
Registrar WHOIS Server	whois.networksolutions.com
Registrar Status	
Registrar Address	
Registrar City	
Registrar State/Province	
Registrar Country	
Registrar Postal Code	

Registrar Postal Code	
Registrar Phone	
Registrar Fax	
Registrar Fax Ext	
Registrar Email	
Registrar Abuse Contact Email	abuse@web.com
Registrar Abuse Contact Phone	+1.8003337680
Sponsoring Registrar	

Whois Information

Tech Email	33c9a077fda0e4b4s@networksolutionsprivateregistration.com
Registrant Postal Code	ecc83fcbe503dd84
Admin Country	US
Registrant Organization	3432650ec337c945
Registrant Name	8792ba892fc41135
Registrar Registration Expiration Date	2020-04-11T04:00:00Z
Registrant Fax	3432650ec337c945
Registrar IANA ID	2
DNSSEC	unsigned
Creation Date	1995-04-10T04:00:00Z
Updated Date	2017-12-20T05:26:25Z | 2018-12-04T14:57:04Z
Admin City	Jacksonville
Tech Country	US
Tech Postal Code	32256
Registrant Email	893a4025c10bd989s@networksolutionsprivateregistration.com
Admin Postal Code	32256
Admin State/Province	FL
Admin Email	893a4025c10bd989s@networksolutionsprivateregistration.com
Registrar URL	http://networksolutions.com
Registrant City	55985aaef9d91102
Registrar	Network Solutions, LLC
Registrant Fax Ext	3432650ec337c945
Registrant State/Province	6eb233f5a5adbed8
Registry Domain ID	1040763_DOMAIN_COM-VRSN
Registrant Phone	40171cfbdb8fe780
Tech City	Jacksonville
Registry Expiry Date	2020-04-11T04:00:00Z
Name Server	NS1.VERIO.COM | NS2.VERIO.COM
Registrar Abuse Contact Phone	+1.8003337680

Domain Status	clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited | clientTransferProhibited https://icann.org/epp#clientTransferProhibited | clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
Registrant Phone Ext	3432650ec337c945
Registrar WHOIS Server	whois.networksolutions.com
Registrant Street	8f73e9118a9c558c
Registrar Abuse Contact Email	abuse@web.com
Registrant Country	US
Tech State/Province	FL
Domain Name	EVIL.COM

Incoming (1)

DNS Name	evil.com

IPv4 Address

maltego.IPv4Address

15.188.66.177

Weight	0
IP Address	15.188.66.177
Internal	false
Date Resolved	2020-09-20T05:52:28Z
Resolver	VirusTotal

Incoming (1)

DNS Name	w3snoop.com

WHOIS Record

maltego.WHOISRecord

evil.com

Weight	0
Name	evil.com
WHOIS Info	Name Server: NS1.VERIO.COM | NS2.VERIO.COM Registrar IANA ID: 2 Registrar Abuse Contact Phone: +1.8003337680 DNSSEC: unsigned Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited | clientTransferProhibited https://icann.org/epp#clientTransferProhibited | clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited Creation Date: 1995-04-10T04:00:00Z Registrar URL: http://networksolutions.com Registrar WHOIS Server: whois.networksolutions.com Updated Date: 2018-12-04T14:57:04Z Registrar: Network Solutions, LLC Registry Expiry Date: 2020-04-11T04:00:00Z Registrar Abuse Contact Email: abuse@web.com Registry Domain ID: 1040763_DOMAIN_COM-VRSN Domain Name: EVIL.COM
Registry Domain ID	1040763_DOMAIN_COM-VRSN
Domain Name	EVIL.COM
Created Date	1995-04-10T04:00:00Z
Registry Expiry Date	2020-04-11T04:00:00Z
Updated Date	2018-12-04T14:57:04Z
Transfer Date	
Nameservers	NS1.VERIO.COM | NS2.VERIO.COM
Name Server IP Addresses	
Mantainer	
Created By	
Updated By	
DNSSEC	unsigned
Domain Status	clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited | clientTransferProhibited https://icann.org/epp#clientTransferProhibited | clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
ENS AuthId	
Registry Registrant ID	
Registrant Name	
Registrant Organization	
Registrant Address	
Registrant Street	
Registrant City	
Registrant State/Province	
Registrant Country	
Registrant Country Code	
Registrant Postal Code	
Registrant Phone	
Registrant Phone Ext	
Registrant Fax	
Registrant Fax Ext	
Registrant Email	
Admin ID	
Admin ID	
Admin Name	
Admin Organization	
Admin Address	
Admin Street	
Admin City	

Admin City	
Admin State/Province	
Admin Country	
Admin Country Code	
Admin Postal Code	
Admin Phone	
Admin Phone Ext	
Admin Fax	
Admin Fax Ext	
Admin Email	
Tech ID	
Tech Name	
Tech Organization	
Tech Address	
Tech City	
Tech State/Province	
Tech Country	
Tech Postal Code	
Tech Phone	
Tech Phone Ext	
Tech Fax	
Tech Fax Ext	
Tech Email	
Registrar ID	
Registrar IANA ID	2
Registrar	Network Solutions, LLC
Registrar Registration Expiration Date	
Registrar URL	http://networksolutions.com
Registrar WHOIS Server	whois.networksolutions.com
Registrar Status	
Registrar Address	
Registrar City	
Registrar State/Province	
Registrar Country	
Registrar Postal Code	
Registrar Phone	
Registrar Fax	
Registrar Fax Ext	
Registrar Email	
Registrar Abuse Contact Email	abuse@web.com
Registrar Abuse Contact Phone	+1.8003337680
Sponsoring Registrar	

Whois Information	
Name Server	NS1.VERIO.COM | NS2.VERIO.COM
Registrar IANA ID	2
Registrar Abuse Contact Phone	+1.8003337680
DNSSEC	unsigned
Domain Status	clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited | clientTransferProhibited https://icann.org/epp#clientTransferProhibited | clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
Creation Date	1995-04-10T04:00:00Z
Registrar URL	http://networksolutions.com
Registrar WHOIS Server	whois.networksolutions.com
Updated Date	2018-12-04T14:57:04Z
Registrar	Network Solutions, LLC
Registry Expiry Date	2020-04-11T04:00:00Z
Registrar Abuse Contact Email	abuse@web.com
Registry Domain ID	1040763_DOMAIN_COM-VRSN
Domain Name	EVIL.COM

Whois Information	
Name Server	NS1.VERIO.COM | NS2.VERIO.COM
Registrar IANA ID	2
Registrar Abuse Contact Phone	+1.8003337680
DNSSEC	unsigned
Domain Status	clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited | clientTransferProhibited https://icann.org/epp#clientTransferProhibited | clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
Creation Date	1995-04-10T04:00:00Z
Registrar URL	http://networksolutions.com
Registrar WHOIS Server	whois.networksolutions.com
Updated Date	2018-12-04T14:57:04Z
Registrar	Network Solutions, LLC
Domain Name	EVIL.COM
Registrar Abuse Contact Email	abuse@web.com
Registry Domain ID	1040763_DOMAIN_COM-VRSN
Registry Expiry Date	2020-04-11T04:00:00Z

Incoming (1)	
DNS Name	evil.com

IPv4 Address

maltego.IPv4Address

3.126.196.163

Weight	0
IP Address	3.126.196.163
Internal	false
Date Resolved	2020-09-18T18:45:32Z
Resolver	VirusTotal

Incoming (1)	
DNS Name	w3snoop.com

Snapshot

maltego.wayback.Snapshot

2000 Oct 18: http://www.evil.com:80/

Weight	2523323
Timestamp	20001018072323
Description	2000 Oct 18: http://www.evil.com:80/
Web Archive URL	https://web.archive.org/web/20001018072323/http://www.evil.com:80/
Original URL	http://www.evil.com:80/
DateTime	18 Oct 2000 07:23:23 +0000
HTTP Status	200
Short title	
URL	https://web.archive.org/web/20001018072323if_/http://www.evil.com:80/
Title	https://web.archive.org/web/20001018072323if_/http://www.evil.com:80/

Entity Data

Archived Page URL	https://web.archive.org/web/20001018072323if_/http://www.evil.com:80/
Web Archive URL	https://web.archive.org/web/20001018072323/http://www.evil.com:80/
Snapshot DateTime	18 Oct 2000 07:23:23 +0000
Original URL	http://www.evil.com:80/

Incoming (1)

Domain	evil.com

WHOIS Record

maltego.WHOISRecord

evil.com

Weight	0
Name	evil.com
WHOIS Info	Tech Email: 05fb701229338138s@networksolutionsprivateregistration.com Registrant Postal Code: ecc83fcbe503dd84 Admin Country: US Registrant Organization: 3432650ec337c945 Registrant Name: 8792ba892fc41135 Registrar Registration Expiration Date: 2023-04-11T04:00:00Z Registrant Fax: 3432650ec337c945 Registrar IANA ID: 2 DNSSEC: unsigned Creation Date: 1995-04-10T04:00:00Z Updated Date: 2019-12-17T16:17:59Z | 2019-12-17T16:51:42Z Admin City: Jacksonville Tech Country: US Tech Postal Code: 32256 Registrant Email: ba70359326469e61s@networksolutionsprivateregistration.com Admin Postal Code: 32256 Admin State/Province: FL Admin Email: ba70359326469e61s@networksolutionsprivateregistration.com Registrar URL: http://networksolutions.com Registrant City: 55985aaef9d91102 Registrar: Network Solutions, LLC Registrant Fax Ext: 3432650ec337c945 Registrant State/Province: 6eb233f5a5adbed8 Registry Domain ID: 1040763_DOMAIN_COM-VRSN Registrant Phone: 40171cfbdb8fe780 Tech City: Jacksonville Registry Expiry Date: 2023-04-11T04:00:00Z Name Server: NS1.VERIO.COM | NS2.VERIO.COM Registrar Abuse Contact Phone: +1.8003337680 Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited | clientTransferProhibited https://icann.org/epp#clientTransferProhibited | clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited Registrant Phone Ext: 3432650ec337c945 Registrar WHOIS Server: whois.networksolutions.com Registrant Street: 8f73e9118a9c558c Registrar Abuse Contact Email: abuse@web.com Registrant Country: US Tech State/Province: FL Domain Name: EVIL.COM
Registry Domain ID	1040763_DOMAIN_COM-VRSN
Domain Name	EVIL.COM
Created Date	1995-04-10T04:00:00Z
Registry Expiry Date	2023-04-11T04:00:00Z
Updated Date	2019-12-17T16:17:59Z | 2019-12-17T16:51:42Z
Transfer Date	
Nameservers	NS1.VERIO.COM | NS2.VERIO.COM
Name Server IP Addresses	
Mantainer	
Created By	
Updated By	
DNSSEC	unsigned
Domain Status	clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited | clientTransferProhibited https://icann.org/epp#clientTransferProhibited | clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
ENS AuthId	
Registry Registrant ID	
Registrant Name	8792ba892fc41135
Registrant Organization	3432650ec337c945
Registrant Address	
Registrant Street	8f73e9118a9c558c
Registrant City	55985aaef9d91102

Registrant State/Province	6eb233f5a5adbed8
Registrant Country	US
Registrant Country Code	
Registrant Postal Code	ecc83fcbe503dd84
Registrant Phone	40171cfbdb8fe780
Registrant Phone Ext	3432650ec337c945
Registrant Fax	3432650ec337c945
Registrant Fax Ext	3432650ec337c945
Registrant Email	ba70359326469e61s@networksolutionsprivateregistration.com
Admin ID	
Admin ID	
Admin Name	
Admin Organization	
Admin Address	
Admin Street	
Admin City	Jacksonville
Admin State/Province	FL
Admin Country	US
Admin Country Code	
Admin Postal Code	32256
Admin Phone	
Admin Phone Ext	
Admin Fax	
Admin Fax Ext	
Admin Email	ba70359326469e61s@networksolutionsprivateregistration.com
Tech ID	
Tech Name	
Tech Organization	
Tech Address	
Tech City	Jacksonville
Tech State/Province	FL
Tech Country	US
Tech Postal Code	32256
Tech Phone	
Tech Phone Ext	
Tech Fax	
Tech Fax Ext	
Tech Email	05fb701229338138s@networksolutionsprivateregistration.com
Registrar ID	
Registrar IANA ID	2
Registrar	Network Solutions, LLC
Registrar Registration Expiration Date	2023-04-11T04:00:00Z
Registrar URL	http://networksolutions.com
Registrar WHOIS Server	whois.networksolutions.com
Registrar Status	
Registrar Address	
Registrar City	
Registrar State/Province	
Registrar Country	
Registrar Postal Code	

Registrar Postal Code	
Registrar Phone	
Registrar Fax	
Registrar Fax Ext	
Registrar Email	
Registrar Abuse Contact Email	abuse@web.com
Registrar Abuse Contact Phone	+1.8003337680
Sponsoring Registrar	

Whois Information

Tech Email	05fb701229338138s@networksolutionsprivateregistration.com
Registrant Postal Code	ecc83fcbe503dd84
Admin Country	US
Registrant Organization	3432650ec337c945
Registrant Name	8792ba892fc41135
Registrar Registration Expiration Date	2023-04-11T04:00:00Z
Registrant Fax	3432650ec337c945
Registrar IANA ID	2
DNSSEC	unsigned
Creation Date	1995-04-10T04:00:00Z
Updated Date	2019-12-17T16:17:59Z | 2019-12-17T16:51:42Z
Admin City	Jacksonville
Tech Country	US
Tech Postal Code	32256
Registrant Email	ba70359326469e61s@networksolutionsprivateregistration.com
Admin Postal Code	32256
Admin State/Province	FL
Admin Email	ba70359326469e61s@networksolutionsprivateregistration.com
Registrar URL	http://networksolutions.com
Registrant City	55985aaef9d91102
Registrar	Network Solutions, LLC
Registrant Fax Ext	3432650ec337c945
Registrant State/Province	6eb233f5a5adbed8
Registry Domain ID	1040763_DOMAIN_COM-VRSN
Registrant Phone	40171cfbdb8fe780
Tech City	Jacksonville
Registry Expiry Date	2023-04-11T04:00:00Z
Name Server	NS1.VERIO.COM | NS2.VERIO.COM
Registrar Abuse Contact Phone	+1.8003337680

Domain Status	clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited | clientTransferProhibited https://icann.org/epp#clientTransferProhibited | clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
Registrant Phone Ext	3432650ec337c945
Registrar WHOIS Server	whois.networksolutions.com
Registrant Street	8f73e9118a9c558c
Registrar Abuse Contact Email	abuse@web.com
Registrant Country	US
Tech State/Province	FL
Domain Name	EVIL.COM

Incoming (1)

DNS Name	evil.com

A Record

maltego.ARecord

evil.co

Weight	0
IPv4 Address	52.128.23.153
Time to Live (TTL)	0
DNS Name	evil.co
Time To Live	3599
Type	A

Incoming (1)

DNS Name	evil.co

IPv4 Address

maltego.IPv4Address

35.181.159.169

Weight	0
IP Address	35.181.159.169
Internal	false
Date Resolved	2020-12-11T13:18:46Z
Resolver	Offensive Security

Incoming (1)

DNS Name	w3snoop.com

Snapshot

maltego.wayback.Snapshot

2000 Oct 19: http://www.evil.com:80/

Weight	2524742
Timestamp	20001019070258
Description	2000 Oct 19: http://www.evil.com:80/
Web Archive URL	https://web.archive.org/web/20001019070258/http://www.evil.com:80/
Original URL	http://www.evil.com:80/
DateTime	19 Oct 2000 07:02:58 +0000
HTTP Status	200
Short title	
URL	https://web.archive.org/web/20001019070258if_/http://www.evil.com:80/
Title	https://web.archive.org/web/20001019070258if_/http://www.evil.com:80/

Entity Data

Archived Page URL	https://web.archive.org/web/20001019070258if_/http://www.evil.com:80/
Web Archive URL	https://web.archive.org/web/20001019070258/http://www.evil.com:80/
Snapshot DateTime	19 Oct 2000 07:02:58 +0000
Original URL	http://www.evil.com:80/

Incoming (1)

Domain	evil.com

WHOIS Record

maltego.WHOISRecord

evil.com

Weight	0
Name	evil.com
WHOIS Info	Name Server: NS1.VERIO.COM | NS2.VERIO.COM Registrar IANA ID: 2 Registrar Abuse Contact Phone: +1.8003337680 DNSSEC: unsigned Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited | clientTransferProhibited https://icann.org/epp#clientTransferProhibited | clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited Creation Date: 1995-04-10T04:00:00Z Registrar URL: http://networksolutions.com Registrar WHOIS Server: whois.networksolutions.com Updated Date: 2019-12-17T16:17:59Z Registrar: Network Solutions, LLC Domain Name: EVIL.COM Registrar Abuse Contact Email: abuse@web.com Registry Domain ID: 1040763_DOMAIN_COM-VRSN Registry Expiry Date: 2023-04-11T04:00:00Z
Registry Domain ID	1040763_DOMAIN_COM-VRSN
Domain Name	EVIL.COM
Created Date	1995-04-10T04:00:00Z
Registry Expiry Date	2023-04-11T04:00:00Z
Updated Date	2019-12-17T16:17:59Z
Transfer Date	
Nameservers	NS1.VERIO.COM | NS2.VERIO.COM
Name Server IP Addresses	
Mantainer	
Created By	
Updated By	
DNSSEC	unsigned
Domain Status	clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited | clientTransferProhibited https://icann.org/epp#clientTransferProhibited | clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
ENS AuthId	
Registry Registrant ID	
Registrant Name	
Registrant Organization	
Registrant Address	
Registrant Street	
Registrant City	
Registrant State/Province	
Registrant Country	
Registrant Country Code	
Registrant Postal Code	
Registrant Phone	
Registrant Phone Ext	
Registrant Fax	
Registrant Fax Ext	
Registrant Email	
Admin ID	
Admin ID	
Admin Name	
Admin Organization	
Admin Address	
Admin Street	
Admin City	

Admin City	
Admin State/Province	
Admin Country	
Admin Country Code	
Admin Postal Code	
Admin Phone	
Admin Phone Ext	
Admin Fax	
Admin Fax Ext	
Admin Email	
Tech ID	
Tech Name	
Tech Organization	
Tech Address	
Tech City	
Tech State/Province	
Tech Country	
Tech Postal Code	
Tech Phone	
Tech Phone Ext	
Tech Fax	
Tech Fax Ext	
Tech Email	
Registrar ID	
Registrar IANA ID	2
Registrar	Network Solutions, LLC
Registrar Registration Expiration Date	
Registrar URL	http://networksolutions.com
Registrar WHOIS Server	whois.networksolutions.com
Registrar Status	
Registrar Address	
Registrar City	
Registrar State/Province	
Registrar Country	
Registrar Postal Code	
Registrar Phone	
Registrar Fax	
Registrar Fax Ext	
Registrar Email	
Registrar Abuse Contact Email	abuse@web.com
Registrar Abuse Contact Phone	+1.8003337680
Sponsoring Registrar	

Whois Information	
Name Server	NS1.VERIO.COM | NS2.VERIO.COM
Registrar IANA ID	2
Registrar Abuse Contact Phone	+1.8003337680
DNSSEC	unsigned
Domain Status	clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited | clientTransferProhibited https://icann.org/epp#clientTransferProhibited | clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
Creation Date	1995-04-10T04:00:00Z
Registrar URL	http://networksolutions.com
Registrar WHOIS Server	whois.networksolutions.com
Updated Date	2019-12-17T16:17:59Z
Registrar	Network Solutions, LLC
Domain Name	EVIL.COM
Registrar Abuse Contact Email	abuse@web.com
Registry Domain ID	1040763_DOMAIN_COM-VRSN
Registry Expiry Date	2023-04-11T04:00:00Z

Incoming (1)	
DNS Name	evil.com

IPv4 Address

maltego.IPv4Address

52.47.187.175

Weight	0
IP Address	52.47.187.175
Internal	false
Date Resolved	2020-09-20T19:09:58Z
Resolver	VirusTotal

Incoming (1)	
DNS Name	w3snoop.com

Snapshot

maltego.wayback.Snapshot

2000 Oct 18: http://www.evil.com:80/

Weight	2523167
Timestamp	20001018044716
Description	2000 Oct 18: http://www.evil.com:80/
Web Archive URL	https://web.archive.org/web/20001018044716/http://www.evil.com:80/
Original URL	http://www.evil.com:80/
DateTime	18 Oct 2000 04:47:16 +0000
HTTP Status	200
Short title	
URL	https://web.archive.org/web/20001018044716if_/http://www.evil.com:80/
Title	https://web.archive.org/web/20001018044716if_/http://www.evil.com:80/

Entity Data

Archived Page URL	https://web.archive.org/web/20001018044716if_/http://www.evil.com:80/
Web Archive URL	https://web.archive.org/web/20001018044716/http://www.evil.com:80/
Snapshot DateTime	18 Oct 2000 04:47:16 +0000
Original URL	http://www.evil.com:80/

Incoming (1)

Domain	evil.com

IPv4 Address

maltego.IPv4Address

99.79.175.42

Weight	0
IP Address	99.79.175.42
Internal	false
Date Resolved	2021-04-02T14:04:07Z
Resolver	VirusTotal

Incoming (1)

DNS Name	w3snoop.com

IPv4 Address

maltego.IPv4Address

52.60.126.229

Weight	0
IP Address	52.60.126.229
Internal	false
Date Resolved	2021-02-05T07:46:16Z
Resolver	VirusTotal

Incoming (1)

DNS Name	w3snoop.com

Domain

maltego.Domain

apitwitter.com.w3snoop.com

Weight	0
Domain Name	apitwitter.com.w3snoop.com
WHOIS Info	Admin City: Tempe Admin Country: US Admin Email: c9b5a1cf1d0c3764s@domainsbyproxy.com Admin Organization: Domains By Proxy, LLC Admin Postal Code: 85284 Admin State/Province: Arizona Creation Date: 2011-06-05T21:04:22Z Creation Date: 2011-06-06T02:04:22Z DNSSEC: unsigned Domain Name: W3SNOOP.COM Domain Status: clientDeleteProhibited http://www.icann.org/epp#clientDeleteProhibited Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited Domain Status: clientRenewProhibited http://www.icann.org/epp#clientRenewProhibited Domain Status: clientRenewProhibited https://icann.org/epp#clientRenewProhibited Domain Status: clientTransferProhibited http://www.icann.org/epp#clientTransferProhibited Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Domain Status: clientUpdateProhibited http://www.icann.org/epp#clientUpdateProhibited Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited Name Server: INDRI.EZOICNS.COM Name Server: SAOLA.EZOICNS.COM Registrant City: a7319ae5e6c95df5 Registrant Country: US Registrant Email: c9b5a1cf1d0c3764s@domainsbyproxy.com Registrant Fax Ext: 3432650ec337c945 Registrant Fax: 9fad764be0c7e95d Registrant Name: 80315b2e6ac1a801 Registrant Organization: b46a98a26fe2fd9f Registrant Phone Ext: 3432650ec337c945 Registrant Phone: d5f66d3a005b000d Registrant Postal Code: 052e5bd148f904f9 Registrant State/Province: 30bdd2917a604c83 Registrant Street: 037792fd5a6fe619 Registrant Street: d733533b6a6c0c21 Registrar Abuse Contact Email: abuse@godaddy.com Registrar Abuse Contact Phone: +1.4806242505 Registrar Abuse Contact Phone: 480-624-2505 Registrar IANA ID: 146 Registrar Registration Expiration Date: 2023-06-05T21:04:22Z Registrar URL: http://www.godaddy.com Registrar WHOIS Server: whois.godaddy.com Registrar: GoDaddy.com, LLC Registry Admin ID: Not Available From Registry Registry Domain ID: 1660071767_DOMAIN_COM-VRSN Registry Expiry Date: 2023-06-06T02:04:22Z Registry Registrant ID: Not Available From Registry Registry Tech ID: Not Available From Registry Tech City: Tempe Tech Country: US Tech Email: c9b5a1cf1d0c3764s@domainsbyproxy.com Tech Organization: Domains By Proxy, LLC Tech Postal Code: 85284 Tech State/Province: Arizona Updated Date: 2020-02-09T21:49:40Z Updated Date: 2020-02-10T04:49:41Z

VirusTotal Domain Summary

VirusTotal Reputation	0
Tags	

VirusTotal Analysis Summary	
Aggregate Result	harmless - 86 / 86

VirusTotal Analysis Stats	
Analysis Type	Number of Analysis
Confirmed Timeout	0
Failure	0
Harmless	86
Malicious	0
Suspicious	0
Timeout	0
Type Unsupported	0
Undetected	0
Total	**86**

View on VirusTotal

GUI Url: https://www.virustotal.com/gui/domain/apitwitter.com.w3snoop.com

Community Votes

Total votes cast: 0

Incoming (1)

DNS Name	apitwitter.com.w3snoop.com

MX Record

maltego.MXRecord

mx.zoho.com

Weight	0
MX Record	mx.zoho.com
Priority	0
Time To Live	3600
Type	MX
Priority	0

Incoming (1)

DNS Name	w3snoop.com

NS Record

maltego.NSRecord

skunk.ezoicns.com

Weight	0
NS Record	skunk.ezoicns.com
Time To Live	21600
Type	NS

Incoming (1)

DNS Name	w3snoop.com

MX Record

maltego.MXRecord

mx2.zoho.com

Weight	0
MX Record	mx2.zoho.com
Priority	0
Time To Live	3600
Type	MX
Priority	0

Incoming (1)

DNS Name	w3snoop.com

Phrase

maltego.Phrase

google-site-verification=Z_UJlgtJtBjgdgQoxs4nDCo72fuLeSdHXHq8huCgmnw

Weight	0
Text	google-site-verification=Z_UJlgtJtBjgdgQoxs4nDCo72fuLeSdHXHq8huCgmnw
Time To Live	3600
Type	TXT

Incoming (1)

DNS Name	w3snoop.com

Phrase

maltego.Phrase

google-site-verification=Z_UJlgtJtBjgdgQoxs4nDCo72fuLeSdHXHq8huCgmn

Weight	0
Text	google-site-verification=Z_UJlgtJtBjgdgQoxs4nDCo72fuLeSdHXHq8huCgmn
Time To Live	3600
Type	TXT

Incoming (1)

DNS Name	w3snoop.com

A Record

maltego.ARecord

apitwitter.com.w3snoop.com

Weight	0
IPv4 Address	35.155.25.163
Time to Live (TTL)	0
DNS Name	apitwitter.com.w3snoop.com
Time To Live	59
Type	A

Incoming (1)

DNS Name	apitwitter.com.w3snoop.com

NS Record

maltego.NSRecord

sheep.ezoicns.com

Weight	0
NS Record	sheep.ezoicns.com
Time To Live	21600
Type	NS

Incoming (1)

DNS Name	w3snoop.com

NS Record

maltego.NSRecord

indri.ezoicns.com

Weight	0
NS Record	indri.ezoicns.com
Refresh	7200
Time To Live	900
Type	SOA
Expire	1209600
Minimum	86400
Serial	1
Rname	awsdns-hostmaster.amazon.com
Retry	900

Incoming (1)

DNS Name	w3snoop.com