Profiling Threat Actors with DNS

SANS DFIR 2020

Taylor Wilkes-Pierce, Senior Sales Engineer

DomainTools Data

Accurate

95%+ of currently registered domains

Timely

All newly registered and discovered domains

Comprehensive

Nearly two decades of historical WHOIS and pDNS data

DOMAINTOOLS®

Observations on Adversary Infrastructure

When malicious actors register and host domains they leave behind data for us to analyze

This data can be applied in our investigations of this activity and can aid our detection and response efforts

This data can give us insight into the operations, the targets of their attacks, the scale of their operations

-Domain Names

-Top Level Domains / Registrars

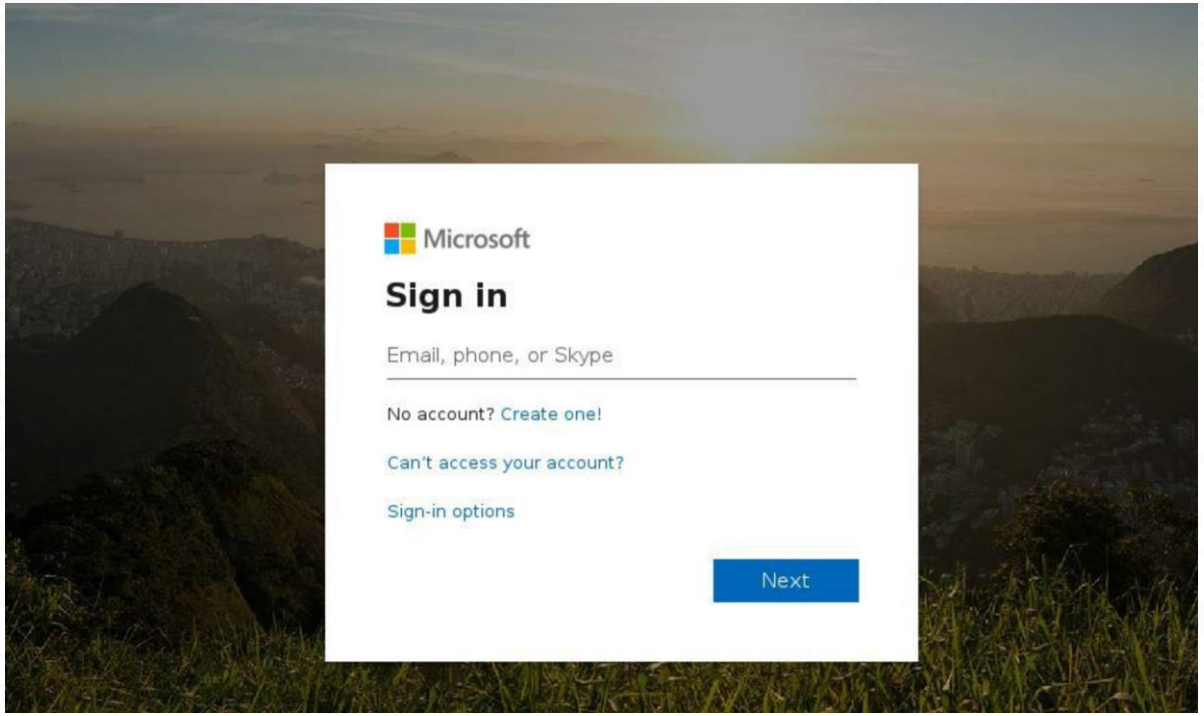
-Hosting Providers

DOMAINTOOLS®

What's in a Name?

Domain names can **reveal intent**

adfs-freedomhouse.org



DOMAINTOOLS®

What's in a Name?

Domain names can **reveal intent**

americanxpresslandingarea.com

americanexpresscustomerareaonline.com

americanexpresslandingarea.com

DOMAINTOOLS®

TL;DR on TLDs / Registrars

Registration Costs Vary Wildly

Top Level Domain	Registration
TK	$ 0.00
ML	$ 0.00
.law.pro	101domain $110.17
CF	$ 0.00
GQ	$ 0.00

**sources: TLD-list.com, freenom.com*

TL;DR c Registrars

Registrars can be

MarkMonitor

CSC

server-linode.in Inspect 1 Guided Pivot	100
securityreview.info Inspect Inactive	100
revoked.info Inspect Inactive	100
reviewsecurity.info Inspect Inactive	100
review-security.info Inspect Inactive 1 Guided Pivot	100
predatord.top Inspect	100

(990 records)

90 Avg Risk

NJALLA

freenom
A Name for Everyone

Hosting Providers

When pivoting on hosting IPv4s, tenancy is key

Multi Tenant Infrastructure

Shared / Managed Hosting / CDN / Domain Parking

Domains hosted on multi tenant IPs often have no relation to each other from an ownership perspective.

Hosting Providers

When pivoting on hosting IPv4s, tenancy is key

Single Tenant Infrastructure

Virtual Private Servers + Dedicated Servers

Pivot on and monitor single tenant IPv4s

IP	ISP IP Information	ASN	Country Code
66.70.191.37	OVH Hosting Inc.	16276	CA

~ 4 domains share this value.

IP

66.70.191.37

97 Avg Risk 27 Avg Age

DOMAIN	RISK SCORE
americanexpresscustomerareao...	100
americanexpresslandingarea.com	98
maintainceamericanexpresscust...	97
americanxpresslandingarea.com	95

Name Servers

Most users s viders default name serve

Bad actors a ey need greater cont

Deviation fr t pivots

Name Server IP

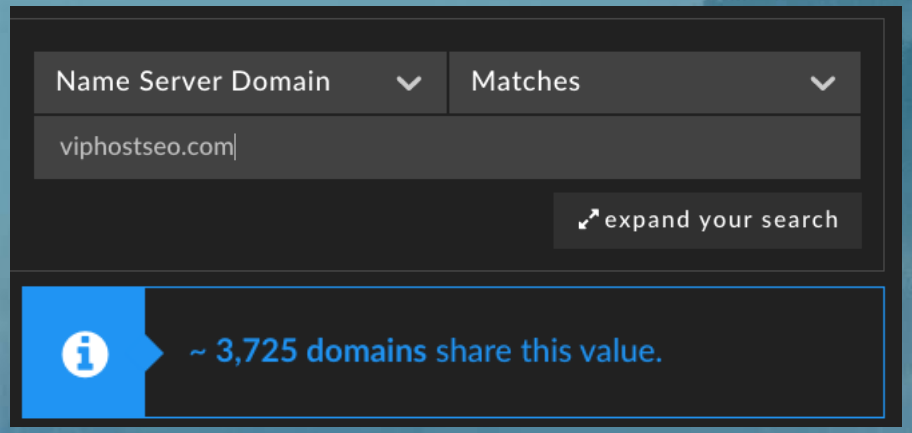
88.150.227.107

94 Avg Risk 1,105 Avg Age

DOMAIN	RISK SCORE
venionne.com	100
ucairtz.com	100
tefanortin.com	100
rcuselynac.com	100
ntjeilliams.com	100
myolton.com	100
irkaimboeuf.com	100
hieryells.com	100
eighrimeau.com	100
carosseda.com	100
adineohler.com	100
vieoulden.com	87
ugdale.com	87
stianois.com	87
saachumpert.com	87
phieuckson.com	87
licailliam.com	87
lausarieur.com	87
eoilson.com	87
denones.com	87

Name Servers

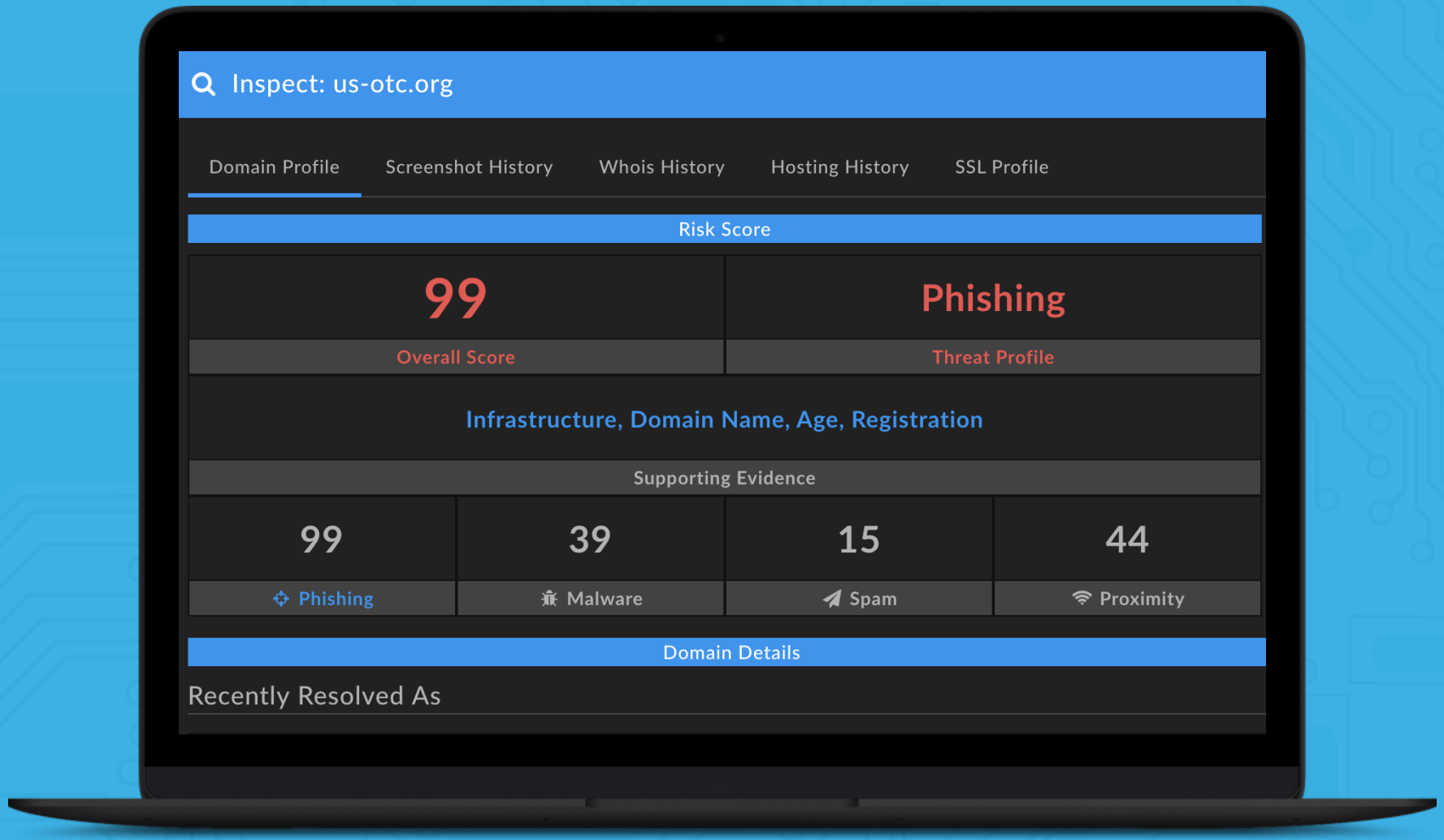
Hosting Providers and their Name Servers can be overrun by malicious activity (perhaps by design?)



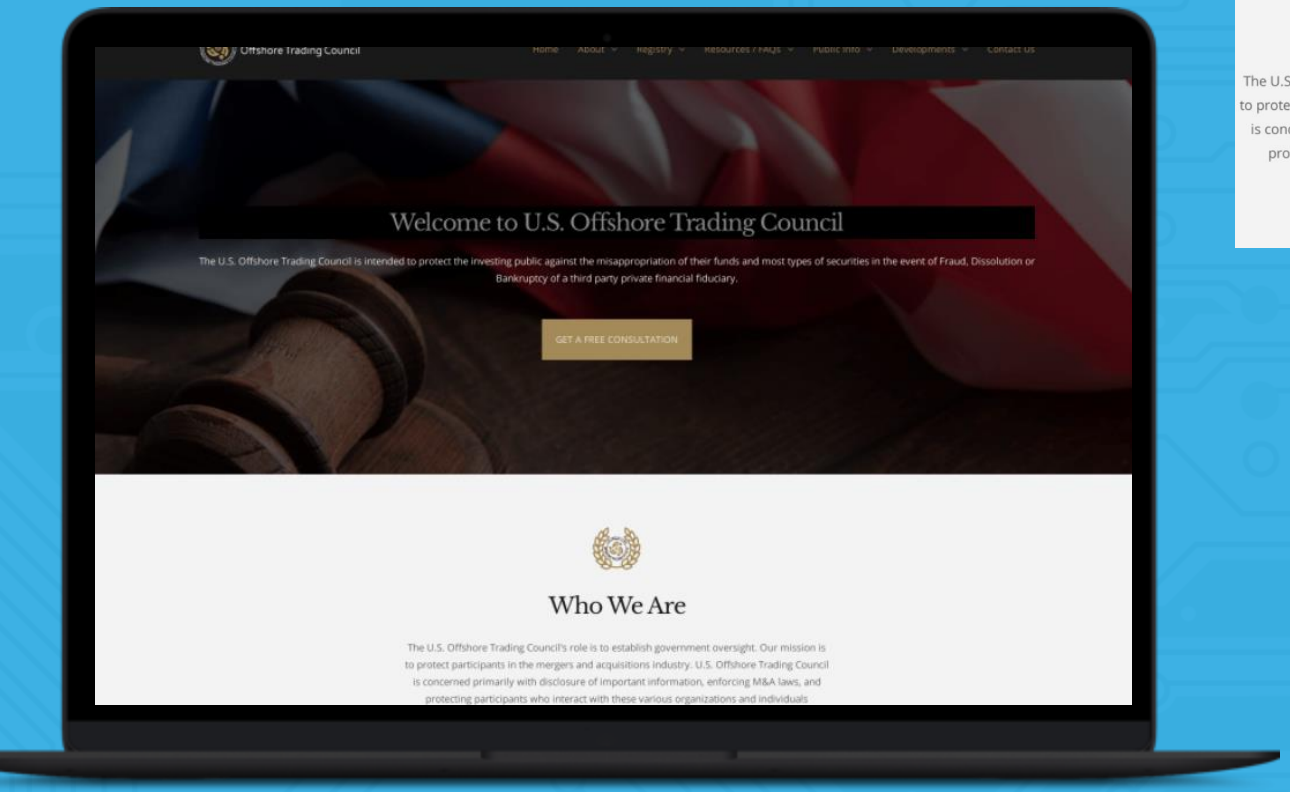
Domain	Risk Score	IP	Create Date	SSL Information	Registrar	Registrant Organization	Contact Information
st-andrews-ac-uk.com Inspect 6 Guided Pivots	95		2020-07-04 *2 days old*		PDR Ltd. d/b/a PublicDomainRegistry.com	macronicltd	Name: Justin Wilson Organiza: macronic
1reliances-ua.com Inspect Inactive	90		2020-07-04 *2 days old*		PDR LTD. D/B/A PUBLICDOMAINREGISTRY.COM	GDPR Masked	Name: GDPR Masked Organiz: GDPR M GDPR Masked GDPR M
uttaragrou.com Inspect 1 Guided Pivot	79		2020-07-03 *3 days old*		PDR LTD. D/B/A PUBLICDOMAINREGISTRY.COM	GDPR Masked	Name: GDPR Masked Organiz: GDPR M GDPR Masked GDPR M
newx-lnc.com Inspect 6 Guided Pivots	99		2020-07-03 *3 days old*		PDR Ltd. d/b/a PublicDomainRegistry.com	Charles Southward Inc	Name: Charles Southward Orga: Char

Domain	Risk Score	IP	Create Date	SSL Information	Registrar	Registrant Organization	Contact Information
plumrver.com Inspect 6 Guided Pivots	76		2020-07-02 *4 days old*		PDR LTD. D/B/A PUBLICDOMAINREGISTRY.COM	kevin Ltd	Name: kevin owen Organizatic: kevin Ltd
joebiiden.com Inspect 6 Guided Pivots	73		2020-07-02 *4 days old*		PDR LTD. D/B/A PUBLICDOMAINREGISTRY.COM	Jirk Enterprice	Name: Tam Jirk Organization: Jirk Enterprice
egmddleton.com Inspect 5 Guided Pivots	99		2020-07-02 *4 days old*		PDR LTD. D/B/A PUBLICDOMAINREGISTRY.COM	james smith inc	Name: peter smith Organizati: james smit
badael-sa.com Inspect 1 Guided Pivot	86		2020-07-02 *4 days old*		PDR LTD. D/B/A PUBLICDOMAINREGISTRY.COM	GDPR Masked	Name: GDPR Masked Organiz: GDPR M GDPR Masked GDPR M

Pivoting Outside of DNS



DOMAINTOOLS®



Create Date

2020-02-04
103 days old

Registrar

Hosting Concepts B.V. d/b/a Openprovider

IP

IP	ISP IP Information	ASN	Country Code
91.235.116.180	THC Projects SRL	51177	FR

DOMAINTOOLS®

SSL Cert Discovery

	us-otc.org
	f458215368099f870e2de8eed39c99280c937a13

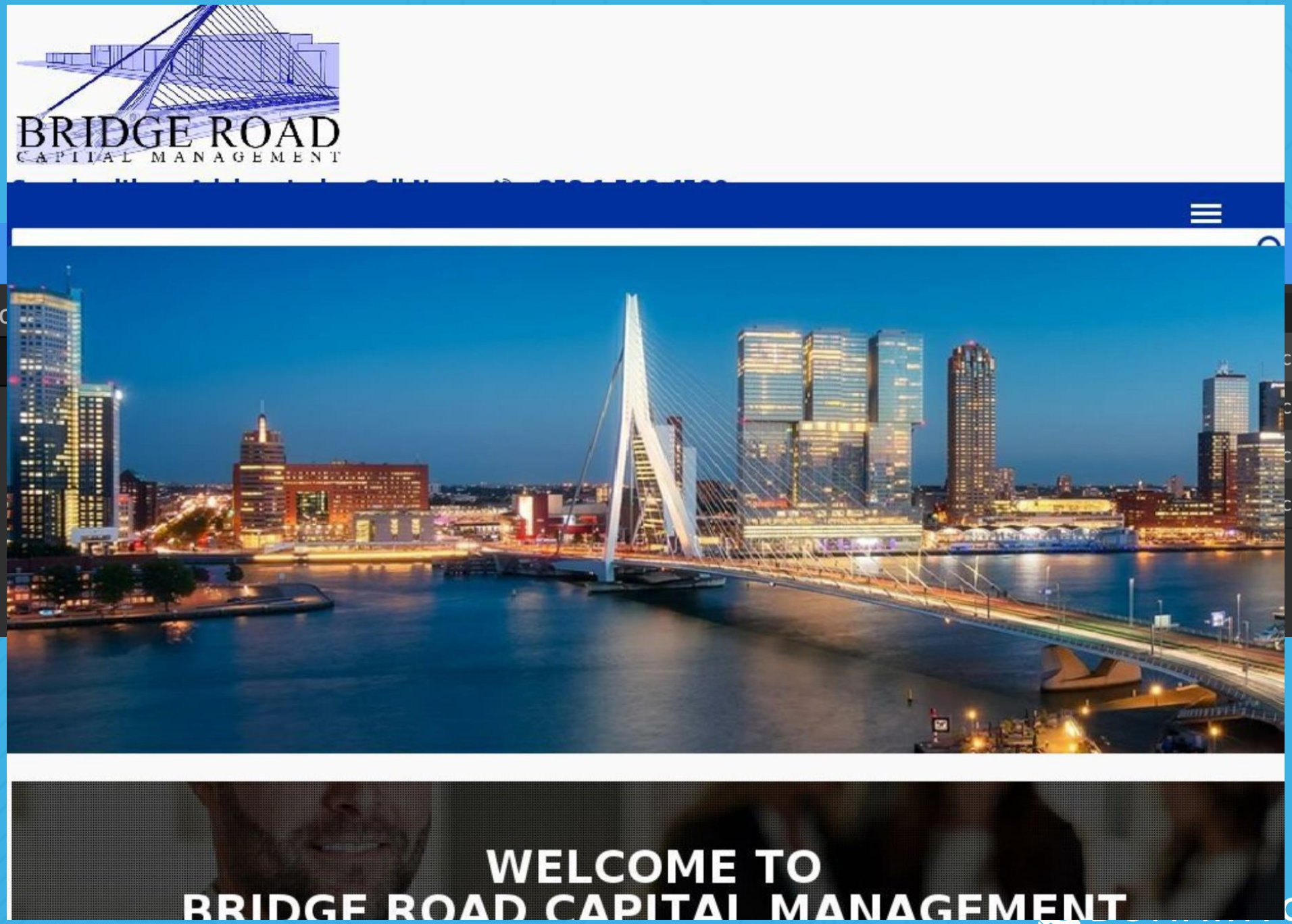
Subject

OID	Value
Subject DN	CN=us-otc.brcm-ie.co
Common Name	us-otc.brcm-ie.co

Issuer

OID	Value
Issuer DN	CN=cPanel\, Inc. Certification Authority,O=cPanel\, Inc.,L=Houston,ST=TX,C=US
Common Name	cPanel, Inc. Certification Authority
Organization Name	cPanel, Inc.
Locality Name	Houston
State Or Province Name	TX
Country Name	US

DOMAINTOOLS®



Domain

brcm-ie.co

Inspect

IP Information

com 192.99.35.216

com 37.187.75.23

com 192.95.19.72

com 94.23.167.164

OOLS®

Domain

bridgestreetca

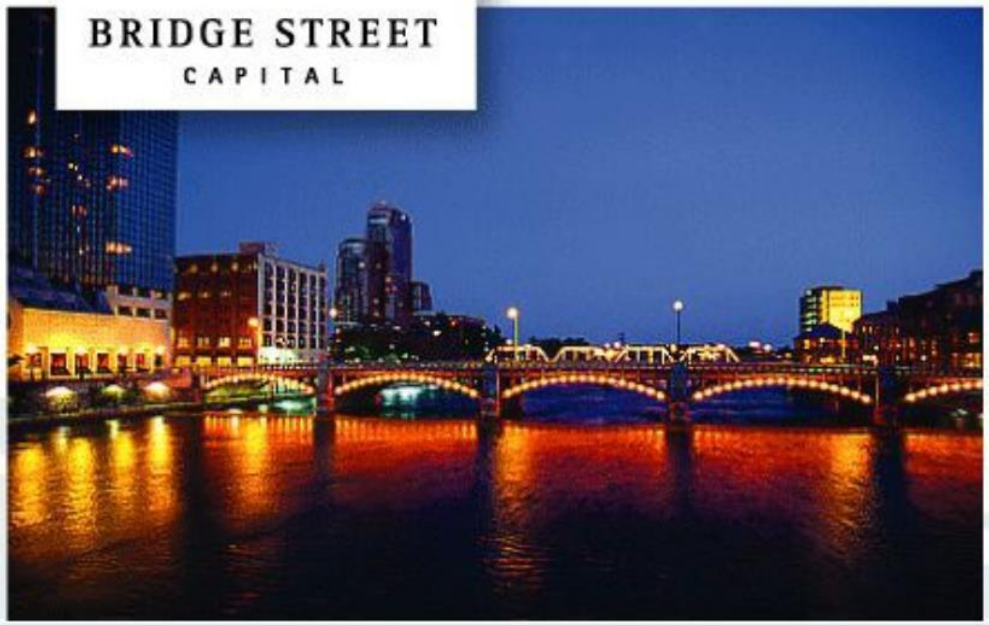
Inspect

8 Guided Pivots

ormation

533e8e93d

BRIDGE STREET
CAPITAL



Strong Principles. Applied Expertise.

» ENTER **Bridge Street Capital Partners LLC.**
connecting profitable growth companies to
the private equity capital we manage.

98 Avg Risk 92 Avg Age

Download | Page 1 of 1 *(2 records)*

Domain	Risk Score	IP	Create Date	Name Server	SSL Information
brcm-ie.co Inspect	98	IP: 91.235.116.180 ISP IP Information: THC Projects SRL ASN: 51177 Country Code: FR	2020-02-27 *80 days old*	Hostname / IP Information: ns1.thcservers.com 192.99.35.216 ns2.thcservers.com 37.187.75.23 ns3.thcservers.com 192.95.19.72 ns4.thcservers.com 94.23.167.164	Hash: eff4d177b2896774e56b2932735
us-otc.org Inspect	99	IP: 91.235.116.180 ISP IP Information: THC Projects SRL ASN: 51177 Country Code: FR	2020-02-04 *103 days old*	Hostname / IP Information: ns1.thcservers.com 192.99.35.216 ns2.thcservers.com 37.187.75.23 ns3.thcservers.com 192.95.19.72 ns4.thcservers.com 94.23.167.164	Hash: f458215368099f870e2de8eed39

DOMAINTOOLS®

98 Avg Risk 92 Avg Age

Download | Page 1 of 1 *(2 records)*

Filters

Narrow Search
Expand Search
New Search
Exclude

IP Tools

IP Profile
Ping
Traceroute
PTR

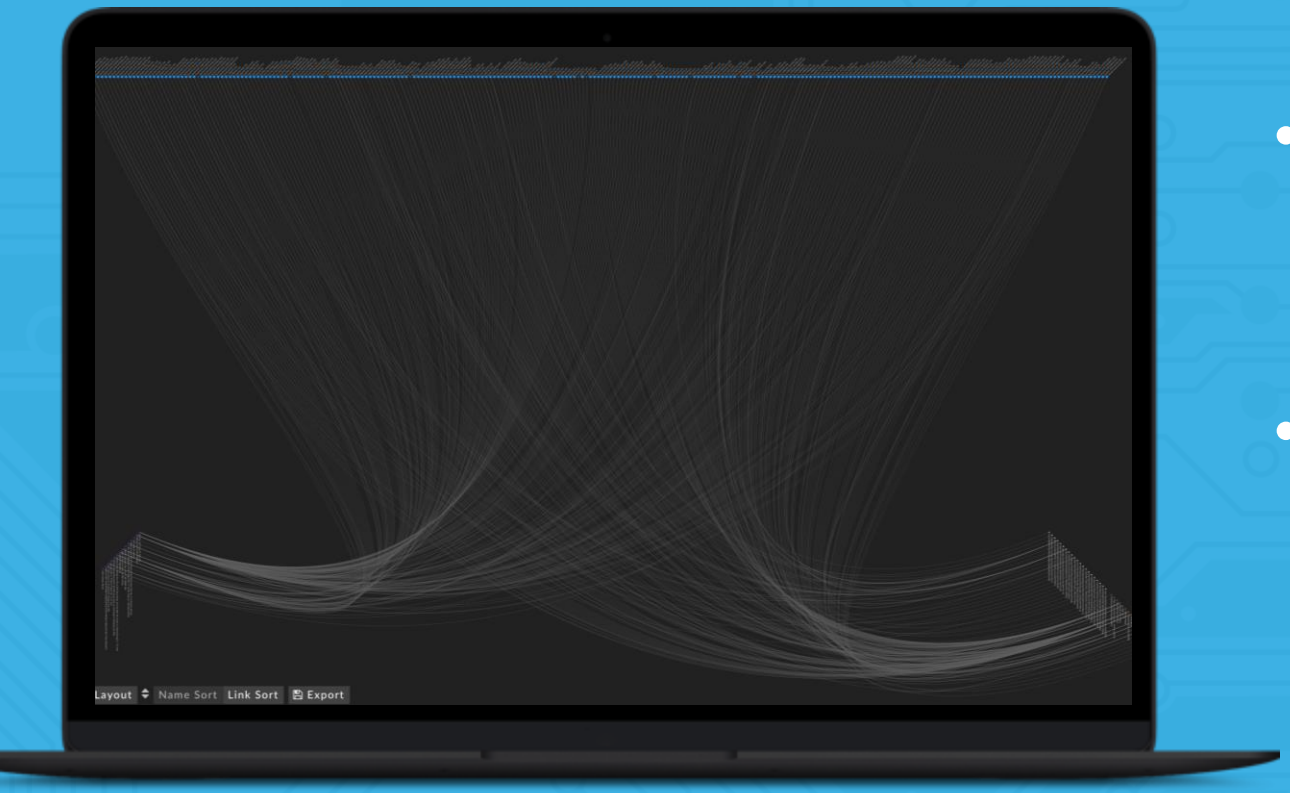
Pin IP | pDNS

~ 1,151 domains share this value.

Domain	Risk Score	IP	Name Server	SSL Information
brcm-ie.co Inspect	98	IP: 91.235.116.180	Hostname / IP Information: ns1.thcservers.com 192.99.35.216 ns2.thcservers.com 37.187.75.23 ns3.thcservers.com 192.95.19.72 ns4.thcservers.com 94.23.167.164	Hash: eff4d177b2896774e56b2932735
us-otc.org Inspect	99	IP / ISP IP Information / ASN / Country Code: 91.235.116.180 THC Projects SRL 51177 FR 2020-02-04 *103 days old*	Hostname / IP Information: ns1.thcservers.com 192.99.35.216 ns2.thcservers.com 37.187.75.23 ns3.thcservers.com 192.95.19.72 ns4.thcservers.com 94.23.167.164	Hash: f458215368099f870e2de8eed39

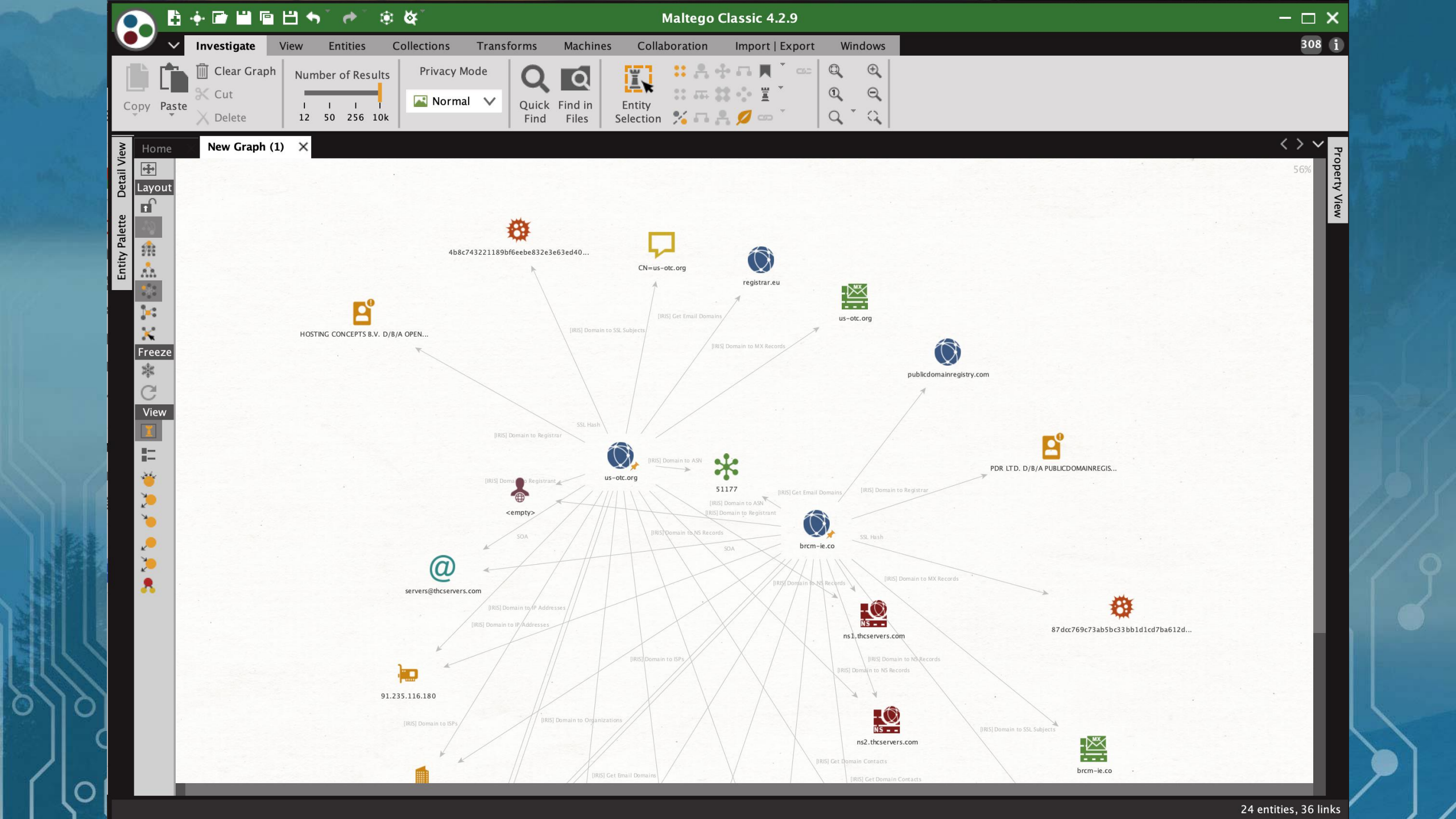
DOMAINTOOLS®

Investigating with Infrastructure OSINT



- Defined investigative pathways speed response times
- Access to Indexed Infrastructure OSINT gives insight into adversary activity
- APIs provide data portability

DOMAINTOOLS®


Maltego Classic 4.2.9
Investigate
View
Entities
Collections
Transforms
Machines
Collaboration
Import | Export
Windows
308
Copy
Paste
Clear Graph
Cut
Delete
Number of Results
12
50
256
10k
Privacy Mode
Normal
Quick Find
Find in Files
Entity Selection
Detail View
Entity Palette
Home
New Graph (1)
Layout
Freeze
View
Property View
56%
4b8c743221189bf6eebe832e3e63ed40...
CN=us-otc.org
registrar.eu
us-otc.org
HOSTING CONCEPTS B.V. D/B/A OPEN...
publicdomainregistry.com
PDR LTD. D/B/A PUBLICDOMAINREGIS...
us-otc.org
51177
<empty>
brcm-ie.co
servers@thcservers.com
ns1.thcservers.com
87dcc769c73ab5bc33bb1d1cd7ba612d...
91.235.116.180
ns2.thcservers.com
brcm-ie.co
[IRIS] Domain to SSL Subjects
[IRIS] Get Email Domains
[IRIS] Domain to MX Records
SSL Hash
[IRIS] Domain to Registrar
[IRIS] Domain to ASN
[IRIS] Domain to Registrant
SOA
[IRIS] Domain to NS Records
[IRIS] Domain to IP Addresses
[IRIS] Domain to ISPs
[IRIS] Domain to Organizations
[IRIS] Get Domain Contacts
24 entities, 36 links

Galaxies

« previous | next » | view all

MISP Threat Sharing

Date	Org	Category	Type	Value	Tags	Galaxies	Comment	Correlate	Related Events	Feed hits	IDS	Distribution	Sightings	Activity	Actions
2020-06-15		Network activity	email-dst	servers@thcservers.com	DomainTools Iris		SOA email (GP: 13,648) from DomainTools Iris	✓				Inherit	(0/0/0)		
2020-06-15		External analysis	ip-src	91.235.116.180	DomainTools Iris		Mail Server IP (GP: 1,525) from DomainTools Iris	✓				Inherit	(0/0/0)		
2020-06-15		External analysis	domain	us-otc.org	DomainTools Iris Guided Pivot		Mail Server Domain (GP: 1) from DomainTools Iris	✓				Inherit	(0/0/0)		
2020-06-15		External analysis	hostname	us-otc.org	DomainTools Iris Guided Pivot		Mail Server Host (GP: 1) from DomainTools Iris	✓				Inherit	(0/0/0)		
2020-06-15		External analysis	ip-src	94.23.167.164	DomainTools Iris		Name Server IP (GP: 11,604) from DomainTools Iris	✓				Inherit	(0/0/0)		
2020-06-15		External analysis	hostname	ns4.thcservers.com	DomainTools Iris		Name Server Host (GP: 11,353) from DomainTools Iris	✓				Inherit	(0/0/0)		
2020-06-15		External analysis	ip-src	192.95.19.72	DomainTools Iris		Name Server IP (GP: 11,866) from DomainTools Iris	✓				Inherit	(0/0/0)		
2020-06-15		External analysis	hostname	ns3.thcservers.com	DomainTools		Name Server Host	✓				Inherit			

DomainTools / playbooks

Watch 6 | Star 0 | Fork 1

Code | Issues 0 | Pull requests 0 | Actions | Projects 0 | Security 0 | Insights

Playbooks to utilize DomainTools data in your security orchestration system

20 commits | 6 branches | 0 packages | 0 releases | 3 contributors

Branch: master | New pull request | Find file | Clone or download

kacieh80 Merge pull request #7 from DomainTools/update_phantom_pb ... Latest commit e07898d on Feb 4

Demisto	Updates to playbooks and automation scripts for Demisto.	6 months ago
Splunk Phantom	Change pivot action from pivot to pivot action for 1.1	7 months ago
README.md	No commit message	7 months ago

README.md

DomainTools Playbooks:

Templates of playbooks and automation scripts inside SOAR applications to automate incident response activities utilizing DomainTools intelligence.

Bringing Infrastructure Intel into the SIEM

Iris Enrich API purpose-built for large-scale event decoration

- Proxy Logs
- DNS Query Logs
- Email Domain Logs

DOMAINTOOLS®

Actor Profiling with OSINT

C&C Servers

ms-ethics.net

deb-cn.net

ap1-acl.net

ms-db.net

aws-check.net

reawk.net

TREND MICRO | SECURITY INTELLIGENCE Blog

SECURITY NEWS DIRECT FROM THREAT DEFENSE EXPERTS

Home | Categories

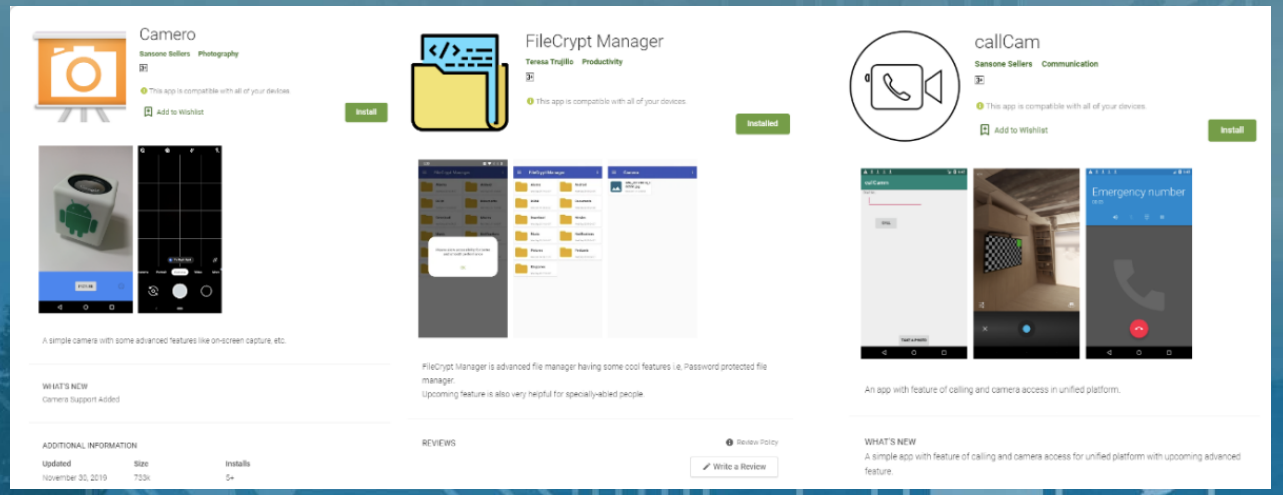
Home » Exploits » First Active Attack Exploiting CVE-2019-2215 Found on Google Play, Linked to SideWinder APT Group

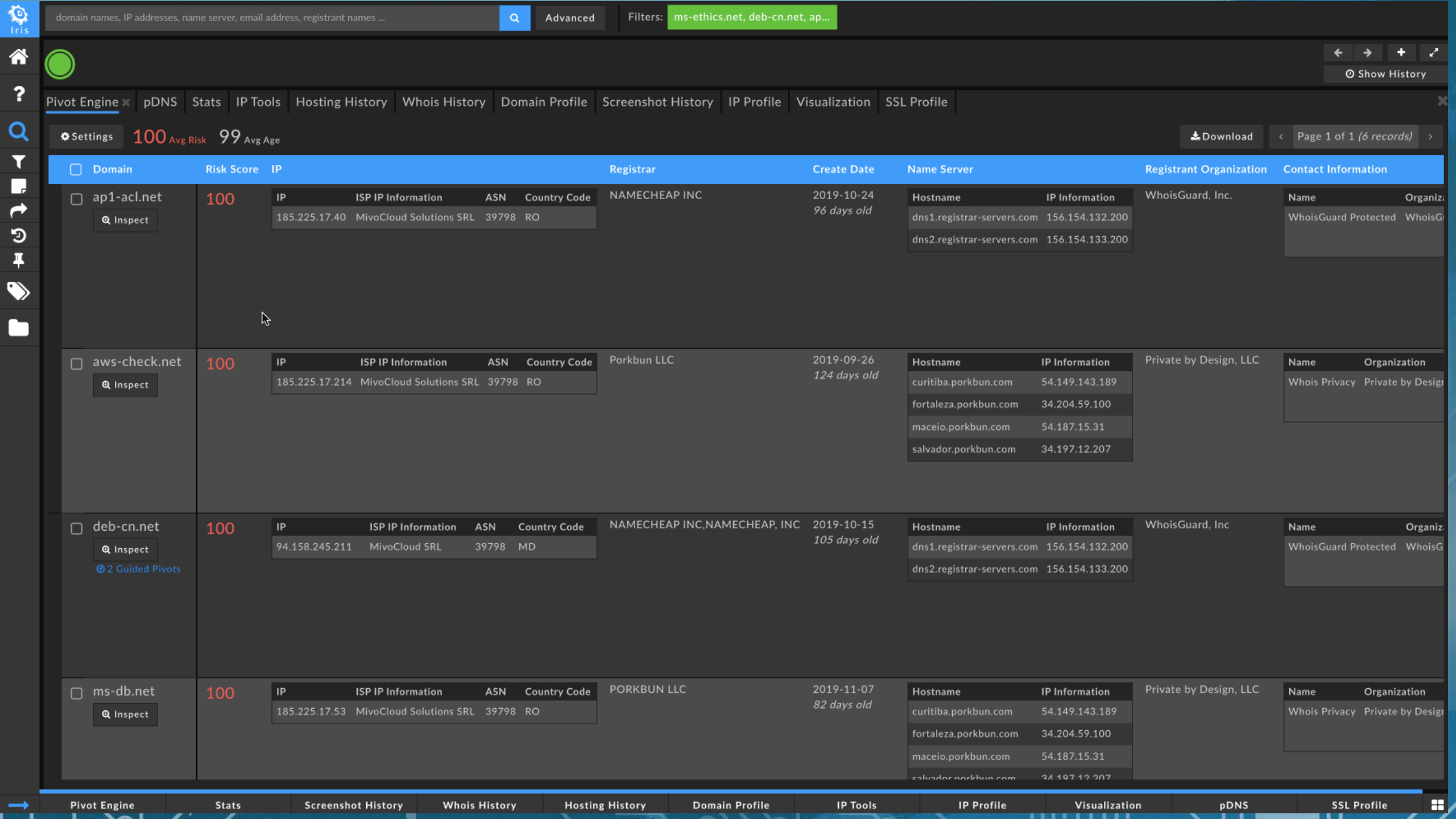
First Active Attack Exploiting CVE-2019-2215 Found on Google Play, Linked to SideWinder APT Group

Posted on: January 6, 2020 at 5:00 am **Posted in:** Exploits, Mobile **Author:** Trend Micro

230

by Ecular Xu and Joseph C Chen




domain names, IP addresses, name server, email address, registrant names ...
Advanced
Filters: ms-ethics.net, deb-cn.net, ap...
Show History
Pivot Engine
pDNS
Stats
IP Tools
Hosting History
Whois History
Domain Profile
Screenshot History
IP Profile
Visualization
SSL Profile
Settings
100 Avg Risk
99 Avg Age
Download
Page 1 of 1 (6 records)
Domain
Risk Score
IP
Registrar
Create Date
Name Server
Registrant Organization
Contact Information
ap1-acl.net
Inspect
100
IP
ISP IP Information
ASN
Country Code
185.225.17.40
MivoCloud Solutions SRL
39798
RO
NAMECHEAP INC
2019-10-24
96 days old
Hostname
IP Information
dns1.registrar-servers.com
156.154.132.200
dns2.registrar-servers.com
156.154.133.200
WhoisGuard, Inc.
Name
Organiz
WhoisGuard Protected
WhoisG
aws-check.net
Inspect
100
IP
ISP IP Information
ASN
Country Code
185.225.17.214
MivoCloud Solutions SRL
39798
RO
Porkbun LLC
2019-09-26
124 days old
Hostname
IP Information
curitiba.porkbun.com
54.149.143.189
fortaleza.porkbun.com
34.204.59.100
maceio.porkbun.com
54.187.15.31
salvador.porkbun.com
34.197.12.207
Private by Design, LLC
Name
Organization
Whois Privacy
Private by Design
deb-cn.net
Inspect
2 Guided Pivots
100
IP
ISP IP Information
ASN
Country Code
94.158.245.211
MivoCloud SRL
39798
MD
NAMECHEAP INC,NAMECHEAP, INC
2019-10-15
105 days old
Hostname
IP Information
dns1.registrar-servers.com
156.154.132.200
dns2.registrar-servers.com
156.154.133.200
WhoisGuard, Inc
Name
Organiz
WhoisGuard Protected
WhoisG
ms-db.net
Inspect
100
IP
ISP IP Information
ASN
Country Code
185.225.17.53
MivoCloud Solutions SRL
39798
RO
PORKBUN LLC
2019-11-07
82 days old
Hostname
IP Information
curitiba.porkbun.com
54.149.143.189
fortaleza.porkbun.com
34.204.59.100
maceio.porkbun.com
54.187.15.31
Private by Design, LLC
Name
Organization
Whois Privacy
Private by Design
Pivot Engine
Stats
Screenshot History
Whois History
Hosting History
Domain Profile
IP Tools
IP Profile
Visualization
pDNS
SSL Profile

Certificates and Subdomains

OID	Value
Subject Alt Name	• ap1-acl.net • cdn.ap1-acl.net • www.ap1-acl.net
Subject Alt Name	• aws-check.net • cdn.aws-check.net • www.aws-check.net
Subject Alt Name	• cdn.ms-db.net • ms-db.net • www.ms-db.net
Subject Alt Name	• cdn.ms-ethics.net • ms-ethics.net • www.ms-ethics.net
Subject Alt Name	• cdn.ms-ethics.net • ms-ethics.net • www.ms-ethics.net
Subject Alt Name	• cdn.reawk.net • reawk.net • www.reawk.net

Recently Resolved As

test.bad.dns.ap1-acl.net	185.225.17.40
cdn.ap1-acl.net	185.225.17.40
ap1-acl.net	185.225.17.40

Recently Resolved As

www.aws-check.net	185.225.17.214
aws-check.net	185.225.17.214
cdn.aws-check.net	185.225.17.214

Recently Resolved As

www.deb-cn.net	94.158.245.211
cdn.deb-cn.net	94.158.245.211
deb-cn.net	94.158.245.211

cdn.ms-db.net	A	C	2	185.225.17.53	2019-11-18, 13:28	2019-11-18, 13:28
cdn.ms-db.net	A	D	2	185.225.17.53	2019-11-08, 13:38	2019-11-08, 13:38
cdn.ms-db.net	A	A	1	185.225.17.53	2019-11-08, 09:27	2020-01-12, 01:11

Recently Resolved As

cdn.ms-ethics.net	185.225.17.205
www.ms-ethics.net	185.225.17.205
ms-ethics.net	185.225.17.205

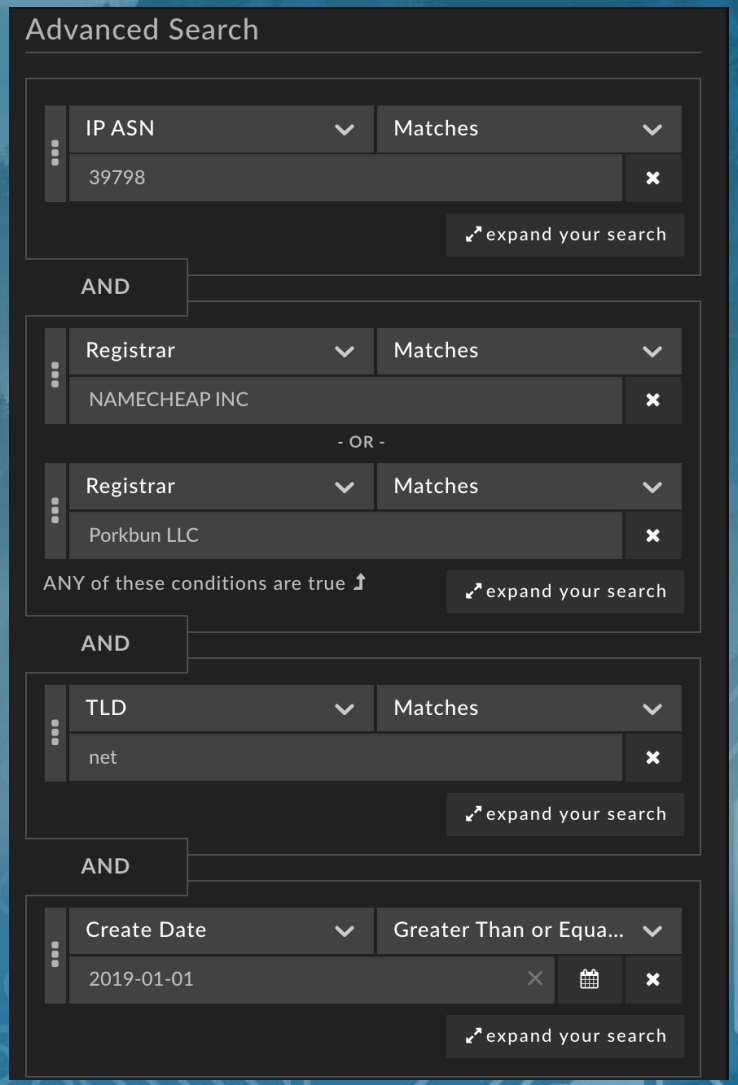
cdn.reawk.net	A	A	1	185.225.17.239	2019-11-12, 12:55	2019-12-06, 18:42

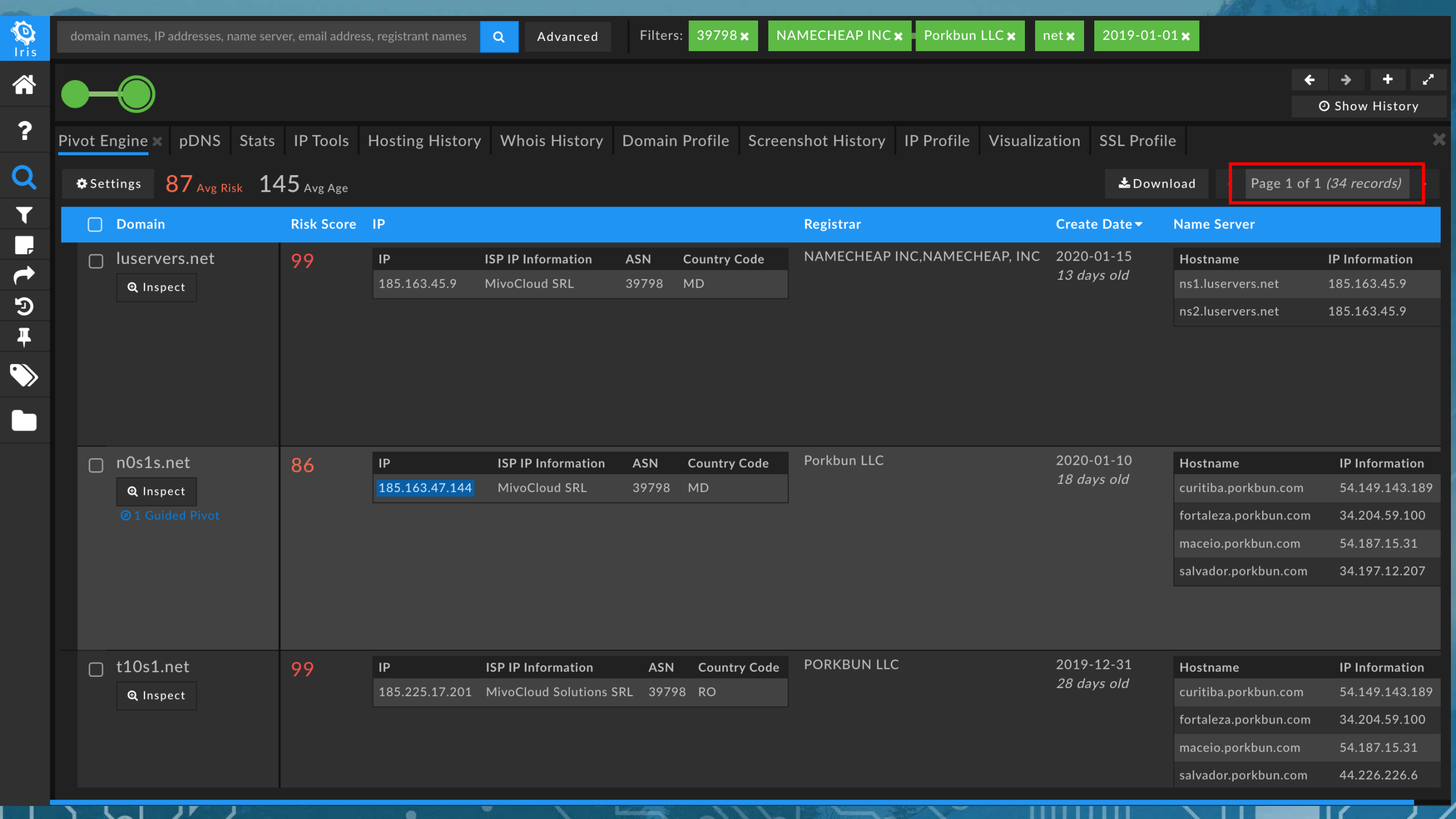
Discover and Pivot on Actor TTPs

Registrar
NAMECHEAP INC
Porkbun LLC

ISP IP Information	ASN
MivoCloud Solutions SRL	39798

TLD
net




domain names, IP addresses, name server, email address, registrant names
Advanced
Filters: 39798 NAMECHEAP INC Porkbun LLC net 2019-01-01
Show History
Pivot Engine
pDNS
Stats
IP Tools
Hosting History
Whois History
Domain Profile
Screenshot History
IP Profile
Visualization
SSL Profile
Settings
87 Avg Risk
145 Avg Age
Download
Page 1 of 1 (34 records)
Domain
Risk Score
IP
Registrar
Create Date
Name Server
luservers.net
Inspect
99
IP
ISP IP Information
ASN
Country Code
185.163.45.9
MivoCloud SRL
39798
MD
NAMECHEAP INC,NAMECHEAP, INC
2020-01-15
13 days old
Hostname
IP Information
ns1.luservers.net
185.163.45.9
ns2.luservers.net
185.163.45.9
n0s1s.net
Inspect
1 Guided Pivot
86
IP
ISP IP Information
ASN
Country Code
185.163.47.144
MivoCloud SRL
39798
MD
Porkbun LLC
2020-01-10
18 days old
Hostname
IP Information
curitiba.porkbun.com
54.149.143.189
fortaleza.porkbun.com
34.204.59.100
maceio.porkbun.com
54.187.15.31
salvador.porkbun.com
34.197.12.207
t10s1.net
Inspect
99
IP
ISP IP Information
ASN
Country Code
185.225.17.201
MivoCloud Solutions SRL
39798
RO
PORKBUN LLC
2019-12-31
28 days old
Hostname
IP Information
curitiba.porkbun.com
54.149.143.189
fortaleza.porkbun.com
34.204.59.100
maceio.porkbun.com
54.187.15.31
salvador.porkbun.com
44.226.226.6

Iris

domain names, IP addresses, name server, email address, registrant names

Advanced

Filters: 39798 NAMECHEAP INC Porkbun LLC net 2019-01-01

Show History

Filters | Notes | Export

Current Search Export

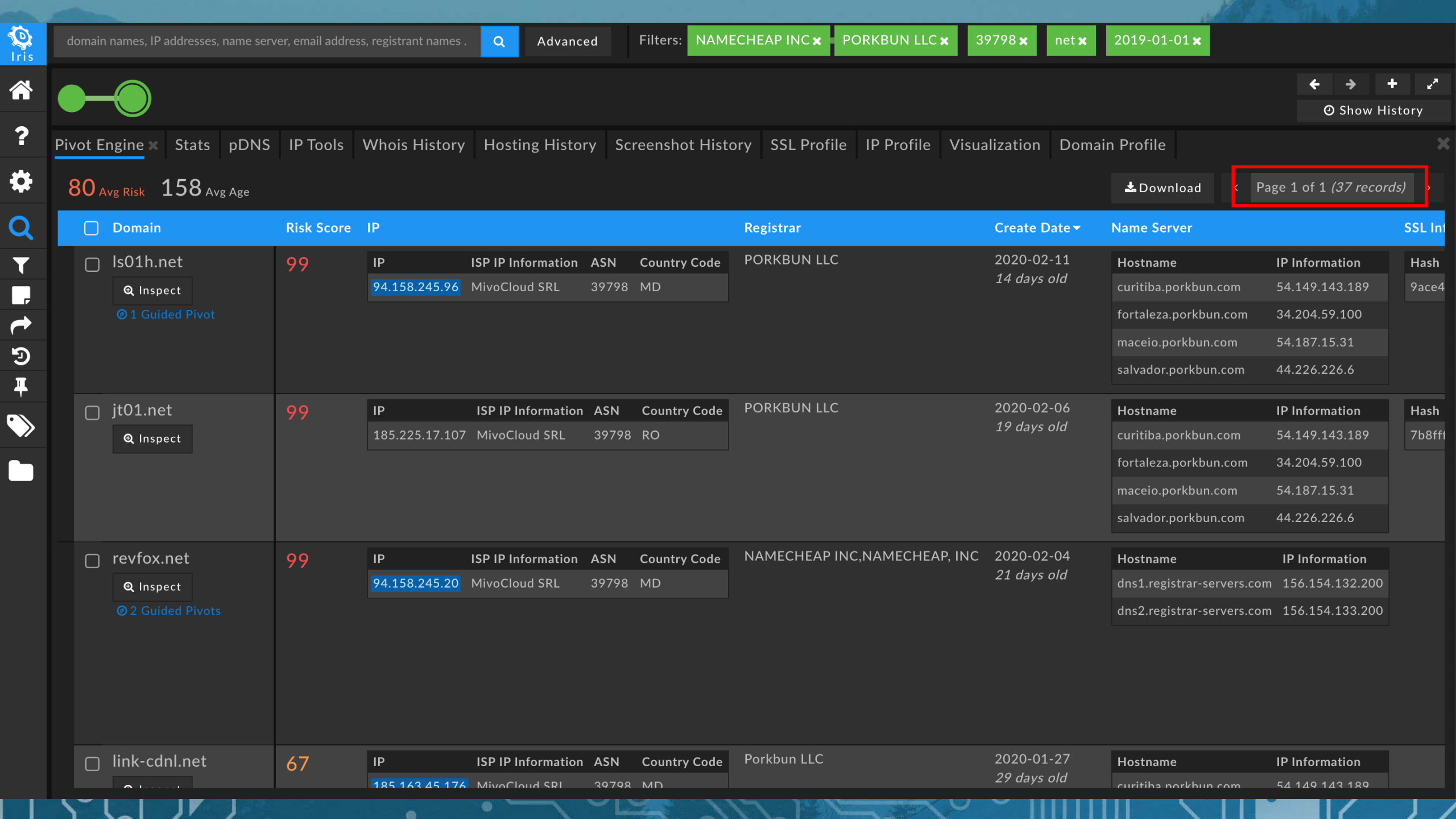
U2FsdGVkX1/RHiPkaU2eWPpWOEFm1LB+ls4eZee1Q+
/8SGbONOIoNeLMEe+9nr
/Ob6DxVW4l4+gGljUzGEm4CgXyLz02G0hWJzFoaXjXcWQa5tkeQl2s4St
3B
/vrEujCYjGl1nnFC4w1HLbisDgICsozCApOj43+kJgKZROx0PFwz48pH62
czFE9IfujJShnVnPUYKJLuyFuglZ3dUOJQf7ajgpIGFog+JefiS1KTxZCGRHh

Import a new Search

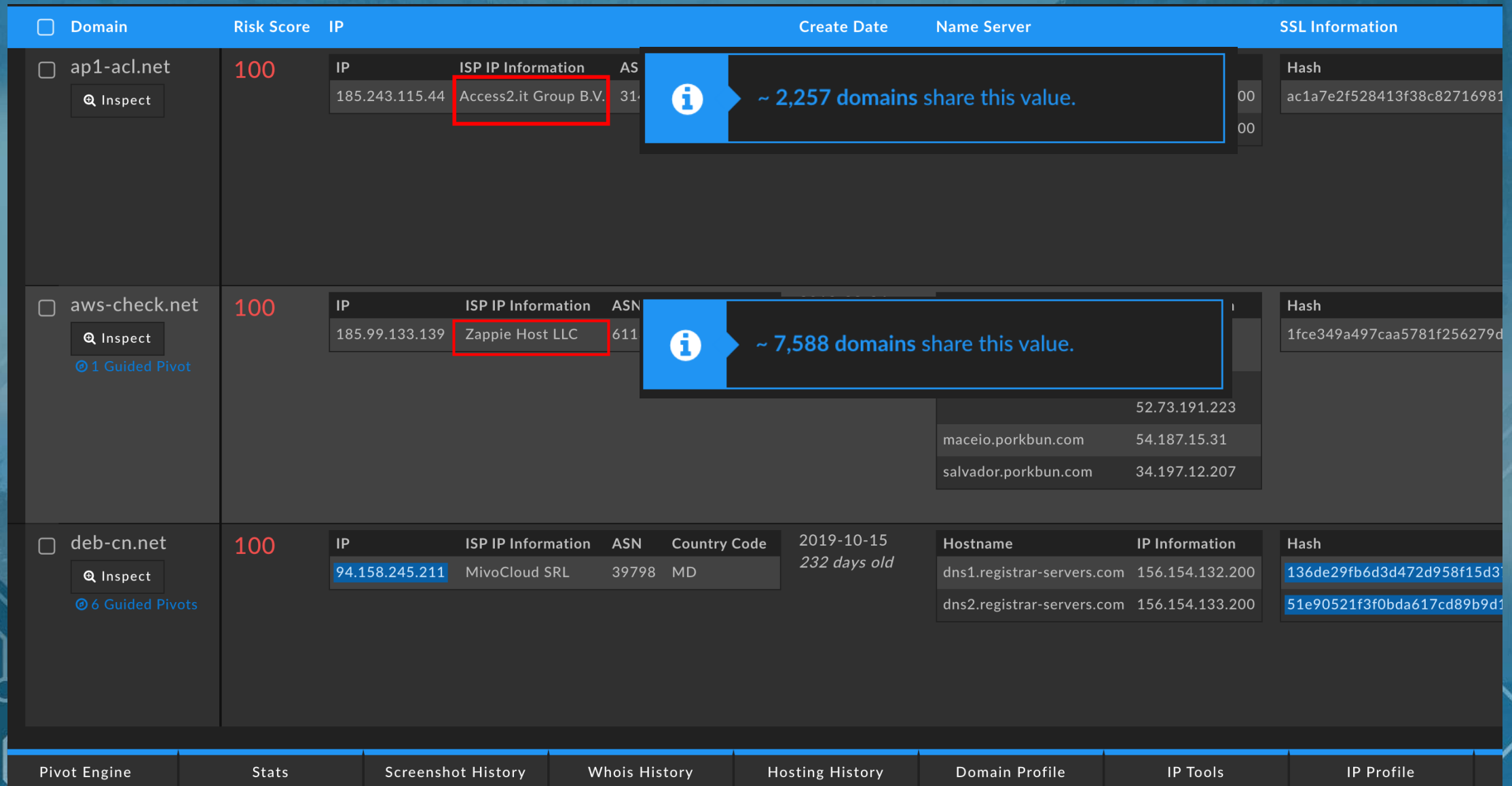
Pivot Engine | pDNS | Stats | IP Tools | Hosting History | Whois History | Domain Profile | Screenshot History

Settings 87 Avg Risk 145 Avg Age Download Page 1 of 1 *(34 records)*

Domain	Risk Score	IP	ISP IP Information	ASN	Country Code	Registrar
luservers.net Inspect	99	185.163.45.9	MivoCloud SRL	39798	MD	NAMECHEAP INC,NAMECH
n0s1s.net Inspect 1 Guided Pivot	86	185.163.47.144	MivoCloud SRL	39798	MD	Porkbun LLC
t10s1.net Inspect	99	185.225.17.201	MivoCloud Solutions SRL	39798	RO	PORKBUN LLC


domain names, IP addresses, name server, email address, registrant names .
Advanced
Filters:
NAMECHEAP INC
PORKBUN LLC
39798
net
2019-01-01
Show History
Pivot Engine
Stats
pDNS
IP Tools
Whois History
Hosting History
Screenshot History
SSL Profile
IP Profile
Visualization
Domain Profile
80 Avg Risk
158 Avg Age
Download
Page 1 of 1 (37 records)
Domain
Risk Score
IP
Registrar
Create Date
Name Server
SSL In
ls01h.net
Inspect
1 Guided Pivot
99
IP
ISP IP Information
ASN
Country Code
94.158.245.96
MivoCloud SRL
39798
MD
PORKBUN LLC
2020-02-11
14 days old
Hostname
IP Information
curitiba.porkbun.com
54.149.143.189
fortaleza.porkbun.com
34.204.59.100
maceio.porkbun.com
54.187.15.31
salvador.porkbun.com
44.226.226.6
Hash
9ace4
jt01.net
Inspect
99
185.225.17.107
MivoCloud SRL
39798
RO
PORKBUN LLC
2020-02-06
19 days old
7b8ff
revfox.net
Inspect
2 Guided Pivots
99
94.158.245.20
MivoCloud SRL
39798
MD
NAMECHEAP INC,NAMECHEAP, INC
2020-02-04
21 days old
dns1.registrar-servers.com
156.154.132.200
dns2.registrar-servers.com
156.154.133.200
link-cdnl.net
67
Porkbun LLC
2020-01-27
29 days old

Track Changes Over Time



Advanced Search

Registrar | Begins With
PORKBUN LLC

- OR -

Registrar | Begins With
NAMECHEAP

ANY of these conditions are true | expand your search

AND

ISP IP Information | Exactly Matches
Access2.it Group B.V.

- OR -

ISP IP Information | Exactly Matches
Zappie Host LLC

- OR -

ISP IP Information | Exactly Matches
MivoCloud SRL

ANY of these conditions are true | expand your search

AND

TLD | Matches
net

expand your search


SEVERAL
MONTHS
LATER...

Pivot Engine | SSL Profile | pDNS | Visualization | IP Profile | IP Tools | Domain Profile | Hosting History | Whois History | Screenshot History | Stats

73 Avg Risk 304 Avg Age

Download ‹ Page 1 of 1 *(71 records)* ›

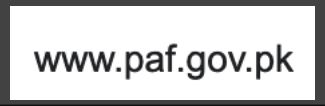
Domain	Risk Score	IP	Create Date	Name Server	SSL Information
				maceio.porkbun.com 54.187.15.31 salvador.porkbun.com 34.197.12.207	
z3st.net Inspect	99	IP: 185.99.133.138 · ISP IP Information: Zappie Host LLC · ASN: 61138 · Country Code: NZ	2020-04-29 *35 days old*	Hostname / IP Information: curitiba.porkbun.com 54.186.3.217 44.226.226.6 fortaleza.porkbun.com 3.224.31.177 52.73.191.223 maceio.porkbun.com 54.187.15.31 salvador.porkbun.com 34.197.12.207	Hash: d1be02f4dabf7b913ae7a66d0b518c7c685353bd
e-crt.net Inspect	99	IP: 185.225.19.207 · ISP IP Information: MivoCloud SRL · ASN: 39798 · Country Code: RO	2020-04-28 *36 days old*	Hostname / IP Information: curitiba.porkbun.com 54.186.3.217 44.226.226.6 fortaleza.porkbun.com 52.73.191.223 3.224.31.177 maceio.porkbun.com 54.187.15.31 salvador.porkbun.com 34.197.12.207	Hash: ab828baf964c3bbf277159afde2a9d950f3bd04d
by0ts.net Inspect 3 Guided Pivots	99	IP: 185.99.133.115 · ISP IP Information: Zappie Host LLC · ASN: 61138 · Country Code: NZ	2020-04-23 *41 days old*	Hostname / IP Information: curitiba.porkbun.com 54.186.3.217 44.226.226.6 fortaleza.porkbun.com 52.73.191.223 3.224.31.177	Hash: 3f1113183f14ee25bc65b1f546e1d2672e96febd

*. nrots.net

Note: wildcards (*) may be used for either hostname or tld.

Record Type:	Source:	Result Limit:	After Date:
A	All	500	YYYY-MM-DD

Query	Type	Source	Count	Response	First Seen	Last Seen
nrots.net	A	C	4	185.163.47.134	2020-04-06, 18:57	2020-04-16, 10:57
www.nrots.net	A	A	1	185.163.47.134	2020-04-06, 18:09	2020-06-02, 10:01
www.csd-gov.nrots.net			1	185.163.47.134	2020-03-16, 08:28	2020-03-27, 05:56
mail-paf-gov-pk.nrots.net		A	1	185.163.47.134	2020-03-16, 05:04	2020-03-16, 05:04
www.mail-paf-gov-pk.nrots.net	A	A	1	185.163.47.134	2020-03-13, 17:03	2020-03-14, 09:41
www.csd-gov-pk.nrots.net	A	A	1	185.163.47.134	2020-03-11, 08:11	2020-03-13, 14:03



Orchestrate with DNS and Infrastructure OSINT

- Speed up Incident Handling by Automating OSINT Collection
- Scale Effective Workflows with OSINT
  - Phishing Response
  - Adversary Infrastructure Discovery
  - Adversary Infrastructure Monitoring

DOMAINTOOLS®

Q/A

sales@domaintools.com