RISKIQ®

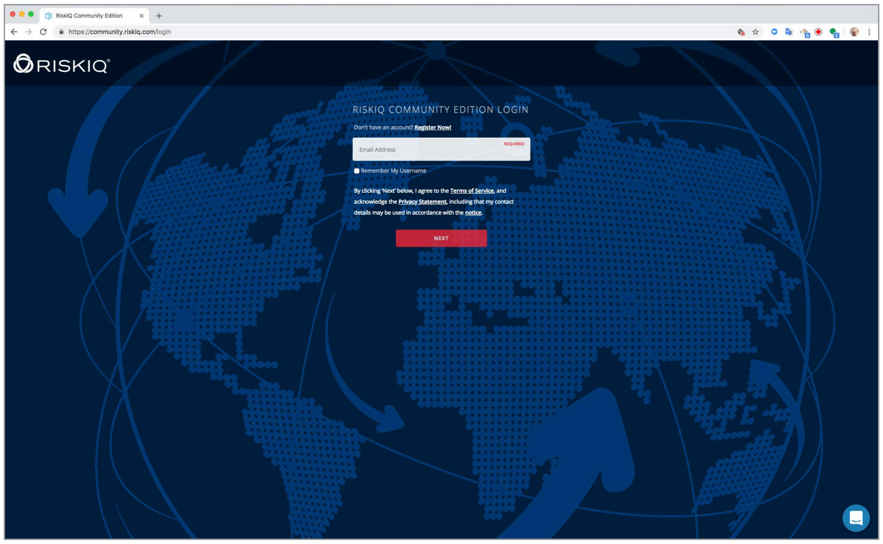
Turla Waterhole Attack Investigation

The Turla Waterhole attack was a malicious reconnaissance campaign that targeted ministry and embassy websites. All of the targeted websites were also located in Washington, D.C. This attack allowed the threat actor to track users that visited the compromised websites without their knowledge. It is believed that the threat actor was using these compromised websites to secretly track dissidents on the internet.

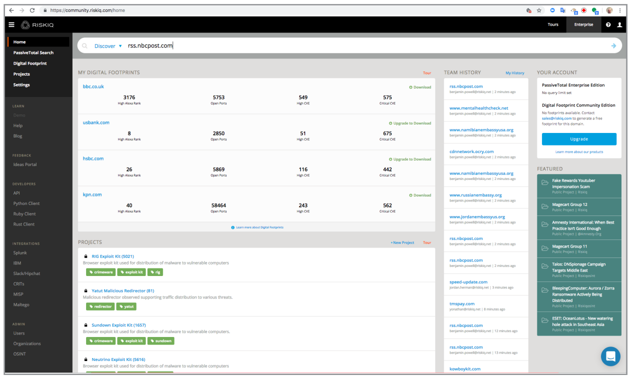
Lets Get Started

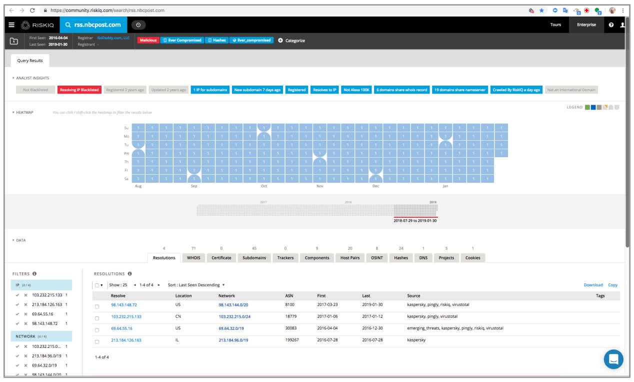
STEP 1: Log in to RiskIQ PassiveTotal™. https://community.riskiq.com/login

In this exercise, you have been given a compromised device. During your investigation, you have isolated a compromised system communicating to rss.nbcpost.com. You are tasked with investigating the domain to gain more information about the threat actor and understand what they are doing.


RiskIQ Community Edition
https://community.riskiq.com/login
RISKIQ
RISKIQ COMMUNITY EDITION LOGIN
Don't have an account? Register Now!
Email Address
REQUIRED
Remember My Username
By clicking 'Next' below, I agree to the Terms of Service, and acknowledge the Privacy Statement, including that my contact details may be used in accordance with the notice.
NEXT

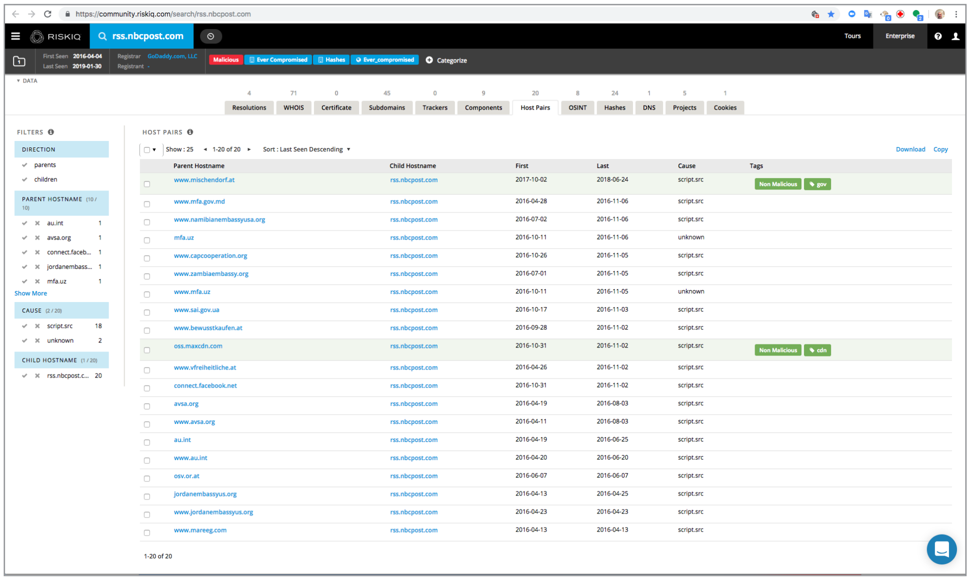
STEP 2: In the Discover window type: "rss[.]nbcpost[.]com" without the quotes or [] and hit the Enter key.





STEP 3: Investigate the Host Pair Tab

- What type of domains are listed?
- Are the domains malicious or non-malicious?
- What causes the domains to be associated with rss[.]nbcpost[.]com?
- What does it mean to be a parent domain to rss[.]nbcpost[.]com?



First Seen 2016-04-04
Last Seen 2019-01-30
Registrar GoDaddy.com, LLC
Registrant -

4	71	0	45	0	9	20	8	24	1	5	1
Resolutions	WHOIS	Certificate	Subdomains	Trackers	Components	Host Pairs	OSINT	Hashes	DNS	Projects	Cookies

DIRECTION
✓ parents
✓ children

PARENT HOSTNAME (10 / 10)

✓	✕	au.int	1
✓	✕	avsa.org	1
✓	✕	connect.faceb...	1
✓	✕	jordanembass...	1
✓	✕	mfa.uz	1

Show More

CAUSE (2 / 20)

✓	✕	script.src	18
✓	✕	unknown	2

CHILD HOSTNAME (1 / 20)

✓	✕	rss.nbcpost.c...	20

□ ▾ Show : 25 ◂ 1-20 of 20 ▸ Sort : Last Seen Descending ▾

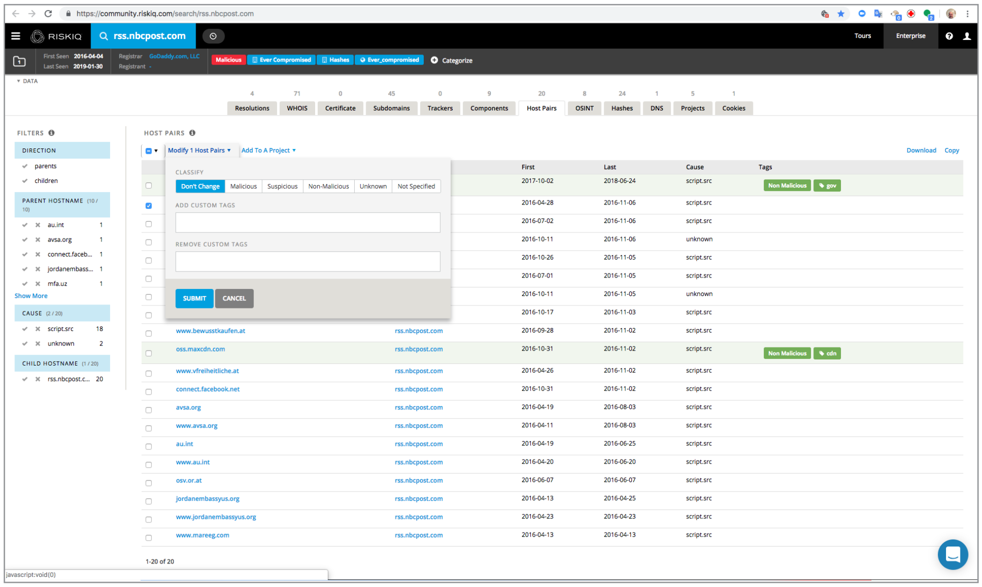
	Parent Hostname	Child Hostname	First	Last	Cause	Tags
□	www.mischendorf.at	rss.nbcpost.com	2017-10-02	2018-06-24	script.src	Non Malicious gov
□	www.mfa.gov.md	rss.nbcpost.com	2016-04-28	2016-11-06	script.src	
□	www.namibianembassyusa.org	rss.nbcpost.com	2016-07-02	2016-11-06	script.src	
□	mfa.uz	rss.nbcpost.com	2016-10-11	2016-11-06	unknown	
□	www.capcooperation.org	rss.nbcpost.com	2016-10-26	2016-11-05	script.src	
□	www.zambiaembassy.org	rss.nbcpost.com	2016-07-01	2016-11-05	script.src	
□	www.mfa.uz	rss.nbcpost.com	2016-10-11	2016-11-05	unknown	
□	www.sai.gov.ua	rss.nbcpost.com	2016-10-17	2016-11-03	script.src	
□	www.bewusstkaufen.at	rss.nbcpost.com	2016-09-28	2016-11-02	script.src	
□	oss.maxcdn.com	rss.nbcpost.com	2016-10-31	2016-11-02	script.src	Non Malicious cdn
□	www.vfreiheitliche.at	rss.nbcpost.com	2016-04-26	2016-11-02	script.src	
□	connect.facebook.net	rss.nbcpost.com	2016-10-31	2016-11-02	script.src	
□	avsa.org	rss.nbcpost.com	2016-04-19	2016-08-03	script.src	
□	www.avsa.org	rss.nbcpost.com	2016-04-11	2016-08-03	script.src	
□	au.int	rss.nbcpost.com	2016-04-19	2016-06-25	script.src	
□	www.au.int	rss.nbcpost.com	2016-04-20	2016-06-20	script.src	
□	osv.or.at	rss.nbcpost.com	2016-06-07	2016-06-07	script.src	
□	jordanembassyus.org	rss.nbcpost.com	2016-04-13	2016-04-25	script.src	
□	www.jordanembassyus.org	rss.nbcpost.com	2016-04-23	2016-04-23	script.src	
□	www.mareeg.com	rss.nbcpost.com	2016-04-13	2016-04-13	script.src	

1-20 of 20

STEP 4: As you investigate each domain click the box next to the domain name and modify the Host Pair Domain.

Classify the Host Pairs as Malicious or Non-Malicious.

You can even add a custom tag to mark the Host Pair domain like embassy, gov, commercial, social-media.



First Seen 2016-04-04
Last Seen 2019-01-30
Registrar GoDaddy.com, LLC
Registrant -

4	71	0	45	0	9	20	8	24	1	5	1
Resolutions	WHOIS	Certificate	Subdomains	Trackers	Components	Host Pairs	OSINT	Hashes	DNS	Projects	Cookies

DIRECTION
✓ parents
✓ children

PARENT HOSTNAME (10 / 10)

✓	✕	au.int	1
✓	✕	avsa.org	1
✓	✕	connect.faceb...	1
✓	✕	jordanembass...	1
✓	✕	mfa.uz	1

Show More

CAUSE (2 / 20)

✓	✕	script.src	18
✓	✕	unknown	2

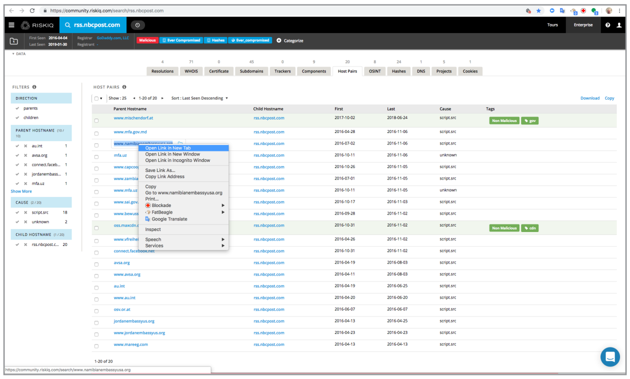
CHILD HOSTNAME (1 / 20)

✓	✕	rss.nbcpost.c...	20

	Parent Hostname	Child Hostname	First	Last	Cause	Tags
□			2017-10-02	2018-06-24	script.src	Non Malicious gov
☑			2016-04-28	2016-11-06	script.src	
□			2016-07-02	2016-11-06	script.src	
□			2016-10-11	2016-11-06	unknown	
□			2016-10-26	2016-11-05	script.src	
□			2016-07-01	2016-11-05	script.src	
□			2016-10-11	2016-11-05	unknown	
□			2016-10-17	2016-11-03	script.src	
□	www.bewusstkaufen.at	rss.nbcpost.com	2016-09-28	2016-11-02	script.src	
□	oss.maxcdn.com	rss.nbcpost.com	2016-10-31	2016-11-02	script.src	Non Malicious cdn
□	www.vfreiheitliche.at	rss.nbcpost.com	2016-04-26	2016-11-02	script.src	
□	connect.facebook.net	rss.nbcpost.com	2016-10-31	2016-11-02	script.src	
□	avsa.org	rss.nbcpost.com	2016-04-19	2016-08-03	script.src	
□	www.avsa.org	rss.nbcpost.com	2016-04-11	2016-08-03	script.src	
□	au.int	rss.nbcpost.com	2016-04-19	2016-06-25	script.src	
□	www.au.int	rss.nbcpost.com	2016-04-20	2016-06-20	script.src	
□	osv.or.at	rss.nbcpost.com	2016-06-07	2016-06-07	script.src	
□	jordanembassyus.org	rss.nbcpost.com	2016-04-13	2016-04-25	script.src	
□	www.jordanembassyus.org	rss.nbcpost.com	2016-04-23	2016-04-23	script.src	
□	www.mareeg.com	rss.nbcpost.com	2016-04-13	2016-04-13	script.src	

1-20 of 20

STEP 5: Right click on www[.]namibianembassyusa[.]org and open link in a new tab



https://community.riskiq.com/search/rss.nbcpost.com

RISKIQ rss.nbcpost.com — Tours — Enterprise

First Seen 2016-04-04 — Last Seen 2019-01-30 — Registrar GoDaddy.com, LLC — Registrant -

Malicious — Ever Compromised — Hashes — Ever_compromised — Categorize

DATA

4	71	0	45	0	9	20	8	24	1	5	1
Resolutions	WHOIS	Certificate	Subdomains	Trackers	Components	Host Pairs	OSINT	Hashes	DNS	Projects	Cookies

FILTERS

DIRECTION: ✓ parents ✓ children

PARENT HOSTNAME (10 / 10)

au.int	1
avsa.org	1
connect.faceb...	1
jordanembass...	1
mfa.uz	1

Show More

CAUSE (2 / 20)

script.src	18
unknown	2

CHILD HOSTNAME (1 / 20)

rss.nbcpost.c...	20

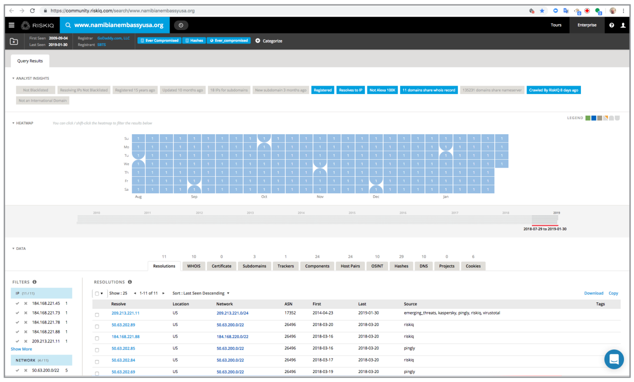
HOST PAIRS

Show : 25 — 1-20 of 20 — Sort : Last Seen Descending — Download — Copy

Parent Hostname	Child Hostname	First	Last	Cause	Tags
www.mischendorf.at	rss.nbcpost.com	2017-10-02	2018-06-24	script.src	Non Malicious, gov
www.mfa.gov.md	rss.nbcpost.com	2016-04-28	2016-11-06	script.src	
www.namibianembassyusa.org	rss.nbcpost.com	2016-07-02	2016-11-06	script.src	
mfa.uz	rss.nbcpost.com	2016-10-11	2016-11-06	unknown	
www.capcoo	rss.nbcpost.com	2016-10-26	2016-11-05	script.src	
www.zambia	rss.nbcpost.com	2016-07-01	2016-11-05	script.src	
www.mfa.uz	rss.nbcpost.com	2016-10-11	2016-11-05	unknown	
www.sai.gov.	rss.nbcpost.com	2016-10-17	2016-11-03	script.src	
www.bewuss	rss.nbcpost.com	2016-09-28	2016-11-02	script.src	
oss.maxcdn.c	rss.nbcpost.com	2016-10-31	2016-11-02	script.src	Non Malicious, cdn
www.vfreihe	rss.nbcpost.com	2016-04-26	2016-11-02	script.src	
connect.facebook.net	rss.nbcpost.com	2016-10-31	2016-11-02	script.src	
avsa.org	rss.nbcpost.com	2016-04-19	2016-08-03	script.src	
www.avsa.org	rss.nbcpost.com	2016-04-11	2016-08-03	script.src	
au.int	rss.nbcpost.com	2016-04-19	2016-06-25	script.src	
www.au.int	rss.nbcpost.com	2016-04-20	2016-06-20	script.src	
osv.or.at	rss.nbcpost.com	2016-06-07	2016-06-07	script.src	
jordanembassyus.org	rss.nbcpost.com	2016-04-13	2016-04-25	script.src	
www.jordanembassyus.org	rss.nbcpost.com	2016-04-23	2016-04-23	script.src	
www.mareeg.com	rss.nbcpost.com	2016-04-13	2016-04-13	script.src	

1-20 of 20

https://community.riskiq.com/search/www.namibianembassyusa.org



https://community.riskiq.com/search/www.namibianembassyusa.org

DATA

11	10	0	3	1	24	24	10	29	10	0	6
Resolutions	WHOIS	Certificate	Subdomains	Trackers	Components	Host Pairs	OSINT	Hashes	DNS	Projects	Cookies

FILTERS

IP (11 / 11)

184.168.221.45	1
184.168.221.73	1
184.168.221.78	1
184.168.221.88	1
209.213.221.11	1

Show More

NETWORK (4 / 11)

50.63.200.0/22	5

RESOLUTIONS

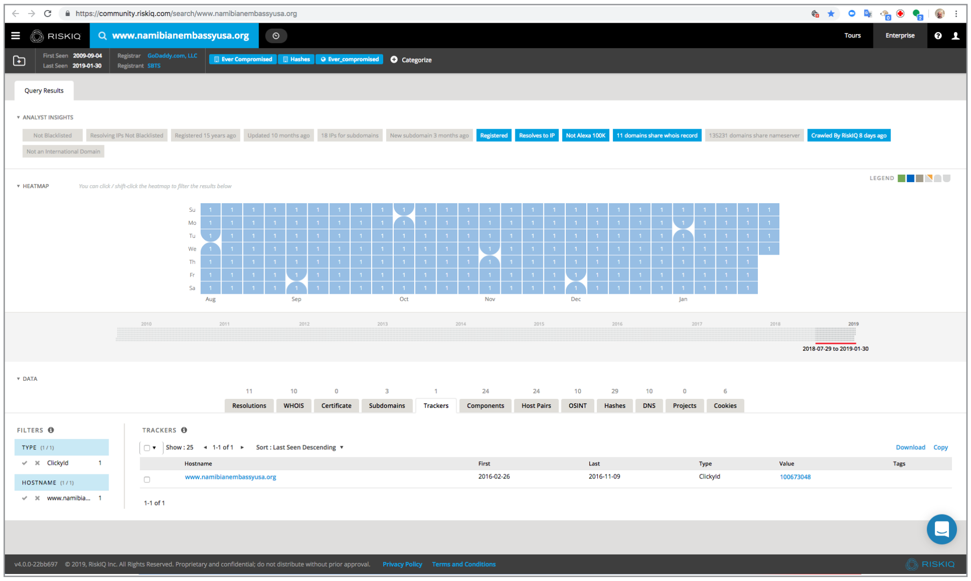
Show : 25 — 1-11 of 11 — Sort : Last Seen Descending — Download — Copy

Resolve	Location	Network	ASN	First	Last	Source	Tags
209.213.221.11	US	209.213.221.0/24	17352	2014-04-23	2019-01-30	emerging_threats, kaspersky, pingly, riskiq, virustotal	
50.63.202.89	US	50.63.200.0/22	26496	2018-03-20	2018-03-20	riskiq	
184.168.221.88	US	184.168.220.0/22	26496	2018-03-16	2018-03-20	riskiq	
50.63.202.85	US	50.63.200.0/22	26496	2018-03-16	2018-03-20	pingly	
50.63.202.84	US	50.63.200.0/22	26496	2018-03-17	2018-03-20	riskiq	
50.63.202.69	US	50.63.200.0/22	26496	2018-03-19	2018-03-20	pingly	

STEP 6: Clicking on the PassiveTotal Tab showing www[.]namibianembassyusa[.]org

Click on the Tracker tab

Investigate clickyId 10673048 by right clicking on the value and open the link in a new tab.



https://community.riskiq.com/search/www.namibianembassyusa.org

RISKIQ www.namibianembassyusa.org — Tours — Enterprise

First Seen 2009-09-04 — Last Seen 2019-01-30 — Registrar GoDaddy.com, LLC — Registrant SBTS

Ever Compromised — Hashes — Ever_compromised — Categorize

Query Results

ANALYST INSIGHTS

Not Blacklisted — Resolving IPs Not Blacklisted — Registered 15 years ago — Updated 10 months ago — 18 IPs for subdomains — New subdomain 3 months ago — Registered — Resolves to IP — Not Alexa 100K — 11 domains share whois record — 135231 domains share nameserver — Crawled By RiskIQ 8 days ago — Not an International Domain

HEATMAP — You can click / shift-click the heatmap to filter the results below — LEGEND

DATA

11	10	0	3	1	24	24	10	29	10	0	6
Resolutions	WHOIS	Certificate	Subdomains	Trackers	Components	Host Pairs	OSINT	Hashes	DNS	Projects	Cookies

FILTERS

TYPE (1 / 1)

ClickyId	1

HOSTNAME (1 / 1)

www.namibia...	1

TRACKERS

Show : 25 — 1-1 of 1 — Sort : Last Seen Descending — Download — Copy

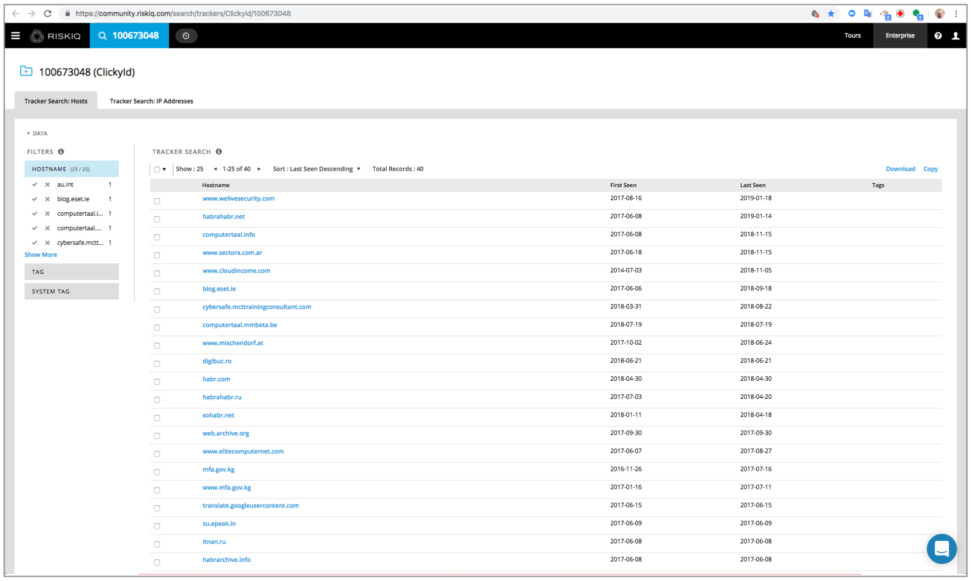
Hostname	First	Last	Type	Value	Tags
www.namibianembassyusa.org	2016-02-26	2016-11-09	ClickyId	100673048	

1-1 of 1

v4.0.0-22bb697 © 2019, RiskIQ Inc. All Rights Reserved. Proprietary and confidential; do not distribute without prior approval. Privacy Policy Terms and Conditions RISKIQ

STEP 7: Examine the Tracker search results for www[.]namibianembassyusa[.]org

Results show the relationship between the tracking id and other domains. These domains appear to be associated with governments and/or embassies.



https://community.riskiq.com/search/trackers/ClickyId/100673048

100673048 (ClickyId)

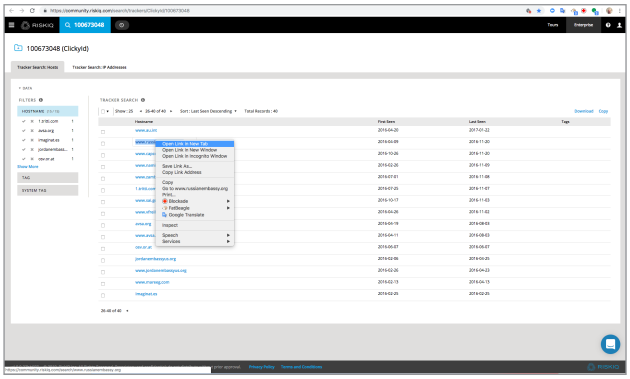
HOSTNAME (25 / 25)	
au.int	1
blog.eset.ie	1
computertaal.i...	1
computertaal....	1
cybersafe.mctt...	1

Show : 25 ◂ 1-25 of 40 ▸ Sort : Last Seen Descending ▾ Total Records : 40

Hostname	First Seen	Last Seen	Tags
www.welivesecurity.com	2017-08-16	2019-01-18	
habrahabr.net	2017-06-08	2019-01-14	
computertaal.info	2017-06-08	2018-11-15	
www.sectorx.com.ar	2017-06-18	2018-11-15	
www.cloudincome.com	2014-07-03	2018-11-05	
blog.eset.ie	2017-06-06	2018-09-18	
cybersafe.mcttrainingconsultant.com	2018-03-31	2018-08-22	
computertaal.mmbeta.be	2018-07-19	2018-07-19	
www.mischendorf.at	2017-10-02	2018-06-24	
digibuc.ro	2018-06-21	2018-06-21	
habr.com	2018-04-30	2018-04-30	
habrahabr.ru	2017-07-03	2018-04-20	
sohabr.net	2018-01-11	2018-04-18	
web.archive.org	2017-09-30	2017-09-30	
www.elitecomputernet.com	2017-06-07	2017-08-27	
mfa.gov.kg	2016-11-26	2017-07-16	
www.mfa.gov.kg	2017-01-16	2017-07-11	
translate.googleusercontent.com	2017-06-15	2017-06-15	
su.epeak.in	2017-06-09	2017-06-09	
itnan.ru	2017-06-08	2017-06-08	
habrarchive.info	2017-06-08	2017-06-08	

STEP 8: Examine the Domain www[.]russianembasy[.]org

Look to see if you find any results only last a couple of days?



https://community.riskiq.com/search/trackers/ClickyId/100673048

100673048 (ClickyId)

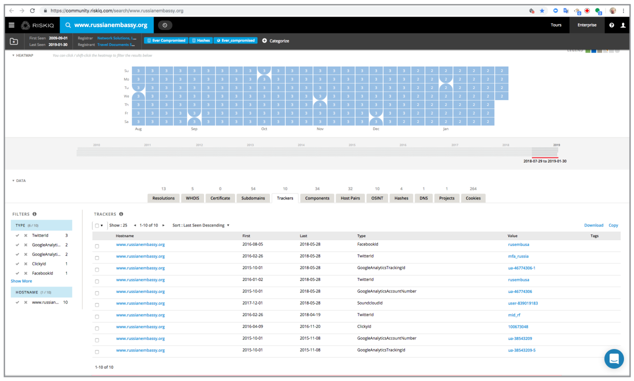
HOSTNAME (15 / 15)	
1.tritti.com	1
avsa.org	1
imaginat.es	1
jordanembass...	1
osv.or.at	1

Show : 25 ◂ 26-40 of 40 ▸ Sort : Last Seen Descending ▾ Total Records : 40

Hostname	First Seen	Last Seen	Tags
www.au.int	2016-04-20	2017-01-22	
www.russi	2016-04-09	2016-11-20	
www.capc	2016-10-26	2016-11-20	
www.nami	2016-02-26	2016-11-09	
www.zamb	2016-07-01	2016-11-08	
1.tritti.com	2016-07-25	2016-11-07	
www.sai.g	2016-10-17	2016-11-03	
www.vfrei	2016-04-26	2016-11-02	
avsa.org	2016-04-19	2016-08-03	
www.avsa.	2016-04-11	2016-08-03	
osv.or.at	2016-06-07	2016-06-07	
jordanembassyus.org	2016-02-06	2016-04-25	
www.jordanembassyus.org	2016-02-26	2016-04-23	
www.mareeg.com	2016-02-13	2016-04-13	
imaginat.es	2016-02-25	2016-02-25	

26-40 of 40 ◂

https://community.riskiq.com/search/www.russianembassy.org



https://community.riskiq.com/search/www.russianembassy.org

First Seen 2009-09-01
Last Seen 2019-01-30
Registrar Network Solutions, L...
Registrant Travel Documents S...

Resolutions	WHOIS	Certificate	Subdomains	Trackers	Components	Host Pairs	OSINT	Hashes	DNS	Projects	Cookies
13	5	0	54	10	34	32	10	4	1	1	264

TYPE (6 / 10)	
TwitterId	3
GoogleAnalyti...	2
GoogleAnalyti...	2
ClickyId	1
FacebookId	1

HOSTNAME (1 / 10)	
www.russian...	10

Show : 25 ◂ 1-10 of 10 ▸ Sort : Last Seen Descending ▾

Hostname	First	Last	Type	Value	Tags
www.russianembassy.org	2016-08-05	2018-05-28	FacebookId	rusembusa	
www.russianembassy.org	2016-02-26	2018-05-28	TwitterId	mfa_russia	
www.russianembassy.org	2015-10-01	2018-05-28	GoogleAnalyticsTrackingId	ua-46774306-1	
www.russianembassy.org	2016-01-02	2018-05-28	TwitterId	rusembusa	
www.russianembassy.org	2015-10-01	2018-05-28	GoogleAnalyticsAccountNumber	ua-46774306	
www.russianembassy.org	2017-12-01	2018-05-28	SoundcloudId	user-839019183	
www.russianembassy.org	2016-02-26	2018-04-19	TwitterId	mid_rf	
www.russianembassy.org	2016-04-09	2016-11-20	ClickyId	100673048	
www.russianembassy.org	2015-10-01	2015-11-08	GoogleAnalyticsAccountNumber	ua-38543209	
www.russianembassy.org	2015-10-01	2015-11-08	GoogleAnalyticsTrackingId	ua-38543209-5	

1-10 of 10

STEP 9: Investigate Trackers www[.]russianembasy[.]org

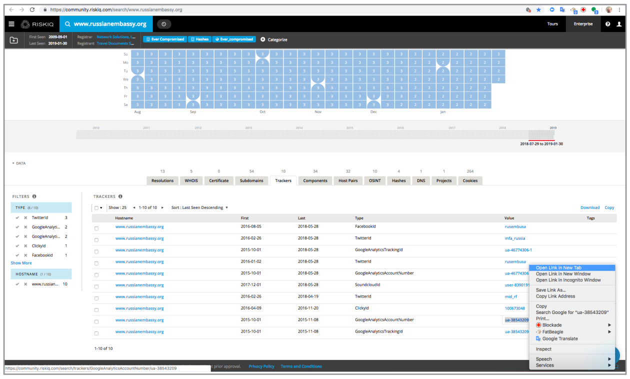
Google Analytics Account Number ua-38543209

And

Google Analytics Tracking Id ua-98543209-5

right clicking on each tracker and open the link in a new tab.

Trackers show a relationship between these trackers and



https://community.riskiq.com/search/www.russianembassy.org

DATA: 13 Resolutions, 5 WHOIS, 0 Certificate, 54 Subdomains, 10 Trackers, 34 Components, 32 Host Pairs, 10 OSINT, 4 Hashes, 1 DNS, 1 Projects, 264 Cookies

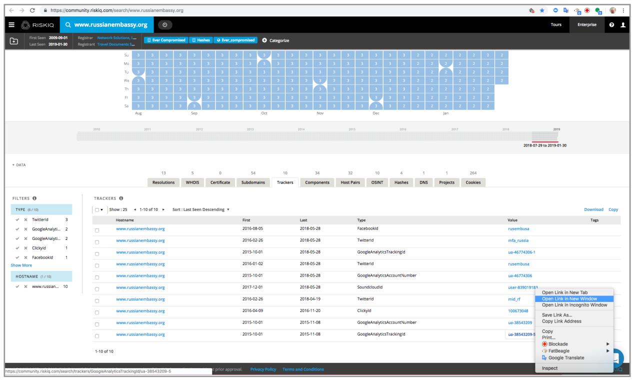
FILTERS — TYPE (6 / 10): TwitterId 3; GoogleAnalyti... 2; GoogleAnalyti... 2; ClickyId 1; FacebookId 1; Show More. HOSTNAME (1 / 10): www.russian... 10

TRACKERS — Show : 25 — 1-10 of 10 — Sort : Last Seen Descending — Download Copy

Hostname	First	Last	Type	Value	Tags
www.russianembassy.org	2016-08-05	2018-05-28	FacebookId	rusembusa	
www.russianembassy.org	2016-02-26	2018-05-28	TwitterId	mfa_russia	
www.russianembassy.org	2015-10-01	2018-05-28	GoogleAnalyticsTrackingId	ua-46774306-1	
www.russianembassy.org	2016-01-02	2018-05-28	TwitterId	rusembusa	
www.russianembassy.org	2015-10-01	2018-05-28	GoogleAnalyticsAccountNumber	ua-46774306	
www.russianembassy.org	2017-12-01	2018-05-28	SoundcloudId	user-8390191	
www.russianembassy.org	2016-02-26	2018-04-19	TwitterId	mid_rf	
www.russianembassy.org	2016-04-09	2016-11-20	ClickyId	100673048	
www.russianembassy.org	2015-10-01	2015-11-08	GoogleAnalyticsAccountNumber	ua-38543209	
www.russianembassy.org	2015-10-01	2015-11-08	GoogleAnalyticsTrackingId	ua-38543209	

1-10 of 10

https://community.riskiq.com/search/trackers/GoogleAnalyticsAccountNumber/ua-38543209



TRACKERS — Show : 25 — 1-10 of 10 — Sort : Last Seen Descending — Download Copy

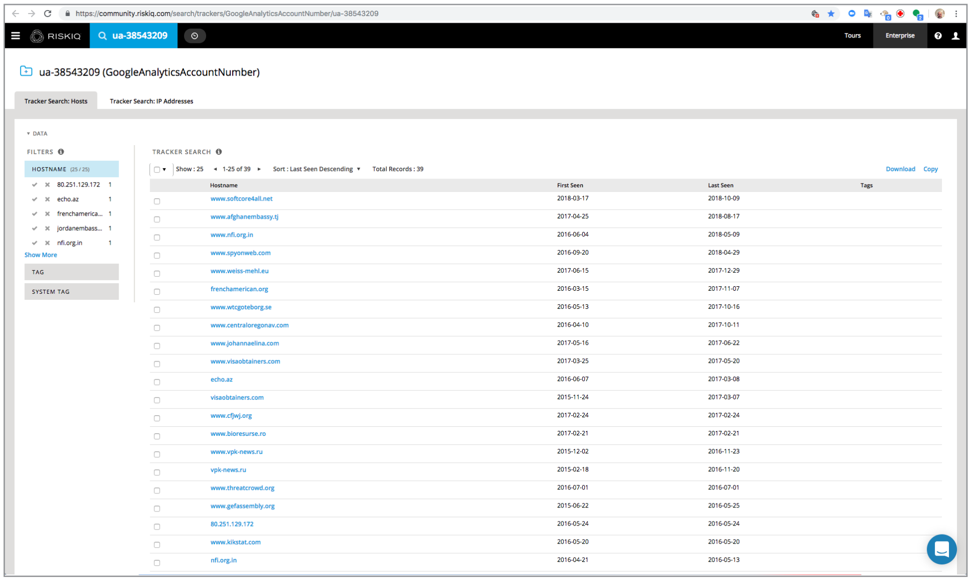
Hostname	First	Last	Type	Value	Tags
www.russianembassy.org	2016-08-05	2018-05-28	FacebookId	rusembusa	
www.russianembassy.org	2016-02-26	2018-05-28	TwitterId	mfa_russia	
www.russianembassy.org	2015-10-01	2018-05-28	GoogleAnalyticsTrackingId	ua-46774306-1	
www.russianembassy.org	2016-01-02	2018-05-28	TwitterId	rusembusa	
www.russianembassy.org	2015-10-01	2018-05-28	GoogleAnalyticsAccountNumber	ua-46774306	
www.russianembassy.org	2017-12-01	2018-05-28	SoundcloudId	user-839019183	
www.russianembassy.org	2016-02-26	2018-04-19	TwitterId	mid_rf	
www.russianembassy.org	2016-04-09	2016-11-20	ClickyId	100673048	
www.russianembassy.org	2015-10-01	2015-11-08	GoogleAnalyticsAccountNumber	ua-38543209	
www.russianembassy.org	2015-10-01	2015-11-08	GoogleAnalyticsTrackingId	ua-38543209-5	

1-10 of 10

https://community.riskiq.com/search/trackers/GoogleAnalyticsTrackingId/ua-38543209-5

STEP 10: Examine the results for Google Analytics Account Number ua-38543209

All of the websites are associated with this same tracker and are part of the threat actors campaign.



https://community.riskiq.com/search/trackers/GoogleAnalyticsAccountNumber/ua-38543209

ua-38543209 (GoogleAnalyticsAccountNumber)

Tracker Search: Hosts — Tracker Search: IP Addresses

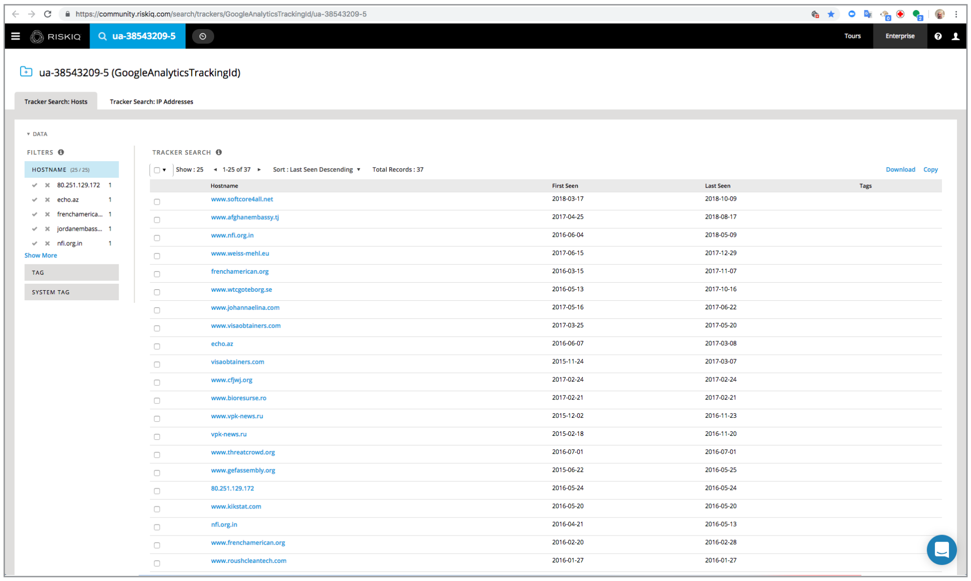
FILTERS — HOSTNAME (25 / 25): 80.251.129.172 1; echo.az 1; frenchamerica... 1; jordanembass... 1; nfi.org.in 1; Show More; TAG; SYSTEM TAG

TRACKER SEARCH — Show : 25 — 1-25 of 39 — Sort : Last Seen Descending — Total Records : 39 — Download Copy

Hostname	First Seen	Last Seen	Tags
www.softcore4all.net	2018-03-17	2018-10-09	
www.afghanembassy.tj	2017-04-25	2018-08-17	
www.nfi.org.in	2016-06-04	2018-05-09	
www.spyonweb.com	2016-09-20	2018-04-29	
www.weiss-mehl.eu	2017-06-15	2017-12-29	
frenchamerican.org	2016-03-15	2017-11-07	
www.wtcgoteborg.se	2016-05-13	2017-10-16	
www.centraloregonav.com	2016-04-10	2017-10-11	
www.johannaelina.com	2017-05-16	2017-06-22	
www.visaobtainers.com	2017-03-25	2017-05-20	
echo.az	2016-06-07	2017-03-08	
visaobtainers.com	2015-11-24	2017-03-07	
www.cfjwj.org	2017-02-24	2017-02-24	
www.bioresurse.ro	2017-02-21	2017-02-21	
www.vpk-news.ru	2015-12-02	2016-11-23	
vpk-news.ru	2015-02-18	2016-11-20	
www.threatcrowd.org	2016-07-01	2016-07-01	
www.gefassembly.org	2015-06-22	2016-05-25	
80.251.129.172	2016-05-24	2016-05-24	
www.kikstat.com	2016-05-20	2016-05-20	
nfi.org.in	2016-04-21	2016-05-13	

STEP 11: Examine the results for Google Analytics Tracking Id ua-98543209-5

All of the websites are associated with this same tracker and are part of the threat actors campaign.


https://community.riskiq.com/search/trackers/GoogleAnalyticsTrackingId/ua-38543209-5
RISKIQ
ua-38543209-5
Tours
Enterprise

ua-38543209-5 (GoogleAnalyticsTrackingId)

80.251.129.172	1
echo.az	1
frenchamerica...	1
jordanembass...	1
nfi.org.in	1

Show : 25 ◂ 1-25 of 37 ▸ Sort : Last Seen Descending ▾ Total Records : 37

Hostname	First Seen	Last Seen	Tags
www.softcore4all.net	2018-03-17	2018-10-09	
www.afghanembassy.tj	2017-04-25	2018-08-17	
www.nfi.org.in	2016-06-04	2018-05-09	
www.weiss-mehl.eu	2017-06-15	2017-12-29	
frenchamerican.org	2016-03-15	2017-11-07	
www.wtcgoteborg.se	2016-05-13	2017-10-16	
www.johannaelina.com	2017-05-16	2017-06-22	
www.visaobtainers.com	2017-03-25	2017-05-20	
echo.az	2016-06-07	2017-03-08	
visaobtainers.com	2015-11-24	2017-03-07	
www.cfjwj.org	2017-02-24	2017-02-24	
www.bioresurse.ro	2017-02-21	2017-02-21	
www.vpk-news.ru	2015-12-02	2016-11-23	
vpk-news.ru	2015-02-18	2016-11-20	
www.threatcrowd.org	2016-07-01	2016-07-01	
www.gefassembly.org	2015-06-22	2016-05-25	
80.251.129.172	2016-05-24	2016-05-24	
www.kikstat.com	2016-05-20	2016-05-20	
nfi.org.in	2016-04-21	2016-05-13	
www.frenchamerican.org	2016-02-20	2016-02-28	
www.roushcleantech.com	2016-01-27	2016-01-27	

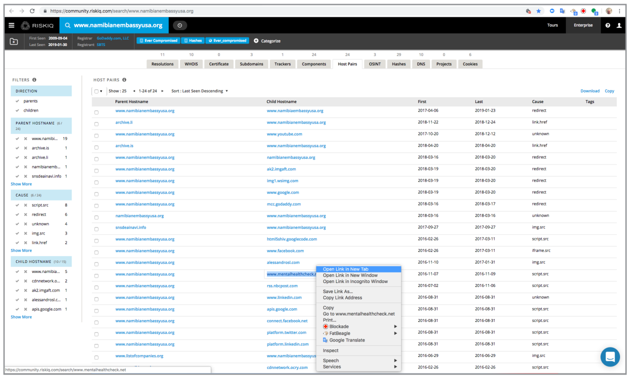
STEP 12: Go back to www[.]namibianembassyusa[.]org and Investigate the following Host Pair Domains:

www[.]mentalhealthcheck[.]net

and

cdnnetwork[.]ocry[.]com

right clicking on each domain and open the link in a new tab.


https://community.riskiq.com/search/www.namibianembassyusa.org
RISKIQ
www.namibianembassyusa.org
Tours
Enterprise
Ever Compromised
Hashes
Ever_compromised
Categorize

First Seen 2009-09-04
Last Seen 2019-01-30
Registrar GoDaddy.com, LLC
Registrant SBTS

Resolutions	WHOIS	Certificate	Subdomains	Trackers	Components	Host Pairs	OSINT	Hashes	DNS	Projects	Cookies
11	10	0	3	1	24	24	3	29	10	0	6

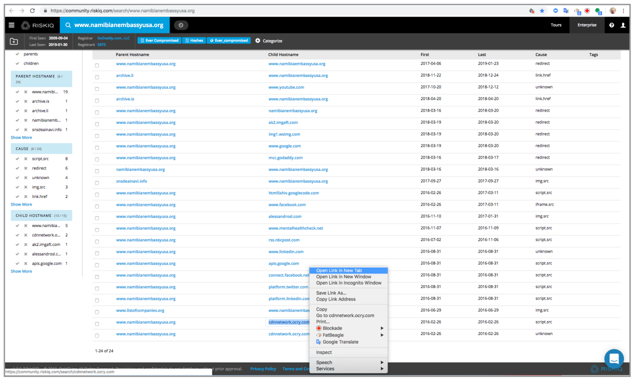
www.namibi...	19
archive.is	1
archive.li	1
namibianemb...	1
snsdeainavi.info	1

script.src	8
redirect	6
unknown	4
img.src	3
link.href	2

www.namibia...	5
cdnnetwork.o...	2
ak2.imgaft.com	1
alessandrosl.c...	1
apis.google.com	1

Show : 25 ◂ 1-24 of 24 ▸ Sort : Last Seen Descending ▾

Parent Hostname	Child Hostname	First	Last	Cause	Tags
www.namibianembassyusa.org	www.namibiaembassyusa.org	2017-04-06	2019-01-23	redirect	
archive.li	www.namibianembassyusa.org	2018-11-22	2018-12-24	link.href	
www.namibianembassyusa.org	www.youtube.com	2017-10-20	2018-12-12	unknown	
archive.is	www.namibianembassyusa.org	2018-04-20	2018-04-20	link.href	
www.namibianembassyusa.org	namibianembassyusa.org	2018-03-16	2018-03-20	redirect	
www.namibianembassyusa.org	ak2.imgaft.com	2018-03-19	2018-03-20	redirect	
www.namibianembassyusa.org	img1.wsimg.com	2018-03-19	2018-03-20	redirect	
www.namibianembassyusa.org	www.google.com	2018-03-19	2018-03-20	redirect	
www.namibianembassyusa.org	mcc.godaddy.com	2018-03-16	2018-03-17	redirect	
namibianembassyusa.org	www.namibianembassyusa.org	2018-03-16	2018-03-16	unknown	
snsdeainavi.info	www.namibianembassyusa.org	2017-09-27	2017-09-27	img.src	
www.namibianembassyusa.org	html5shiv.googlecode.com	2016-02-26	2017-03-11	script.src	
www.namibianembassyusa.org	www.facebook.com	2016-02-26	2017-03-11	iframe.src	
www.namibianembassyusa.org	alessandrosl.com	2016-11-10	2017-01-31	img.src	
www.namibianembassyusa.org	www.mentalhealthcheck.n	2016-11-07	2016-11-09	script.src	
www.namibianembassyusa.org	rss.nbcpost.com	2016-07-02	2016-11-06	script.src	
www.namibianembassyusa.org	www.linkedin.com	2016-08-31	2016-08-31	unknown	
www.namibianembassyusa.org	apis.google.com	2016-08-31	2016-08-31	script.src	
www.namibianembassyusa.org	connect.facebook.net	2016-08-31	2016-08-31	script.src	
www.namibianembassyusa.org	platform.twitter.com	2016-08-31	2016-08-31	script.src	
www.namibianembassyusa.org	platform.linkedin.com	2016-08-31	2016-08-31	script.src	
www.listofcompanies.org	www.namibianembassyus	2016-06-29	2016-06-29	img.src	
	cdnnetwork.ocry.com	2016-02-26	2016-02-26	script.src	


https://community.riskiq.com/search/www.namibianembassyusa.org
RISKIQ
www.namibianembassyusa.org
Tours
Enterprise
Ever Compromised
Hashes
Ever_compromised
Categorize

First Seen 2009-09-04
Last Seen 2019-01-30
Registrar GoDaddy.com, LLC
Registrant SBTS

www.namibi...	19
archive.is	1
archive.li	1
namibianemb...	1
snsdeainavi.info	1

script.src	8
redirect	6
unknown	4
img.src	3
link.href	2

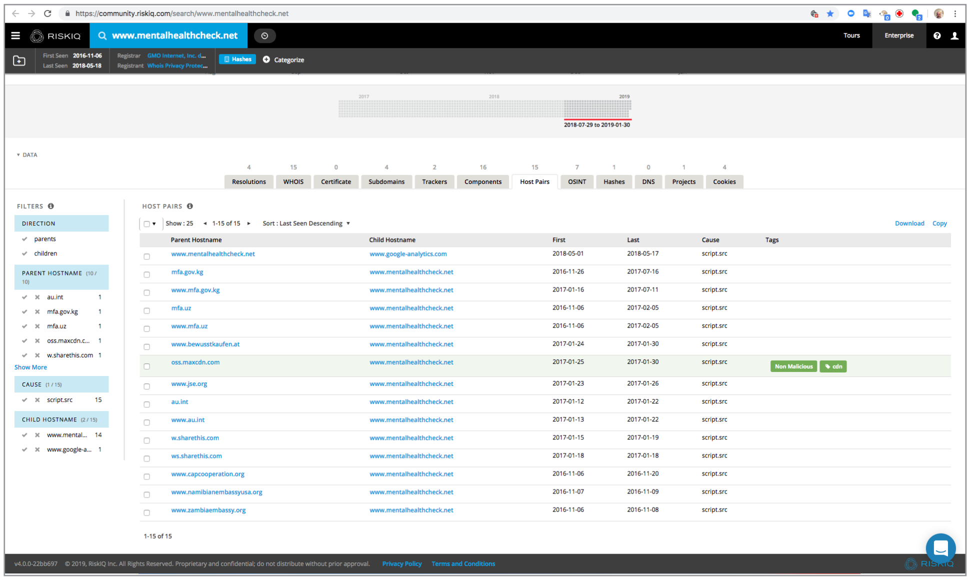
www.namibia...	5
cdnnetwork.o...	2
ak2.imgaft.com	1
alessandrosl.c...	1
apis.google.com	1

Parent Hostname	Child Hostname	First	Last	Cause	Tags
www.namibianembassyusa.org	www.namibiaembassyusa.org	2017-04-06	2019-01-23	redirect	
archive.li	www.namibianembassyusa.org	2018-11-22	2018-12-24	link.href	
www.namibianembassyusa.org	www.youtube.com	2017-10-20	2018-12-12	unknown	
archive.is	www.namibianembassyusa.org	2018-04-20	2018-04-20	link.href	
www.namibianembassyusa.org	namibianembassyusa.org	2018-03-16	2018-03-20	redirect	
www.namibianembassyusa.org	ak2.imgaft.com	2018-03-19	2018-03-20	redirect	
www.namibianembassyusa.org	img1.wsimg.com	2018-03-19	2018-03-20	redirect	
www.namibianembassyusa.org	www.google.com	2018-03-19	2018-03-20	redirect	
www.namibianembassyusa.org	mcc.godaddy.com	2018-03-16	2018-03-17	redirect	
namibianembassyusa.org	www.namibianembassyusa.org	2018-03-16	2018-03-16	unknown	
snsdeainavi.info	www.namibianembassyusa.org	2017-09-27	2017-09-27	img.src	
www.namibianembassyusa.org	html5shiv.googlecode.com	2016-02-26	2017-03-11	script.src	
www.namibianembassyusa.org	www.facebook.com	2016-02-26	2017-03-11	iframe.src	
www.namibianembassyusa.org	alessandrosl.com	2016-11-10	2017-01-31	img.src	
www.namibianembassyusa.org	www.mentalhealthcheck.net	2016-11-07	2016-11-09	script.src	
www.namibianembassyusa.org	rss.nbcpost.com	2016-07-02	2016-11-06	script.src	
www.namibianembassyusa.org	www.linkedin.com	2016-08-31	2016-08-31	unknown	
www.namibianembassyusa.org	apis.google.com	2016-08-31	2016-08-31	script.src	
www.namibianembassyusa.org	connect.facebook.net	2016-08-31	2016-08-31	script.src	
www.namibianembassyusa.org	platform.twitter.com	2016-08-31	2016-08-31	script.src	
www.namibianembassyusa.org	platform.linkedin.com	2016-08-31	2016-08-31	script.src	
www.listofcompanies.org	www.namibianembas	2016-06-29	2016-06-29	img.src	
www.namibianembassyusa.org	cdnnetwork.ocry.com	2016-02-26	2016-02-26	script.src	
www.namibianembassyusa.org	cdnnetwork.ocry.com	2016-02-26	2016-02-26	unknown	

1-24 of 24

STEP 13: Examine the Host Pairs for www[.]mentalhealthcheck[.]net

Here we see additional websites associated with attack campaign.



First Seen 2016-11-06
Last Seen 2018-05-18
Registrar GMO Internet, Inc. d...
Registrant Whois Privacy Protec...

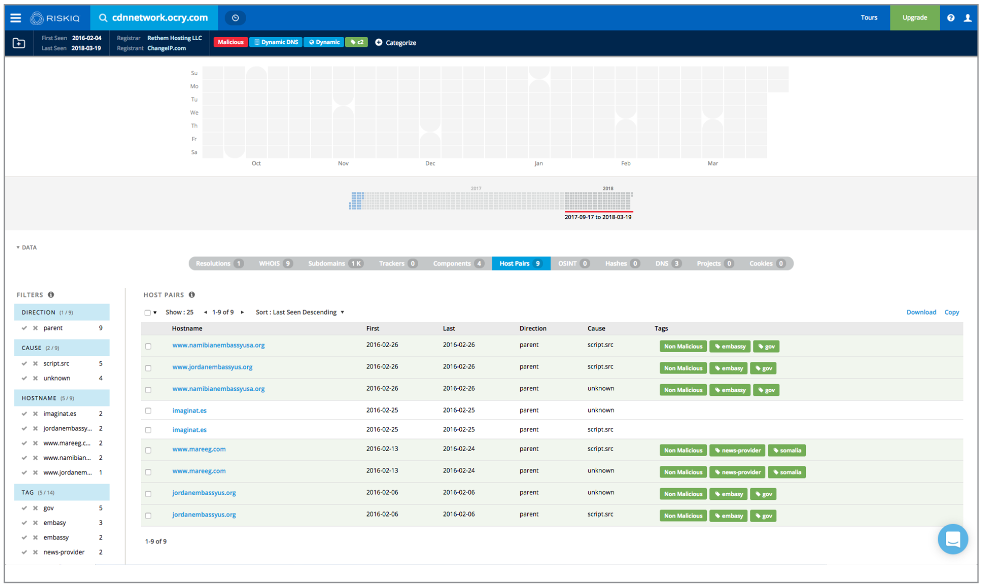
1-15 of 15

Parent Hostname	Child Hostname	First	Last	Cause	Tags
www.mentalhealthcheck.net	www.google-analytics.com	2018-05-01	2018-05-17	script.src	
mfa.gov.kg	www.mentalhealthcheck.net	2016-11-26	2017-07-16	script.src	
www.mfa.gov.kg	www.mentalhealthcheck.net	2017-01-16	2017-07-11	script.src	
mfa.uz	www.mentalhealthcheck.net	2016-11-06	2017-02-05	script.src	
www.mfa.uz	www.mentalhealthcheck.net	2016-11-06	2017-02-05	script.src	
www.bewusstkaufen.at	www.mentalhealthcheck.net	2017-01-24	2017-01-30	script.src	
oss.maxcdn.com	www.mentalhealthcheck.net	2017-01-25	2017-01-30	script.src	Non Malicious cdn
www.jse.org	www.mentalhealthcheck.net	2017-01-23	2017-01-26	script.src	
au.int	www.mentalhealthcheck.net	2017-01-12	2017-01-22	script.src	
www.au.int	www.mentalhealthcheck.net	2017-01-13	2017-01-22	script.src	
w.sharethis.com	www.mentalhealthcheck.net	2017-01-15	2017-01-19	script.src	
ws.sharethis.com	www.mentalhealthcheck.net	2017-01-18	2017-01-18	script.src	
www.capcooperation.org	www.mentalhealthcheck.net	2016-11-06	2016-11-20	script.src	
www.namibianembassyusa.org	www.mentalhealthcheck.net	2016-11-07	2016-11-09	script.src	
www.zambiaembassy.org	www.mentalhealthcheck.net	2016-11-06	2016-11-08	script.src	

1-15 of 15

STEP 14: Examine the Host Pairs for cdnnetwork[.]ocry[.]com

Here we see associations connecting to the Jordan Embassy.



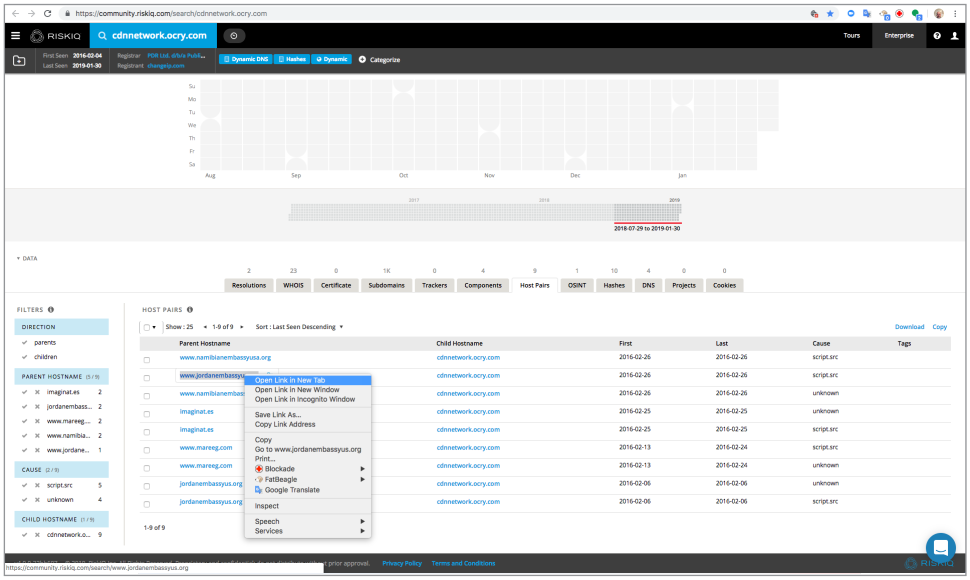
First Seen 2016-02-04
Last Seen 2018-03-19
Registrar Rethem Hosting LLC
Registrant ChangeIP.com

1-9 of 9

Hostname	First	Last	Direction	Cause	Tags
www.namibianembassyusa.org	2016-02-26	2016-02-26	parent	script.src	Non Malicious embassy gov
www.jordanembassyus.org	2016-02-26	2016-02-26	parent	script.src	Non Malicious embasy gov
www.namibianembassyusa.org	2016-02-26	2016-02-26	parent	unknown	Non Malicious embassy gov
imaginat.es	2016-02-25	2016-02-25	parent	unknown	
imaginat.es	2016-02-25	2016-02-25	parent	script.src	
www.mareeg.com	2016-02-13	2016-02-24	parent	script.src	Non Malicious news-provider somalia
www.mareeg.com	2016-02-13	2016-02-24	parent	unknown	Non Malicious news-provider somalia
jordanembassyus.org	2016-02-06	2016-02-06	parent	unknown	Non Malicious embasy gov
jordanembassyus.org	2016-02-06	2016-02-06	parent	script.src	Non Malicious embasy gov

1-9 of 9

STEP 15: Right click on jordanembassyus[.]org that has a Cause from script.src and open link in a new tab



2	23	0	1K	0	4	9	1	10	4	0	0
Resolutions	WHOIS	Certificate	Subdomains	Trackers	Components	Host Pairs	OSINT	Hashes	DNS	Projects	Cookies

HOST PAIRS

Show : 25 1-9 of 9 Sort : Last Seen Descending Download Copy

Parent Hostname	Child Hostname	First	Last	Cause	Tags
www.namibianembassyusa.org	cdnnetwork.ocry.com	2016-02-26	2016-02-26	script.src	
www.jordanembassyu	cdnnetwork.ocry.com	2016-02-26	2016-02-26	script.src	
www.namibianembas	cdnnetwork.ocry.com	2016-02-26	2016-02-26	unknown	
imaginat.es	cdnnetwork.ocry.com	2016-02-25	2016-02-25	unknown	
imaginat.es	cdnnetwork.ocry.com	2016-02-25	2016-02-25	script.src	
www.mareeg.com	cdnnetwork.ocry.com	2016-02-13	2016-02-24	script.src	
www.mareeg.com	cdnnetwork.ocry.com	2016-02-13	2016-02-24	unknown	
jordanembassyus.org	cdnnetwork.ocry.com	2016-02-06	2016-02-06	unknown	
jordanembassyus.org	cdnnetwork.ocry.com	2016-02-06	2016-02-06	script.src	

1-9 of 9

FILTERS

DIRECTION	
parents	
children	
PARENT HOSTNAME (5 / 9)	
imaginat.es	2
jordanembass...	2
www.mareeg....	2
www.namibia...	2
www.jordane...	1
CAUSE (2 / 9)	
script.src	5
unknown	4
CHILD HOSTNAME (1 / 9)	
cdnnetwork.o...	9

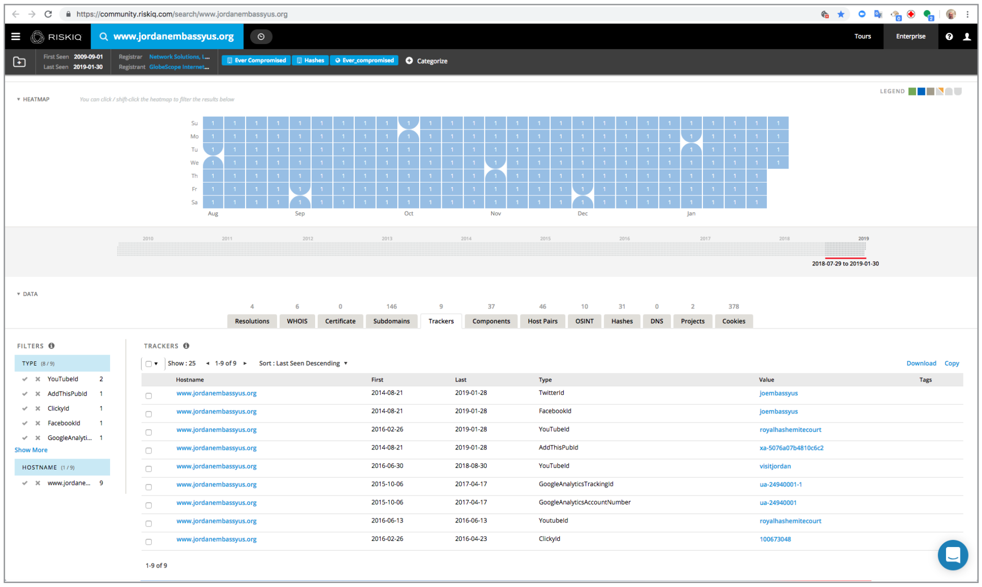
STEP 16: Examine Trackers for jordanembassyus[.]org

Investigate Google Analytics Account Number ua-24940001

And

Google Analytics Tracking Id ua-24940001-1

right clicking on each tracker and open the link in a new tab.



4	6	0	146	9	37	46	10	31	0	2	378
Resolutions	WHOIS	Certificate	Subdomains	Trackers	Components	Host Pairs	OSINT	Hashes	DNS	Projects	Cookies

TRACKERS

Show : 25 1-9 of 9 Sort : Last Seen Descending Download Copy

Hostname	First	Last	Type	Value	Tags
www.jordanembassyus.org	2014-08-21	2019-01-28	TwitterId	joembassyus	
www.jordanembassyus.org	2014-08-21	2019-01-28	FacebookId	joembassyus	
www.jordanembassyus.org	2016-02-26	2019-01-28	YouTubeId	royalhashemitecourt	
www.jordanembassyus.org	2014-08-21	2019-01-28	AddThisPubId	xa-5076a07b4810c6c2	
www.jordanembassyus.org	2016-06-30	2018-08-30	YouTubeId	visitjordan	
www.jordanembassyus.org	2015-10-06	2017-04-17	GoogleAnalyticsTrackingId	ua-24940001-1	
www.jordanembassyus.org	2015-10-06	2017-04-17	GoogleAnalyticsAccountNumber	ua-24940001	
www.jordanembassyus.org	2016-06-13	2016-06-13	Youtubeld	royalhashemitecourt	
www.jordanembassyus.org	2016-02-26	2016-04-23	ClickyId	100673048	

1-9 of 9

FILTERS

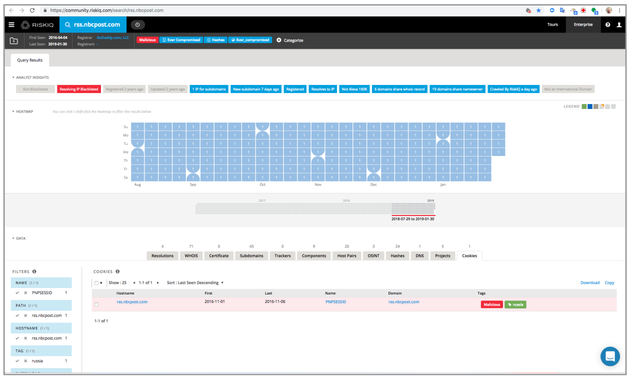
TYPE (8 / 9)	
YouTubeId	2
AddThisPubId	1
ClickyId	1
FacebookId	1
GoogleAnalyti...	1
Show More	
HOSTNAME (1 / 9)	
www.jordane...	9

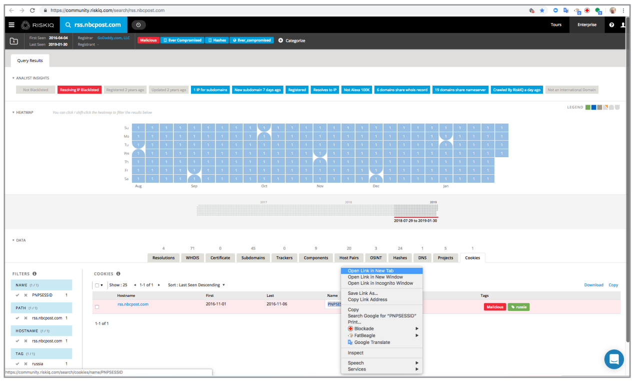
STEP 17: Go back to the tab for rss[.]nbcpost[.]com

Click on the cookie tab

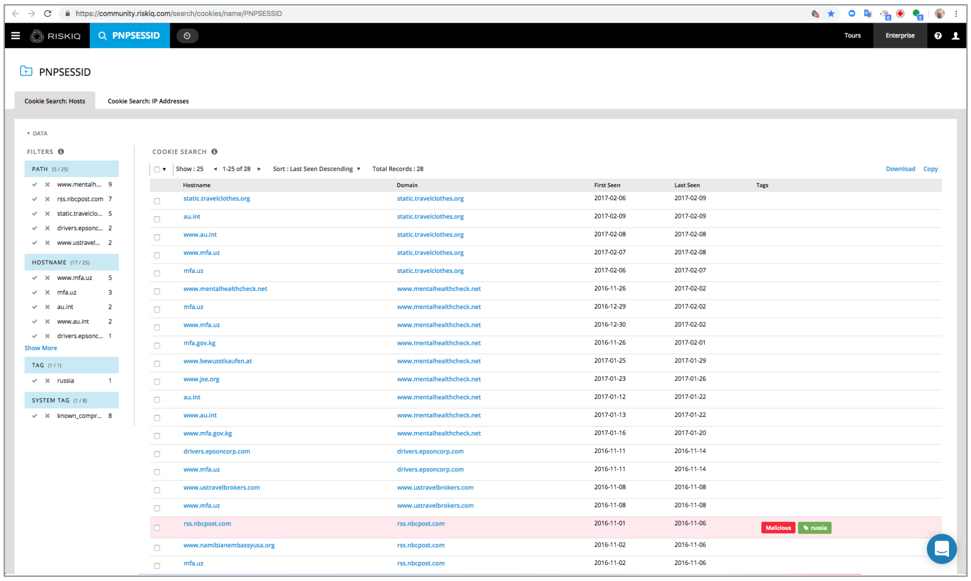
Investigate cookie named PNPSESSID

right clicking on the cookie name and open the link in a new tab.





STEP 18: This cookie was used to track users on all of the websites listed.



PNPSESSID

Cookie Search: Hosts | Cookie Search: IP Addresses

DATA

FILTERS

PATH (5 / 25)	
www.mentalh...	9
rss.nbcpost.com	7
static.travelclo...	5
drivers.epsonc...	2
www.ustravel...	2

HOSTNAME (17 / 25)	
www.mfa.uz	5
mfa.uz	3
au.int	2
www.au.int	2
drivers.epsonc...	1

Show More

TAG (1 / 1)	
russia	1

SYSTEM TAG (1 / 8)	
known_compr...	8

COOKIE SEARCH

Show : 25 ◂ 1-25 of 28 ▸ Sort : Last Seen Descending ▾ Total Records : 28 Download Copy

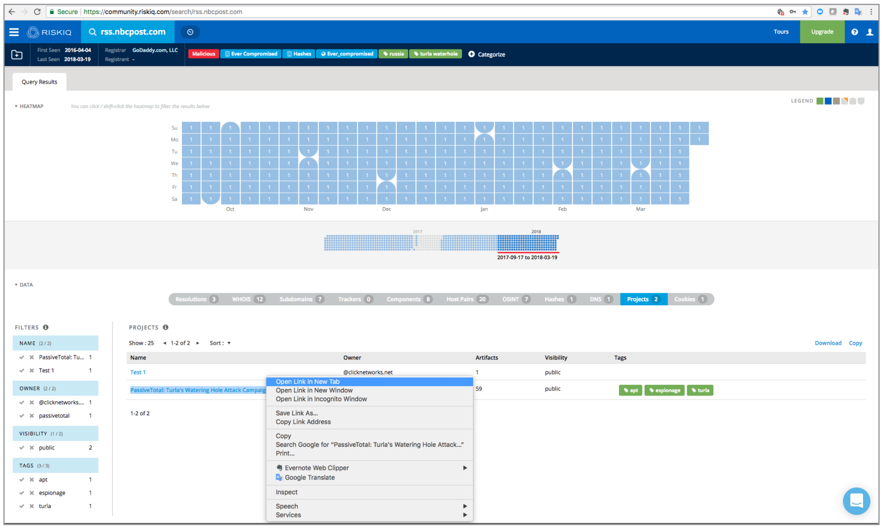
Hostname	Domain	First Seen	Last Seen	Tags
static.travelclothes.org	static.travelclothes.org	2017-02-06	2017-02-09	
au.int	static.travelclothes.org	2017-02-09	2017-02-09	
www.au.int	static.travelclothes.org	2017-02-08	2017-02-08	
www.mfa.uz	static.travelclothes.org	2017-02-07	2017-02-08	
mfa.uz	static.travelclothes.org	2017-02-06	2017-02-07	
www.mentalhealthcheck.net	www.mentalhealthcheck.net	2016-11-26	2017-02-02	
mfa.uz	www.mentalhealthcheck.net	2016-12-29	2017-02-02	
www.mfa.uz	www.mentalhealthcheck.net	2016-12-30	2017-02-02	
mfa.gov.kg	www.mentalhealthcheck.net	2016-11-26	2017-02-01	
www.bewusstkaufen.at	www.mentalhealthcheck.net	2017-01-25	2017-01-29	
www.jse.org	www.mentalhealthcheck.net	2017-01-23	2017-01-26	
au.int	www.mentalhealthcheck.net	2017-01-12	2017-01-22	
www.au.int	www.mentalhealthcheck.net	2017-01-13	2017-01-22	
www.mfa.gov.kg	www.mentalhealthcheck.net	2017-01-16	2017-01-20	
drivers.epsoncorp.com	drivers.epsoncorp.com	2016-11-11	2016-11-14	
www.mfa.uz	drivers.epsoncorp.com	2016-11-11	2016-11-14	
www.ustravelbrokers.com	www.ustravelbrokers.com	2016-11-08	2016-11-08	
www.mfa.uz	www.ustravelbrokers.com	2016-11-08	2016-11-08	
rss.nbcpost.com	rss.nbcpost.com	2016-11-01	2016-11-06	Malicious russia
www.namibianembassyusa.org	rss.nbcpost.com	2016-11-02	2016-11-06	
mfa.uz	rss.nbcpost.com	2016-11-02	2016-11-06	

STEP 19:

Go back to the tab for rss[.]nbcpost[.]com

Review the project tab.

Click on the project named “PassiveTotal: Turla’s Watering Hole Attack Campaign”



First Seen 2016-04-04
Last Seen 2018-03-19
Registrar GoDaddy.com, LLC
Registrant -

2017-09-17 to 2018-03-19

FILTERS

NAME (2 / 2)	
PassiveTotal: Tu...	1
Test 1	1
OWNER (2 / 2)	
@clicknetworks....	1
passivetotal	1
VISIBILITY (1 / 2)	
public	2
TAGS (3 / 3)	
apt	1
espionage	1
turla	1

PROJECTS

Show : 25 ◂ 1-2 of 2 ▸ Sort : ▾

Name	Owner	Artifacts	Visibility	Tags
Test 1	@clicknetworks.net	1	public	
PassiveTotal: Turla's Watering Hole Attack Campaig		59	public	apt espionage turla

1-2 of 2

STEP 20:

PassiveTotal: Turla’s Watering Hole Attack Campaign

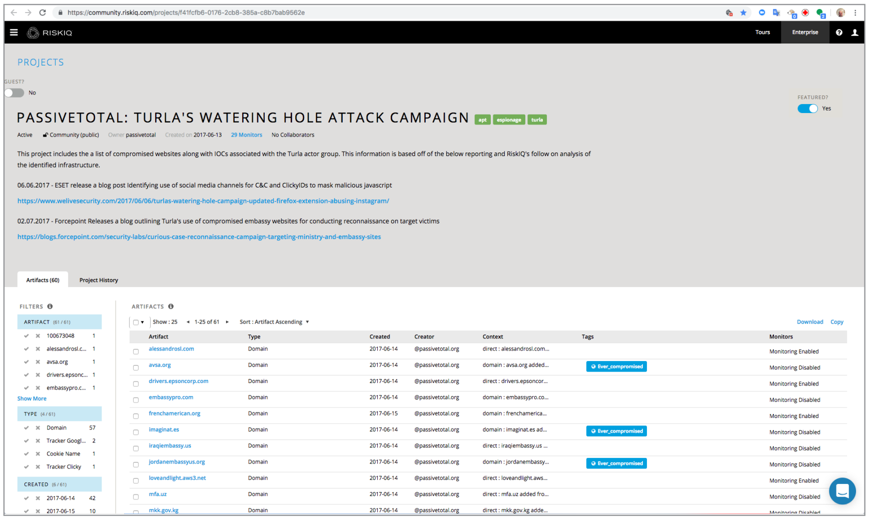
This project includes the list of compromised websites along with IOCs associated with the Turla actor group. This information is based off of the below reporting and RiskIQ’s follow on analysis of the identified infrastructure.

06.06.2017 - ESET release a blog post Identifying use of social media channels for C&C and ClickyIDs to mask malicious javascript

https://www.welivesecurity.com/2017/06/06/turlas-watering-hole-campaign-updated-firefox-extension-abusing-instagram/

02.07.2017 - Forcepoint Releases a blog outlining Turla’s use of compromised embassy websites for conducting reconnaissance on target victims

https://blogs.forcepoint.com/security-labs/curious-case-reconnaissance-campaign-targeting-ministry-and-embassy-sites



PASSIVETOTAL: TURLA'S WATERING HOLE ATTACK CAMPAIGN apt espionage turla

Active Community (public) Owner passivetotal Created on 2017-06-13 29 Monitors No Collaborators

This project includes the a list of compromised websites along with IOCs associated with the Turla actor group. This information is based off of the below reporting and RiskIQ's follow on analysis of the identified infrastructure.

06.06.2017 - ESET release a blog post Identifying use of social media channels for C&C and ClickyIDs to mask malicious javascript

https://www.welivesecurity.com/2017/06/06/turlas-watering-hole-campaign-updated-firefox-extension-abusing-instagram/

02.07.2017 - Forcepoint Releases a blog outlining Turla's use of compromised embassy websites for conducting reconnaissance on target victims

https://blogs.forcepoint.com/security-labs/curious-case-reconnaissance-campaign-targeting-ministry-and-embassy-sites

FILTERS

ARTIFACT (61 / 61)	
100673048	1
alessandrosl.c...	1
avsa.org	1
drivers.epsonc...	1
embassypro.c...	1
TYPE (4 / 61)	
Domain	57
Tracker Googl...	2
Cookie Name	1
Tracker Clicky	1
CREATED (6 / 61)	
2017-06-14	42
2017-06-15	10

ARTIFACTS

□ ▾ Show : 25 ◂ 1-25 of 61 ▸ Sort : Artifact Ascending ▾

	Artifact	Type	Created	Creator	Context	Tags	Monitors
□	alessandrosl.com	Domain	2017-06-14	@passivetotal.org	direct : alessandrosl.com...		Monitoring Enabled
□	avsa.org	Domain	2017-06-14	@passivetotal.org	domain : avsa.org added...	Ever_compromised	Monitoring Disabled
□	drivers.epsoncorp.com	Domain	2017-06-14	@passivetotal.org	direct : drivers.epsoncor...		Monitoring Enabled
□	embassypro.com	Domain	2017-06-14	@passivetotal.org	domain : embassypro.co...		Monitoring Disabled
□	frenchamerican.org	Domain	2017-06-15	@passivetotal.org	domain : frenchamerica...		Monitoring Enabled
□	imaginat.es	Domain	2017-06-14	@passivetotal.org	domain : imaginat.es ad...	Ever_compromised	Monitoring Disabled
□	iraqiembassy.us	Domain	2017-06-14	@passivetotal.org	direct : iraqiembassy.us ...		Monitoring Disabled
□	jordanembassyus.org	Domain	2017-06-14	@passivetotal.org	domain : jordanembassy...	Ever_compromised	Monitoring Disabled
□	loveandlight.aws3.net	Domain	2017-06-14	@passivetotal.org	direct : loveandlight.aws...		Monitoring Enabled
□	mfa.uz	Domain	2017-06-14	@passivetotal.org	direct : mfa.uz added fro...		Monitoring Disabled
□	mkk.gov.kg	Domain	2017-06-14	@passivetotal.org	direct : mkk.gov.kg adde...		Monitoring Disabled

Conclusion

This attack was a reconnaissance campaign that actively targeted visitors to government websites. The tactics and the targeting of this campaign overlaps with those of the Turla group. However, no conclusive evidence is available to confirm a relationship or the motive behind this campaign.

This use case was the reason why RiskIQ released this new ***Cookies*** data set that was created from crawl data. This new data set helped to uncover how the threat actor operated and tracked users identifying the compromised websites.

RiskIQ, Inc.
22 Battery Street, 10th Floor
San Francisco, CA. 94111

✉ sales@riskiq.net
☎ 1 888.415.4447

Learn more at riskiq.com