

Domain Investigation Exercise

antivirus.safetynote.xyz

Welcome to this exercise that explores how you can use PassiveTotal® to investigate a suspicious domain.

In this exercise, you have been given a domain from your firewall logs to investigate. You are tasked with investigating the domain to determine if it is malicious or associated with malicious domains.

Lets Get Started

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

← → C a Secure https://www.passivetotal.org/home	♣ ♥ Q ☆ :
	RISKIQ
	RISKIQ COMMUNITY EDITION LOGIN Dom have an account it register how Email Address It Country It Coun
	Password REQUIRED SHOW PASSWORD
	Forgot password? By logging in, you agree with our <u>Terms of Service</u> 8 <u>Privary Policy</u> ,

STEP 2:

- In the Discover window type: "antivirus.safetynote.xyz" without the quotes and hit the Enter key.
 - Can you determine if the domain still active?
- When was the last time the domain was active?

C Decover + antivirus.safet	meteogr			
Berjamin Powell				
P001943435.00	Fair fungetion	HATUNG	Radio Property	
PROJECTS (IN	New Project Inc. Projects	Public Project Philating Comains Overant registered in the unit in philating activities		
6	6	Analysis and constancy A harpen for relations arg		Start searching to
		Public Propert Known Positive APO (Ps		populate your history
	jects to monitor track a threat group	Public Project Public Alto National Interdini Tallice Alto National Inter day Institution advance descende in Path Alto Nationale	ward bing and larger.	
	eocra an Astfactra adol i ta a propet jectrism a projecta detal screen	Rubb, Singer: Chican Lab, PackBAT Jaid Hamme wated to PachBAT	dag and danhering.	
		Public Propert Refs (Explain CC Browner explicit to used for distribution of matures to solverable computers		
		Public Propert Citizen Latt, NSD Group Induces Fren Viga Instantial org/ITV/Binithen datar dastern phone and	the respiration	
		Public Project Surdown Dightit KX Broken capter Kr. and for declaration of nations is subwalds computers.		
		Rubic Project Damoon Walkane Trais & Fana Adminy: Majuritechangu alana Amdoud soni alketiandigaar M	dag Atala Pasa.	
		Prest for	n dhe Owen: Cookle Data Set in Riskt? PassiveTota	
Kow to Search wereduction to		and the second se	taria set in MobQ ParaberTatal is Teach from the over, When new, we think of web crowing, browser associate and most whithen the Overs Casilia Data Set in MobD2 ParaberTata	n most people hear the word cookies, they imagine fresh-baland confliction importantly, data's lifter senseral weeks of testing, we are finally happy to re al sciences first on Risk12.
+ Video : The New			Ref Citra	

		O recessor									Consumity billion Tax's May Consul
Latter Steel	Inginese MARCH			and David State	and [New	Theoheems 0 c	Canagorites				
Question Assess											
· HERRICH Proceeding											115150
			-								
				-		76	Var	AP	Nig	Jan.	
								2017			
								PA Galeria 2017-36-08			
	HIGGIN	015 0		- Contraction				NOTES (2) 100 (2) 100			
		045 0 N-15 1-5478 + - 5	Sert - Last Seen Descen								Involut
# (8/26) # X 1048/10/04 1	0.4 34		Sert just See Decen		AIN	Free	Les	James		Tap.	(earlier)
	0.4 34	wið 1840 + 5		-					00	Taga Chalar Count Int. Chanadh	Destinal
# (8/26) # X 1048/10/04 1	0.0	ne:20 1-20178 + 3 Insula	Lauritors	ing - Marant	ADA	Frei	Last	Bourse			Seathart
	0 · 9	w.8 18478 + 5 houte houte	Lauriton 1/3	ting * Nerwork 107,056017	484 6267	First 2014-08-07	Last 2016-09-21	James James		🗄 Ogital Course Inc. 🔄 Boulation	(contract
0 (01/0) → × 1044510/04 1 → × 1044510/03 1 → × 102/0522 1 → × 102/0522 1 → × 102/0522 1 → × 10200 100 1 → × 1024000 1 5000/0000	0 · 9	10000239 00000239 00000239	Laudies 10 11	ng - Natasak 101,066017 10202845	484 6267 1918	First 2014-09-07 2014-09-10	Land 2014-09-21 2014-09-03	Searce projectorij scoperajectorij		Copfei Cours-Inc. Contextual Anacon-Cors-Inc. Contextual Con	-
# (96.76) # 304.86.16/56 1 # 304.86.16/56 1 # 304.86.16/50 1 # 304.86.16/50 1 # 304.86.160 1 # 304.84.16/50 1 # 304.84.16/50 1 # 304.84.16/50 1 # 304.84.16/50 1	0 · 9	ne 26 1254718 + 5 houte 02101233 0210175181 NE20141245	Lauriton 13 15 15	Mag • Kanash VE7356041 VE2560415 VE2560016	434 6267 1473 2714	Pase 2016-08-07 2016-08-10 2016-08-20	Last 2014-09-21 2014-09-01 2014-09-00	Janes pengurang kaserang anggurang mutatal penggurang		C Dybli Chan br. C Bardib Annan Santha. C Bardib C BhAnashada. C Bhaddib C BhAnashada. C Bhaddib	
0 (01/0) → × 1044510/04 1 → × 1044510/03 1 → × 102/0522 1 → × 102/0522 1 → × 102/0522 1 → × 10200 100 1 → × 1024000 1 5000/0000	0 · p	ne 25 1-254739 + 5 booke 02/00/201 02/201/5.00 00/201/5.00 00/201/5.00	Launten ult ult ult ult	ng • Mawash 107/06/047 52202445 102266/078 102266/078	Als 6267 1408 294 294	Pase 2016-06-07 2016-06-09 2016-06-29 2016-07-29	Last 2014-09-21 2014-09-03 2014-09-08 2014-09-08	Barrat page-rate stage-rate page-rate page-rate			
IP (00/76) I IP (A) (0445150 (04) I IP (A) (045150 (04)) I		ner 20 1.20 ef 70 e - 5 headar 10 x 00 2.20 10 20 x 02 20 10 20 x 02 20 x 02 20 x 02 20 10 20 x 02 20 x 02 20 x 02	iauaten 13 13 13 13 13 15 15	Maraini Maraini Milliona Milli	Als 2007 3414 2014 2014 403 403	First 2016-00-07 2014-06-00 2014-06-00 2014-06-00 2014-06-00 2014-06-00	Last 2014/08/21 2014/08/23 2014/08/23 2014/08/24 2014/08/24 2014/08/24	Narre programa nagrama programa programa programa nagram nagram n n n n n n n n n n n n n n n n n n n		Elyter Counter See, Electrical Extended Counter See, Electrical Entropy See, Electrical Entropy See, See, See, See, See, See, See, See	famlar
in (SU/SE) in X V0445110-00 1		NY 20 1-2017/0 × 5 books 62/00/2018 62/00/2018 62/00/2018 62/00/2018 62/00/2018 62/00/2018 62/00/2018 62/00/2018 62/00/2018	iaudes al al al al al al al al al al al al al	Maran K Maran K Mit Jakoban Mit Jakoban Mit Jakoban Mit Jakoban Mit Jakoban Mit Jakoban Mit Jakoban Mit Jakoban Mit Jakoban	AB 2007 3438 2914 2914 463 463 463 3019	First 2014-06-07 2014-06-10 2014-06-10 2014-06-08 2014-06-08 2014-06-08	Last 2014-09-21 2014-09-21 2014-09-20 2014-00 2	Name programs programs sources programs programs programs programs programs programs		C Dyla Comato. C Dalabo C Dalamatana. C Dalabo C Dalamatana. C Dalabo C Dalabo. C Dalabo C Dalabo. C Dalabonatana C Dalabo. C Dalabonatana C Dalabo. C Dalabonatana	Sector
# (8)/16 ** VA45115/06 1 ** VA45115/07 1 1 ** VA45115/07 1 1 ** VA54115/07 1 1 ** VA5115/07 1 1 ** VA5115/07 <td></td> <td>Ner (6 1254/16 e) 5 booke 00000223 00000223 00000223 000000223 000000223 00000000</td> <td>iaudes al al al al al al al al al al al al al</td> <td>Mg • McGel VL7/56/017 VL7/56/017 VL7/56/014 VL7/56/014 VL7/56/014 VL7/56/014</td> <td>488 6267 2414 2414 663 663 808 808 809 809</td> <td>Fine 2014-00-07 2014-00-10 2014-00-10 2014-00-00 2014-00-00 2014-00-00 2014-00-00 2014-00-00</td> <td>Last 2014-09-21 2014-09-21 2014-09-20 2014-00 2</td> <td>Narre Jarge rise Aspereg jarge rise invester garge rise rise rise rise rise</td> <td></td> <td>Dyd Janubi, Filmain Manainen, Blanain Manainen, Blanainen Manainen, Blanainen Manainen, Blanainen Manainen, Blanainen Manainen, Blanainen Manainen, Blanainen Manainen, Blanainen</td> <td></td>		Ner (6 1254/16 e) 5 booke 00000223 00000223 00000223 000000223 000000223 00000000	iaudes al al al al al al al al al al al al al	Mg • McGel VL7/56/017 VL7/56/017 VL7/56/014 VL7/56/014 VL7/56/014 VL7/56/014	488 6267 2414 2414 663 663 808 808 809 809	Fine 2014-00-07 2014-00-10 2014-00-10 2014-00-00 2014-00-00 2014-00-00 2014-00-00 2014-00-00	Last 2014-09-21 2014-09-21 2014-09-20 2014-00 2	Narre Jarge rise Aspereg jarge rise invester garge rise rise rise rise rise		Dyd Janubi, Filmain Manainen, Blanain Manainen, Blanainen	
# (8)/16 ** VA45115/06 1 ** VA45115/07 1 1 ** VA45115/07 1 1 ** VA54115/07 1 1 ** VA5115/07 1 1 ** VA5115/07 <td></td> <td>NY 20 1-2017/0 × 5 books 62/00/2018 62/00/2018 62/00/2018 62/00/2018 62/00/2018 62/00/2018 62/00/2018 62/00/2018 62/00/2018</td> <td>iaudes al al al al al al al al al al al al al</td> <td>Maran K Maran K Mit Jakoban Mit Jakoban Mit Jakoban Mit Jakoban Mit Jakoban Mit Jakoban Mit Jakoban Mit Jakoban Mit Jakoban</td> <td>AB 2007 3438 2914 2914 463 463 463 3019</td> <td>First 2014-06-07 2014-06-10 2014-06-10 2014-06-08 2014-06-08 2014-06-08</td> <td>Lee 2014/03/21 2014/03/03 2014/03/03 2014/03/04 2014/03/04 2014/03/04 2014/03/04 2014/03/04 2014/03/23</td> <td>Name programs programs sources programs programs programs programs programs programs</td> <td></td> <td>C Dyla Comato. C Dalabo C Dalamatana. C Dalabo C Dalamatana. C Dalabo C Dalabo. C Dalabo C Dalabo. C Dalabonatana C Dalabo. C Dalabonatana C Dalabo. C Dalabonatana</td> <td></td>		NY 20 1-2017/0 × 5 books 62/00/2018 62/00/2018 62/00/2018 62/00/2018 62/00/2018 62/00/2018 62/00/2018 62/00/2018 62/00/2018	iaudes al al al al al al al al al al al al al	Maran K Maran K Mit Jakoban Mit Jakoban Mit Jakoban Mit Jakoban Mit Jakoban Mit Jakoban Mit Jakoban Mit Jakoban Mit Jakoban	AB 2007 3438 2914 2914 463 463 463 3019	First 2014-06-07 2014-06-10 2014-06-10 2014-06-08 2014-06-08 2014-06-08	Lee 2014/03/21 2014/03/03 2014/03/03 2014/03/04 2014/03/04 2014/03/04 2014/03/04 2014/03/04 2014/03/23	Name programs programs sources programs programs programs programs programs programs		C Dyla Comato. C Dalabo C Dalamatana. C Dalabo C Dalamatana. C Dalabo C Dalabo. C Dalabo C Dalabo. C Dalabonatana C Dalabo. C Dalabonatana C Dalabo. C Dalabonatana	
(0.10) × 0.041/0.04 1		Ner (6 1254/16 e) 5 booke 00000223 0000523 0000524 0000501 0000501 0000501 0000501 0000501 0000501 0000501 0000501 0000501 0000501 0000501 0000501 0000501 000050 000500 00050 000000	iaudes al al al al al al al al al al al al al	Mg • McGel VL7/56/017 VL7/56/017 VL7/56/014 VL7/56/014 VL7/56/014 VL7/56/014	488 6267 2414 2414 663 663 808 808 809 809	Fine 2014-00-07 2014-00-10 2014-00-10 2014-00-00 2014-00-00 2014-00-00 2014-00-00 2014-00-00	Last 2014-09-21 2014-09-21 2014-09-20 2014-00 2	Narre Jarge rise Aspereg jarge rise invester garge rise rise rise rise rise		Dyd Janubi, Filmain Manainen, Blanain Manainen, Blanainen	
0 (0170) 0 0.0411000 0 0 × 0.04410000 1 0 0 0 × 0.04410000 1 0 0 0 × 0.0140000 1 0 0 0 × 0.0140000 1 0 0 0 × 0.0140000 1 0 0 V × 0.01400000 1 0 0 V × 0.01400000 1 0 0 V × 0.0140000000000000000000000000000000000		Ne 18 6 65 678 4 5 5 Noxada No 10 0 2.21 No 20 6 2.21	Landon 13 15 15 15 15 15 15 15 15 15 15 15	Mg • Worket U2365607 U2366507 U2366507 U236607 U236607 U236607 U236607 U236607 U236607 U236607 U236607 U236607 U236607	48 1227 1428 274 274 460 304 204 204	Faue 2014-00-07 2014-00-10 2014-01-09 2014-03-08 2014-03-08 2014-03-08 2014-03-08 2014-03-08 2014-03-08	Lee 2014/03/21 2014/03/03 2014/03/03 2014/03/04 2014/03/04 2014/03/04 2014/03/04 2014/03/04 2014/03/23	Bane ungerinst			
$\begin{array}{c} 0 \\ (0,10) \\ ($		Ne 18 6.25478 4 3 5 Noxee Second 2.23 Second 2.23 Sec	Landon 13 15 15 15 15 15 15 15 15 15 15 15 15 15	Mg + MU204001 SU204045 SU204055 SU204059 SU205059	484 4200 2014 2014 460 3009 3009 3009 3009 3009 3009 3009 30	Faul 2014-00-07 2014-00-10 2014-01-10 2014-01-00 2014-00-00 2014-00-00 2014-00-00 2014-00-00 2014-00-00	Law 2014/03/21 2014/03/23 2014/03/24 2014/03/24 2014/03/24 2014/03/24 2014/03/24 2014/03/24	Norm Importants surgerinnes surgerinnes importants import		Synthesis Synthesis Texture State Synthesis State	
x State State 1		NY 26 426476 4 2 3 NY 26 426476 4 2 3 NY 264476 4 2 4 4 NY 26476 4 2 4 NY 26476 4 2 NY 2	Laadden 23 23 23 23 23 25 25 25 25 25 25 25 25 25 25 25 25 25	Ming * Minosit 403/05.0013 403/05.0014 403.05.0014 404.0014 404.000	484 4200 2014 2014 460 3009 3009 3009 3009 3009 3009 3009 30	Proj 2014/00 (2014/00 ()	Lee 2004/04/27 2014/04/28 2014/04/28 2014/04/28 2014/04/28 2014/04/28 2014/04/28 2014/04/28	beet (any) andi (ang) andi			

STEP 3: • Click on the **WHOIS** data tab

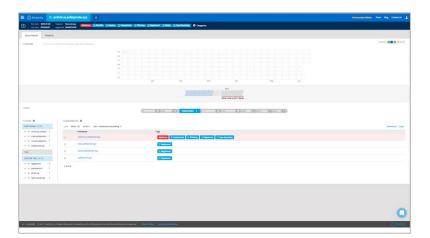
- Is the registrant information privacy protected?
- Examine the Change history and determine if any of the entries contain information that is not privacy protected?

Oniovo Q.			
Texten Brank	Inginer Kanadang	E Baldel (Diverse) (Diverse) (Diverse) (Diverse) (Diverse) (Diverse)	
		p 10 10 10 10 10	
		and the second se	
		Dist Game 20 Mark	
		Analysis (1) 1990 (2) Indexes (1) Indexes (2) Index (2)	
ANDE HISTORY	RECORD PROM 301	1.46.41	
17.44.05		at & norths ago ((notest a year ago	
12.49-18	All them	Your	
018-11-01	WHOS Server	and the second	
017-09-04	highlar	Nanachap	
116-10-13	Enul.	mentantine pendingthramentappi seen (regionant, adrise), kelling, teol (
016-08-28	harve	RECTINED RED LINES	
116-09-25	Ergenisation.	SubSOUD (splerur, adro), joing seys	
118-08-14 118-08-23	literi	1 MBL K. GAMME BAG, SURT 200 (Highware) 1 MBL K. GAMME BAG, SURT 200 (Highware)	
16-10-27	09	(d5.408)(35.3) system or Latrice, bring tach	
10.02.02	Sure .	GA (regionary, usino, billing, such	
	Period	900kt (registrars, admit, linking lant)	
	Durity	UNITS DATES Implement administration and	
	Protect	Net (F18) (Net All Pagement, Advin, String, Sett)	
		ndi dramatany am	
	Nandarous	nd demokragion nd demokragion nd demokragion	-

	Topor Renders	Canada Canada Canada Canada Canada Canada Canada Canada Canada	
Latter Brack2	Teptore NURDER		
		J Company 1 1 1 2 2	
CHARGE HISTORY	RECORD FROM 1	(making) and) Making (Denois) and () and () and ()	
2017-06-05		na na serie en la constante e para ago	
2017-03-13	Abriture	New Conception of the Concepti	
2010-11-01	W405 Server		
2017-03-06	New	Netros	
2017-03-06	Nger v Drut	Non-Neg el/s/Solubilediad/SolfMillindup/neg/en/ace/papers/arty_bitg.se/j	
2016-10-13			
2014-07-14	(mat	WMATERIALMANATIVATIONS and the second s	
2014-05-13 2014-05-14 2014-06-28 2014-06-25	linal Nativ	Manifers Juniors Julians republic republic and regrouping representation of the second representation of the second representation of the second representation regroup representation of the second representation of the	
2014-05-13 2014-05-14 2014-05-25 2014-06-25 2014-06-14	Druit Narie Organization	Mich Challengen and C	
2014-10-15 2014-06-28 2014-06-28 2014-06-25 2014-06-25 2014-06-14 2014-06-29	Small Name Organisation Sirent	NY Shadabadara Ny Balana amin'ny fisiana amin'ny fisiana Fisiana amin'ny fisiana amin'ny fisiana amin'ny fisiana amin'ny fisiana amin'ny fisiana amin'ny fisiana amin'ny	
2014-16-19 2014-01-14 2014-06-28 2014-06-25 2014-06-25 2014-06-29 2014-06-27	Enal Nore Oprison Stat. Op Bas	Watalanda Katalana Andrana Katalana (Katalana) Malaka Katalana Katalana (Katalana) Malaka Katalana Katalana Malaka Katalana (Katalana) Malaka Katalana (Katalana) Managang Katalana (Katalana)	
2014-10-10 2014-07-14 2014-08-20 2014-08-25 2014-08-25 2014-08-25 2014-08-29 2014-08-29	bred Name Organisation Street Op Balee Pasal	Alterature and region and r	
2014-16-19 2014-01-14 2014-06-28 2014-06-25 2014-06-25 2014-06-29 2014-06-27	brui Nare Ogradon Seet Oy Sait Naal Gorry	Watalandara Watana Antonya wa Antonya Watalandara Watana Antonya Watalandara Watana Watan Watana Watana Watan Watana Watana Wata	
2014-05-13 2014-05-14 2014-06-28 2014-06-25	bred Name Organisation Street Op Balee Pasal	Alterature and region and r	

STEP 4: • Click on the **Subdomain** data tab

- Are any of the entries colored?
- If yes, what color is used?
- What do you think the color indicates?
- What tags are associated with the entry?



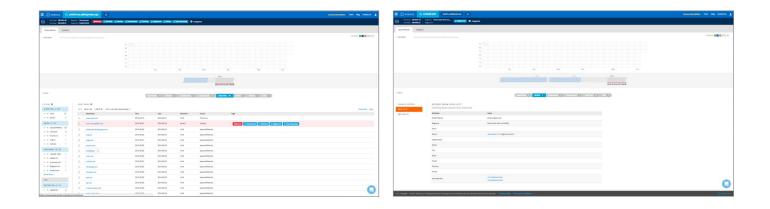
STEP 5:

- Click on the Host Pair data tab
 Examine the domain names
- What domains are forwarding to antivirus.safetynote.xyz (Direction – Child)?
- Are any of the domains typosquatted?
- What must happen to make a typosquatted domain illegal?
- Is there any non-privacy protected WHOIS information on any of the typosquatted domains?

C a Secure h	ttps://www.passivetotal.org/search/a	intivirus.safetynote.x	12				6 Q 2 6
	ttvirus.safetynote.xyz						Community Edition Tears Mog Contact Us
Fest Seen 2016-01-29	Augustrate Madicionen C. Handware						
Last See 204409-21	legitrunt +	and Change Change	and Contraction	• • • • • • • •	2017		
					2016-11-13 1	2217-05-18	
DATA.		feedbare (1)	105 (1)		mponens 😰 Haat P	n Ja CONT () Factor () DNL ()	
ULTERS O	HOST PAIRS 0						
DIRECTION (2/38)		Last Seen Descending *					Download Copy
✓ x chid 3t ✓ x parent 7	Hostname	First 2016-03-10	Last 2016-09-21	Direction	Cause trame.org	Tags	
CAUSE (5/30)	arrestrap.com	2016-02-01	2016-02-04	and a	relies.		
✓ H topLevelRedra., 29	U track.newlg400.com					Mathema D Pauloscal D Phabling D Registered	Type Squatting
v X unlenown 6	El hadie persiant/bpages.com	2016-02-04	2016-02-06	oie	topieve/Redirect		
v it thateas 1	E wijen	2016-02-02	2016-02-04	chie	topLevelRedirect		
w in length t	El pago.com	2016-02-01	2016-02-06	one	topLevelRedrect		
✓ it redirect 1	E taysrus.on	2016-02-02	2016-02-03	010	topLevelRedirect		
HOSTNAME (387.38)	0 unitediam	2016-02-09	2016-02-08	oie	topievelledirect		
✓ X adobe.om 1	E setures	2016-02-09	2016-02-03	child	topLeveRedirect		
✓ X areasnap.com 1	C tumbicam	2016-02-01	2016-02-03	one	topiave/Redirect		
✓ X blogspotom 1	ehatsapp.om	2016-02-02	2016-02-03	child	topLave/Redirect		
w it boxfee.com 1 Show More	C dropbex.om	2016-02-09	2016-02-03	chie	topLevelRedrect		
740	() poten	2016-02-02	2016-02-03	one	topLevelRedirect		
SYSTEM TAG (7/12)	D ignore	2016-02-08	2016-02-03	014	topieveilledirect		
× X registered 6	E trackssummit, info	2016-02-02	2016-02-03	chid	topLeve/Redirect		
✓ X known,compro 1	E trackzektSiefe	2016-02-02	2016-02-08	ene	topLevelRedrect		
✓ × passivetatal 1	El Ipch/kvoluumtrk.com	2016-02-09	2016-02-08	010	topLevelHedrect		
✓ X phaking 1 ✓ X redependence. 1	U titudiam	2016-02-08	2016-02-03	one	topLeveRedirect		
Shew More	D beefes.com	2016-02-02	2016-02-08	orie	topLeveRednect		
	E adobe are	2016-02-02	2016-02-03	one	topLeve/Redirect		
	B specify ann	2016-02-02	2016-02-05	one	topLevelRedirect		
	www.facebook.com	2016-02-02	2016-02-02	child	ingarc		
	D blogspot.om	2016-02-02	2016-02-02	chie	topieveRedrect		
	© redftam	2016-02-02	2016-02-02	016	topLove/Redirect		
	C trailon	2016-02-02	2016-02-02	ana	topiave/Redirect		6
	0 1042981395	2016-02-02	2016-02-02	parent	unimown	E Reckspace Heating E Routable	

STEP 6: Click on united.ocm and check the WHOIS registration.

- Is the registration privacy protected?
- Click on the WHOIS data tab.



STEP 7: Click on antivirus.safetynote.xyz

	antidrus.safegrese.sys O								Community Edition Teurs Blog Contect Us
Pint Seen 2014-01-14	Bightror Omen Data Ferk LLC	Categorine							
Query Results Feetp									
		\							iterne 🔳 🖬 🕄 🕾
EATMAP The set of	$\beta (\beta / \gamma h) \beta + \beta (\beta / \beta) + hout (h) g (\beta / \beta) her Die of hout (h) hout (h)$	1							
		-							
		-							
		7							
			her.	Aug.	Mar	Apr	May	Jan	
							2017		
							2016-12-04 to 2017-06-06		
			Contraction	3 WHOS 2 Sales	0	0	0		
HANGE HISTORY	RECORD FROM 2016-10-17 Checked by RokiQ [Expiration NVA [Chaldon NV		Contraction	B WHOS 2 SAN	0				
HANGE HISTORY 016-10-17	Checked by RiskiQ Expiration NVA Creation N/ Attribute	Value		13 WHOS 2 544	0	erren () menter (H			
NANGE HISTORY	Checked by RokiQ Exprosion Nok Creation No Accribute WHOS Server	Value whois.registry.o	-	x (3) WHOS 2, 5A4	0	eren O mutan O			
HANGE HISTORY	Checked by RokiQ Expiration Noh Crustion Noh Attribute WHG3 Server Registrer	Value	-	* (3) MHOS 2, 544	0	ymenn () – Henrikans (H			
NANGE HISTORY	Checked by RokiQ (Expiration Nok (Checkton No Actibule WHX05 Server Register Email	Value whois registry o Oman Data Pari	94 9 LLC (004)	() WHOG 2 244	and in a first	yaant () minter (M			
ANGE HISTORY	Chester by Ball (Equation NA) Cheston NA Attribute WHO'S Samer Register Email Name	Value whois registry o Oman Data Pari	-	() WHOG 2 244	anan () bay	wana () markan (d			
NANGE HISTORY	Checked by HeixiQ Expendent NA Charlon An Retroya Heixio Sanner Registrer Email Name Organisation	Value whois registry o Oman Data Pari	94 9 LLC (004)	O MHOE 2 DAM	anan () bay	waan () markan (d			
NANGE HISTORY	Checkel by Hold (Expiration Nut (Calation No Refibule 1995) Street Register Email Nome Organization Street	Value whois registry o Oman Data Pari	94 9 LLC (004)	0 000 1 LAA	amatan () Davy	eenen () – murkke (4			
HANGE HISTORY 016-10-17	Checkel by Mail () Expiration NAI () Calation ND Refloxer Refloxer Registrar Registrar Remei Remei Street Chy	Value whois registry o Oman Data Pari	94 9 LLC (004)	0 MOG 2 GA	anatan () Dary	pont () milita (H			
HANGE HISTORY	Checkel by HealD Expenden NAI Chellon Ho Hendbare Hendbare Envel Envel Name Digenostyn Stark	Value whois registry o Oman Data Pari	94 9 LLC (004)	0 000 1 000	amatan 3 Dary	gann () — Handsin (M			
HANGE HISTORY 016-10-17	Declarating registrations from a constraint of	Value whois registry o Oman Data Pari	94 N.L.C. (004)			eens O multipation of			
HANGE HISTORY 016-10-17	Checkel by Hold (Exproduct NAI (Charlon NA Refubule WHO Sover Apploy Email Organization Organizion Organization Organizion Organizion O	Value whois registry o Oman Data Pari	94 N.L.C. (004)	0 m0 1 ***		para () matrix ()			
HANGE HISTORY	Declarating registrations from a constraint of	Value which registry and Omen Data Part	un KLLC(DOP) ((regenent koh)	0 mod 1 ***		gann () — Handkin (A			
waase wistoor waase histoor Diseato	Checkel by Hold (Exproduct NAI (Charlon NA Refubule WHO Sover Apploy Email Organization Organizion Organization Organizion Organizion O	Value whois registry o Oman Data Pari	en Nuc (son (spanner, tud)						

- STEP 8: Click back on antivirus. safetynote.xyz
 - Review the host pairs again.
 - Review the result track. mcwtg400.com. Is the domain a child or parent?

		safetynote.xyz untetim with	drus salage case at							
First Seen. 2016-01-29 Last Seen. 2016-09-21	Ingener No.	Manada Bankar Bankar Bankar	Constant (Damage)	Departed [Hotel	Declaring O c	xagoria				
Arritouts Netprit										
										1551ND 🖬 🖬 🖄 🗇 🕖
HOCHER IN THE PROPERTY IN										0 10 10 10 10 10 10 10 10
			10 m							
			-							
					No	Mar	Apr	May Jun		
						3817				
							04 to 2017-06-08			
						211.24	of the sector of the			
ATA .										
			C	lation (7) and (Subbreaker Ø 	Colorent (2) Med	thirs 38 CONTID	riefer (). 245 ()		
LTEAS 0		ST PARS O								
		Show (25 1-25 of 38 + Seri) Lost Seen								Described Copy
K 658 31		Hestsame	Int	Lest	Direction	Cause	Taga			Described Capp
r x elle 31 r X pret 3		Hestsame		Last 2016-09-21	Direction	Cause thama.org				Descripted Copy
r X etile 31 r X piret 7 Most 0/36		Restruite ansaragizan	Int						lyes Rewalling	Described Capy
r X phile 31 r X parent 7 CAUSE (5738) r X topcanthedric, 29	-	Mesthume anestrap.com track.mestgatil.com	Rest. 2016-00-10	2016-09-21	016	Parent		Tanana (Tanan) Tanan	See Several Sec.	Downlawt Copy
v X ehit 31 v X pret 7 XXSE (5738) v X topcastiledric 29 v X uninsen 6	0 0	Horowne anastrajstvin track movingstill com hutte person Rykgins com	Pine 2016-00-10 2016-00-01	2016-09-21 2016-00-04	ons parent	thama.org		tuutened 2 Mathing 2 Magdaland 21	ge bywing	Downlawt Copy
 X parent 7 CASSE (5738) X topcastRedre	8	Kestname ansakraja Jum track moungelik eem hude jensen flijkeges com opj an	Pink 2016-00-10 2016-00-01 2016-00-01 2016-00-04 2016-00-00	2016-09-21 2016-00-04 2016-00-04 2016-00-04	one prest one one	rhamung rednest topLeverRednest topLeverRednest		Statut Statut Statut	and grant of	Dourinal Copy
 × chil × paret 7 Child (5/36) × Spichelfedric, 29 × urknam 4 v dramanc 1 	0	Hoshane ansakapatin trask norsytöllen bade proverfigeen con wej on prepare	Pine 2014-00-10 2014-02-01 2014-02-04 2014-02-04 2014-02-01	2016-00-21 2016-00-04 2016-00-04 2016-00-04 2016-00-04	one pret one one one	themsang network Septemethedness Septemethedness Septemethedness		Industri (Chaires) (Chairman) (Chairman)		Dearbest Cag
r X shid 31 r X peret 7 Audit 01/36 7 r X topcontributing 29 r X topcontributing 29 r X topcontributing 6 r X topcontributing 1 r X topcontributing 1 r X topcontributing 1 r X topcontributing 1	0 0 0 0 0	Heatmanne Arreach.arg. a fair Strach.arg. a fair Strach.arg. a fair Strach.arg. a fair Arreach.arg. a fair Arg. a	Pine 2014-03-15 2014-03-01 2014-03-04 2014-03-04 2014-03-04 2014-03-04	2014-09-21 2014-02-04 2014-02-04 2014-02-04 2014-02-04 2014-08-03	one prest one one one	Hamuns rednet teptaveflednet teptaveflednet septaveflednet teptaveflednet		Papinski 🛛 Ridveg 🖸 Replaced 💿	(or forming	Deveload Cog
Y 2HB 31 Y parent 7 AbSE (51/36) F 2P Y topcanthetins	0	Heatmanne Arreach.arg. a fair Strach.arg. a fair Strach.arg. a fair Strach.arg. a fair Arreach.arg. a fair Arg. a	Pine 2014-00-10 2014-02-01 2014-02-04 2014-02-04 2014-02-01	2016-00-21 2016-00-04 2016-00-04 2016-00-04 2016-00-04	one pret one one one	themsang network Septemethedness Septemethedness Septemethedness		inning Carry Councy (Deveload Cog
r X bNd 31 r X parent 7 XX552 CF3/bit - r X spannelhedres	0 0 0 0 0	Magane anatagasin tackinongkilion holepinanigasian mgan gagaan gagaan ugunuum	Pine 2014-03-15 2014-03-01 2014-03-04 2014-03-04 2014-03-04 2014-03-04	2014-09-21 2014-02-04 2014-02-04 2014-02-04 2014-02-04 2014-08-03	one prest one one one	Hamuns rednet teptaveflednet teptaveflednet septaveflednet teptaveflednet		Teninini (Tenny Chymrof)		Devided Top
r X bNd 31 r X parent 7 AppSL D*100	0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	Magane anatagasin tackinongkilion holepinanigasian mgan gagaan gagaan ugunuum	Ping 2016-00-10 2016-00-00 2016-00-00 2016-00-00 2016-00-00 2016-00-00	2014-09-21 2014-02-04 2014-02-04 2014-02-04 2014-02-04 2014-08-03 2014-02-03	oue oue oue oue teaut oue	Hamuss rednot topkovthohod topkovthohod spkovthohod topkovthohod topkovthohod topkovthohod		199999 (2009) (2009) (3	An Ennity	Davied Egy
Xi able 31 Xi parent 7 Accil: 0.7.00 7 Xi calculation 29 Xi calculation 29 Xi calculation 6 Xi magnetic 1 Xi magnetic 1 GOTSCAME (24) 1 Xi ablescom 1 Xi ablescom 1 Xi ablescom 1	0 0 0 0 0 0 0	Radiume antastagioni fundi mengengistan Andre persentipegistan anglasi gagistan gagistan ustratam sebuari	Pink 2016-80-10 2016-80-10 2016-80-00 2016-80-00 2016-80-00 2016-80-00 2016-80-00 2016-80-00 2016-80-00 2016-80-00 2016-80-00 2016-80-00 2016-80-00	2014-00-21 2014-02-04 2014-02-04 2014-02-04 2014-02-04 2014-02-04 2014-02-03 2014-02-03 2014-02-03	015 54465 016 016 016 016 016 016	Hansurs Heinest Leptenethelmest Leptenethelmest Leptenethelmest Leptenethelmest		Standard (Starter)		Davidd flig
P X photo 31 P X parket 7 MSSE (07.56) X sparketMolex. 29 V SparketMolex. 29 4 V SparketMolex. 1 1		Retreet Sectory Sectory Sectory Sectory Reprise Sectory Sector	Pine 2014-03-15 2014-03-05 2014-03-06 2014-03-06 2014-03-06 2014-03-06 2014-03-06 2014-03-06 2014-03-06 2014-03-06 2014-03-06 2014-03-06 2014-03-06 2014-03-06	2016-00-21 2016-00-24 2016-00-24 2016-00-24 2016-00-24 2016-00-28 2016-00-28 2016-00-28 2016-00-28	ond parent ond ond ond ond ond ond ond ond ond ond	Hamauri Hamauri Splavetholmai Splavetholmai Splavetholmai Splavetholmai Splavetholmai Splavetholmai		ining Sking Stand (S	Ye general	Davidat (bg
X (hid) 31 X parent 7 Alcol In/View 7 X Y X parent 6 X X parent 6 X X parent 1 Y X parent 1 V X parent 1 ODTMARK (INVI) Y X parent Y X parent 1 Y Margant 1 Y Margant 1 1		Pennya Ananaya Ana Ananaya Ana Kata pengantagan ana Ang pengan Ang	ина 2014-00-10 2014-00-00 2014-00-00 2014-00-00 2014-00-00 2014-00-00 2014-00-00	2016-00-21 2016-00-34 2016-00-34 2016-00-34 2016-00-38 2016-00-38 2016-00-38 2016-00-38 2016-00-38 2016-00-38	005 parent 005 005 005 005 005 005 005 005	Harne, se Harne, se Hapitane Rushvasi Hapitane Rushvasi Hapitane Rushvasi Hapitane Rushvasi Hapitane Rushvasi Hapitane Rushvasi Hapitane Rushvasi Hapitane Rushvasi Hapitane Rushvasi		annan (anna (anna) (a		Audual By
x 2010 31 x parent 7 Debsite (xr/m) 20 20 x supervention 20 x supervention 1 x manufacture 1 x manufacture 1 x manufacture 1 x manufacture 1 x supervention 1		Handhar Annala ann Annala ann Annala ann Annala Ann	ня 214403 214403 214404 214404 214404 214404 214404 214404 214404 214404	2016-00-21 2016-00-34 2016-00-34 2016-00-36 2016-00-39 2016-00-39 2016-00-39 2016-00-39 2016-00-39 2016-00-39 2016-00-39	end parent end end end end end end end end end end	Harra yı Adrea Gişsenfikalındı Gişsenfikalındı Gişsenfikalındı Gişsenfikalındı Gişsenfikalındı Gişsenfikalındı Gişsenfikalındı Gişsenfikalındı Gişsenfikalındı		annan ann ann ann a		Savid (g
v N ohie 31 v N ohie 31 v N ohie 31 v N ohie 32 v N ohie 31 v N ohie 32 v N ohie 31 v No 31 v No 31		Pennya Ananaya Ana Ananaya Ana Kata pengantagan ana Ang pengan Ang	не 294409 294409 294409 294409 294409 294409 294409 294409 294400 294400	2016-00-21 2016-00-26 2016-00-26 2016-00-26 2016-00-28 2016-00-28 2016-00-28 2016-00-28 2016-00-28 2016-00-28	015 015 015 015 016 016 016 016 016 016 016 016	Hamaya Anibati Supportanian Supportanian Supportanian Supportanian Supportanian Supportanian Supportanian Supportanian Supportanian Supportanian		annan anna annan a		for the second sec
v K Physical 21 V X Appendix 21 OLASSE SILVAL X Appendix 22 V X Appendix 23 V X Appendix 24 V X Appendix 1 V X Appendix 1 <td></td> <td>Handhar Annala ann Annala ann Annala ann Annala Ann</td> <td>ня 214403 214403 214404 214404 214404 214404 214404 214404 214404 214404</td> <td>2016-00-21 2016-00-34 2016-00-34 2016-00-36 2016-00-39 2016-00-39 2016-00-39 2016-00-39 2016-00-39 2016-00-39 2016-00-39</td> <td>end parent end end end end end end end end end end</td> <td>Harra yı Adrea Gişsenfikalındı Gişsenfikalındı Gişsenfikalındı Gişsenfikalındı Gişsenfikalındı Gişsenfikalındı Gişsenfikalındı Gişsenfikalındı Gişsenfikalındı</td> <td></td> <td>Tenned Tenne Conned T</td> <td></td> <td></td>		Handhar Annala ann Annala ann Annala ann Annala Ann	ня 214403 214403 214404 214404 214404 214404 214404 214404 214404 214404	2016-00-21 2016-00-34 2016-00-34 2016-00-36 2016-00-39 2016-00-39 2016-00-39 2016-00-39 2016-00-39 2016-00-39 2016-00-39	end parent end end end end end end end end end end	Harra yı Adrea Gişsenfikalındı Gişsenfikalındı Gişsenfikalındı Gişsenfikalındı Gişsenfikalındı Gişsenfikalındı Gişsenfikalındı Gişsenfikalındı Gişsenfikalındı		Tenned Tenne Conned T		

What You've Done

Now you have learned the techniques to research a domain and identify typosquatting. You now know all the domains that were being targeted by the threat actor. Armed with this knowledge you now know which domains to block on your firewall to prevent users from accidentally going to the targeted typosquatted domains.



RisklQ, Inc.

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

- Learn more at riskiq.com
- Copyright © 2020 RisklQ, Inc. RisklQ, the RisklQ logo and RisklQ family of marks are registered trademarks or trademarks of RisklQ, Inc. in the United States and other countries. Other trademarks mentioned herein may be trademarks of RisklQ or other companies.01_20
- ≤ sales@riskiq.net
- **L** 1888.415.4447