Domain Investigation Exercise

antivirus.safetynote.xyz

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

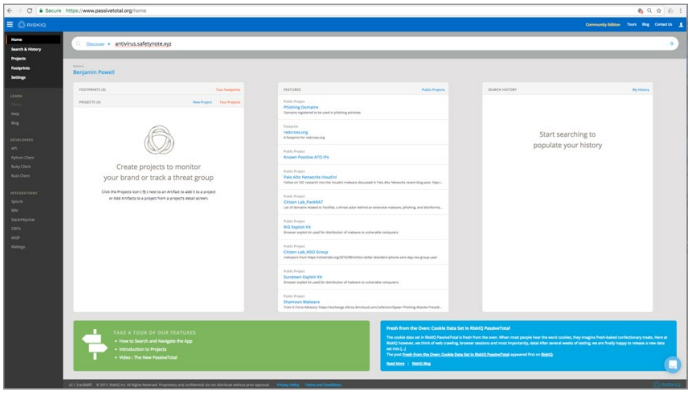
In this exercise, you have been given a domain from your firewall logs to investigate. You are tasked with investigating the domain to determine if it is malicious or associated with malicious domains.

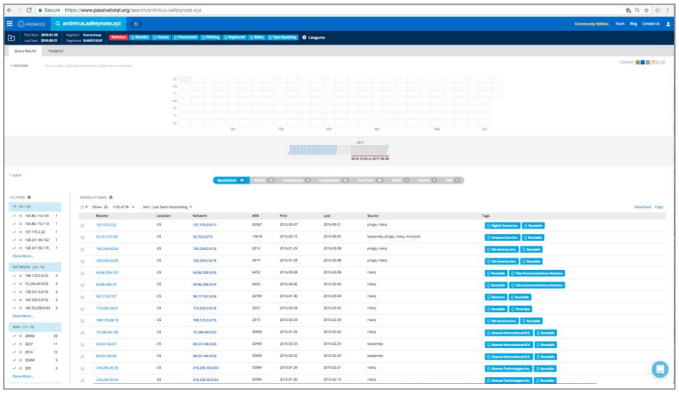
Lets Get Started

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

STEP 2:

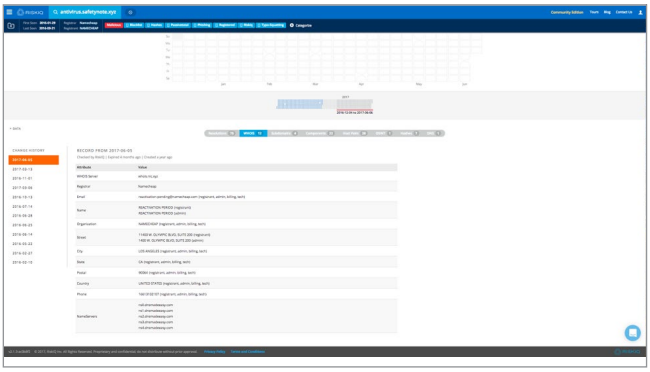
- In the Discover window type: "**antivirus.safetynote.xyz**" without the quotes and hit the **Enter** key.
- Can you determine if the domain still active?
- When was the last time the domain was active?

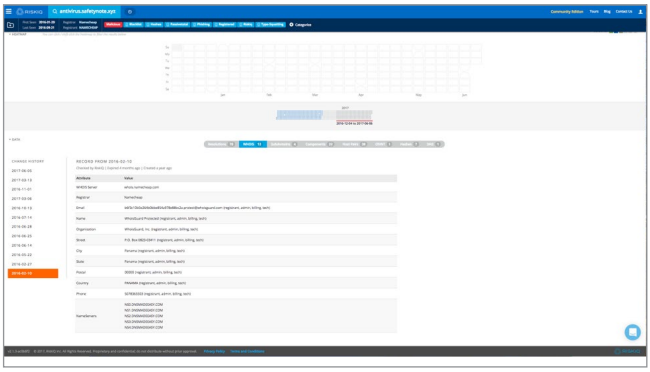




STEP 3:

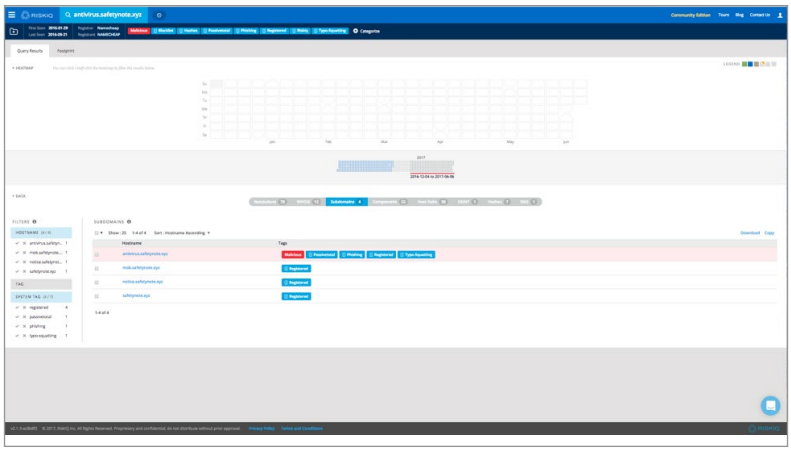
- Click on the **WHOIS** data tab
- Is the registrant information privacy protected?
- Examine the Change history and determine if any of the entries contain information that is not privacy protected?





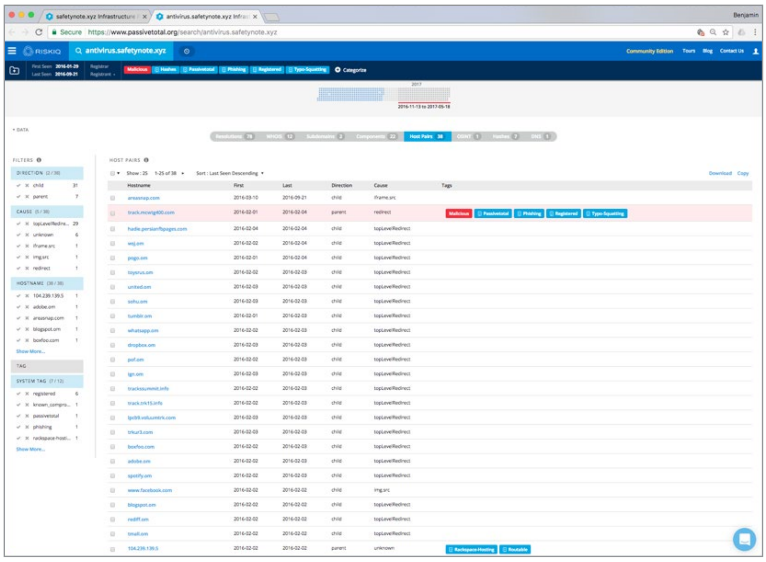
STEP 4:

- 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?



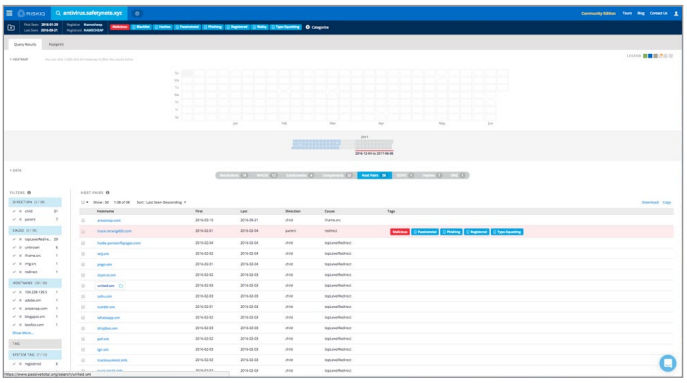
STEP 5:

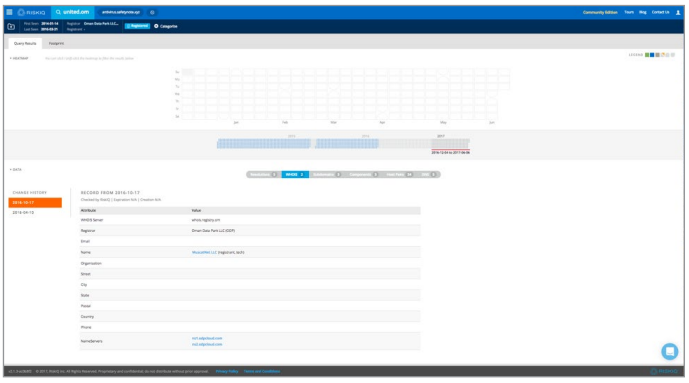
- Click on the **Host Pair** data tab
- Examine the domain names
- What domains are forwarding to antivirus.safetynote.xyz (Direction – Child)?
- Are any of the domains typosquatted?
- What must happen to make a typosquatted domain illegal?
- Is there any non-privacy protected WHOIS information on any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



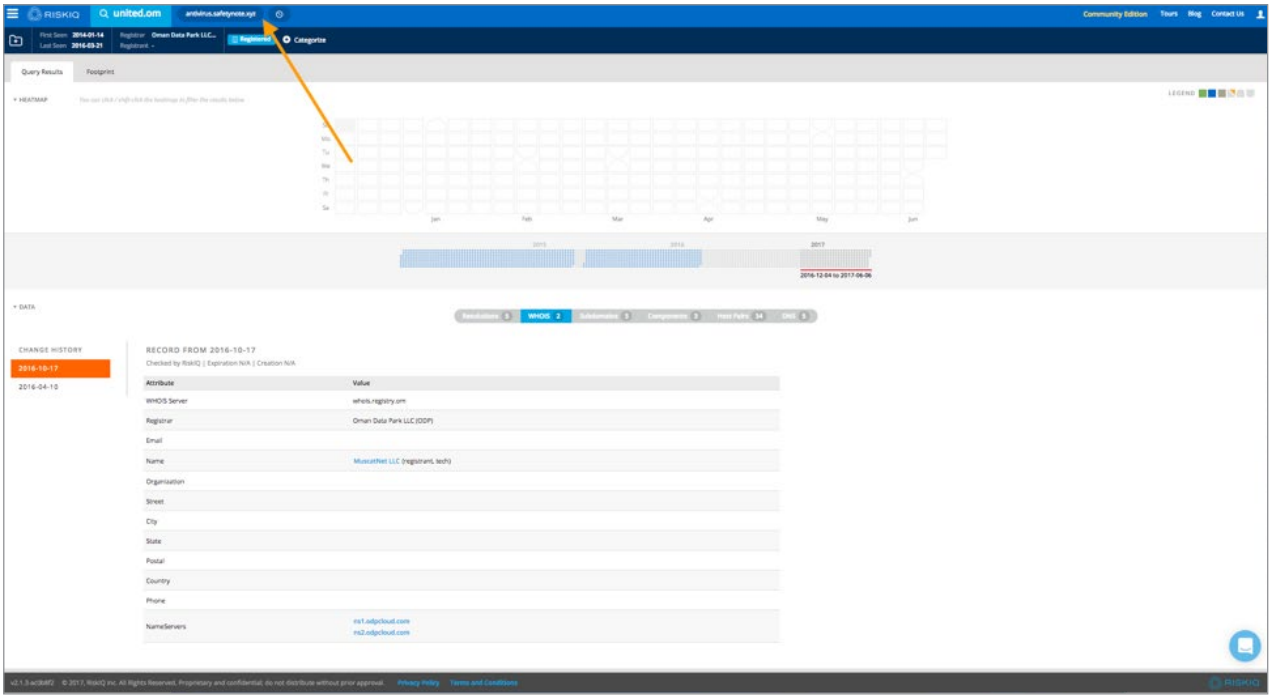
STEP 6:

- Click on united.ocm and check the WHOIS registration.
- Is the registration privacy protected?
- Click on the WHOIS data tab.



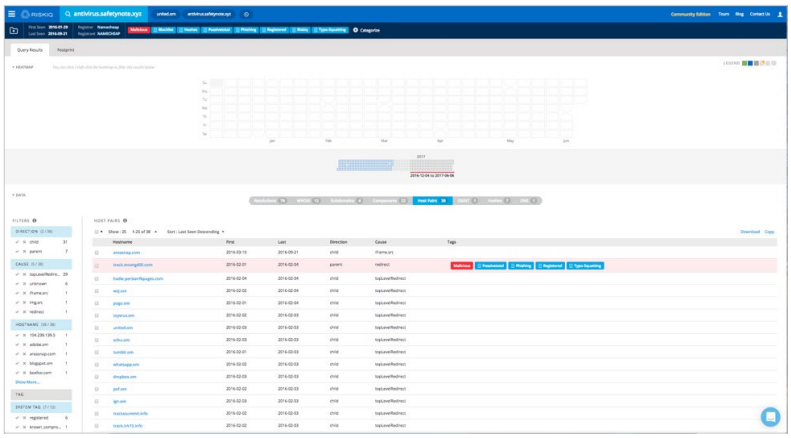


STEP 7: Click on antivirus.safetynote.xyz



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?



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.

RISKIQ®

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

sales@riskiq.net
1 888.415.4447

Learn more at riskiq.com