(TS) NSA QUANTUM Tasking Techniques for the R&T Analyst

POC: [redacted] ([redacted])
TAO RTD | Team [redacted] – Booz Allen Hamilton SDS2

The overall classification of this brief is

TOP SECRET//SI//REL USA, AUS, CAN, GBR, NZL

Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20370801

- (TS//SI//REL) Only R&T Analysts can submit QUANTUMTHEORY Tasking to the QUANTUM team. TOPI Analysts can submit QUANTUMNATION Tasking through Target Profiler. The biggest difference is QUANTUMTHEORY deploys a stage1 implant called VALIDATOR (soon to be COMMONDEER) and QUANTUMNATION deploys a stage0 implant called SEASONEDMOTH (SMOTH). SMOTHs die within 30 days of deployment unless requested to extend the life.

- (TS//SI//REL) This presentation does not cover FAA QUANTUM, but if you identify an active selector, compare the SIGAD in Marina to the SIGAD on the GO QUANTUM wiki page to see if FAA QUANTUM is an option.

- (TS//SI//REL) This presentation is geared towards targets seen at US-[redacted]. If you are unfamiliar with this SIGAD, it is equivalent to a TS//NF SIGAD that cannot be mentioned in this PowerPoint. You can contact the POC of this brief for more information.

Web Browsing (Exploit with QUANTUM man-on-the-side)

- The concept
  - QUANTUM is a man-on-the-side capability. If your target has a selector that is active in the last 14 days, vulnerable to the QUANTUM technique, and seen by an SSO site that has QUANTUM capabilities, then there might be the opportunity to detect that communication in real-time and piggy back with the requested content back into the target's network and implant the host.
  - QUANTUMTHEORY can be used only if a TAO Project is set up (must coordinate with your R&T Analyst)
  - QUANTUMNATION can be used regardless of a TAO Project (TOPI does the tasking in Target Profiler)
  - The biggest difference is QUANTUMTHEORY deploys a stage1 implant called VALIDATOR (soon to be COMMONDEER) and QUANTUMNATION deploys a stage0 implant called SEASONEDMOTH (SMOTH). SMOTHs die within 30 days of deployment unless requested to extend the life. The exploit technique is the same.

What is QUANTUM?

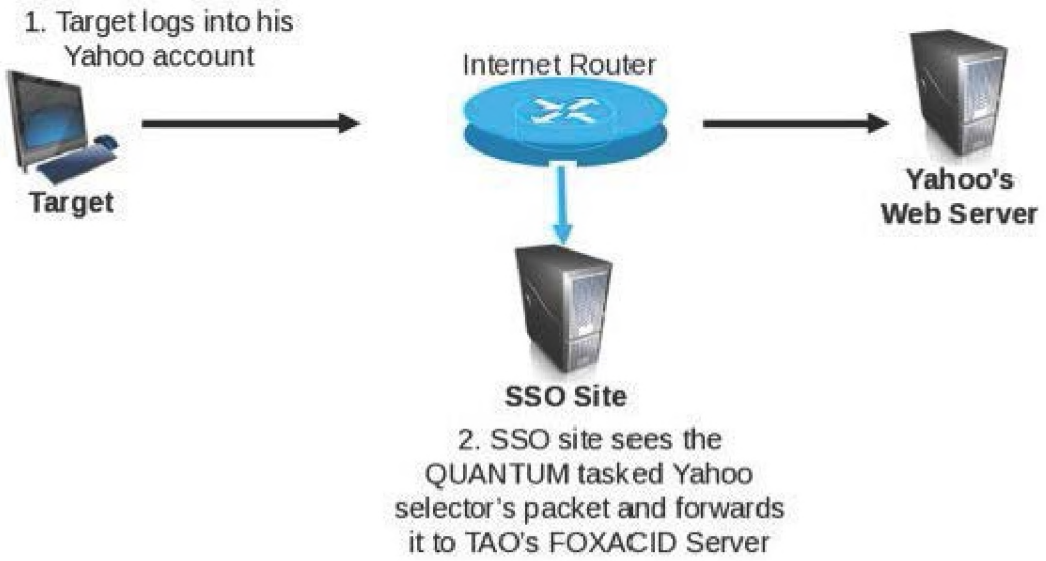
QUANTUM Generic Animation – High Level of How It Works

What is QUANTUM?

QUANTUM Generic Animation – High Level of How It Works

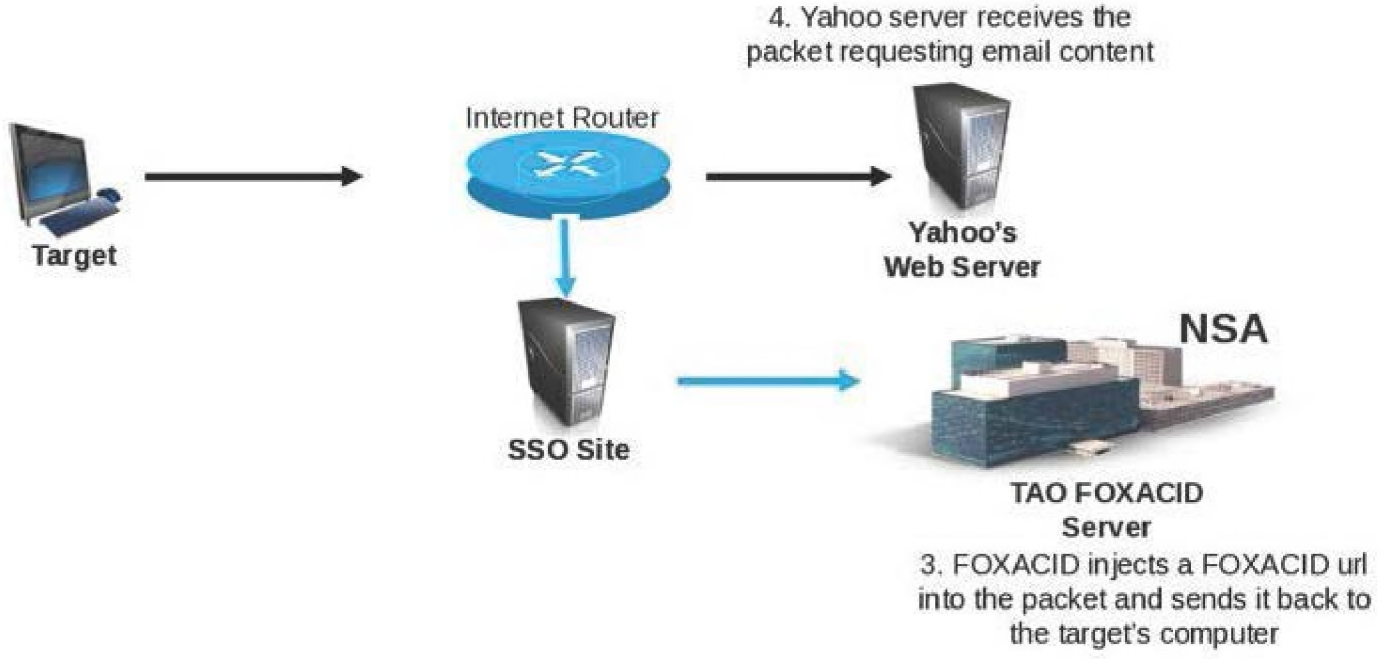
What is QUANTUM?

QUANTUM Generic Animation – High Level of How It Works



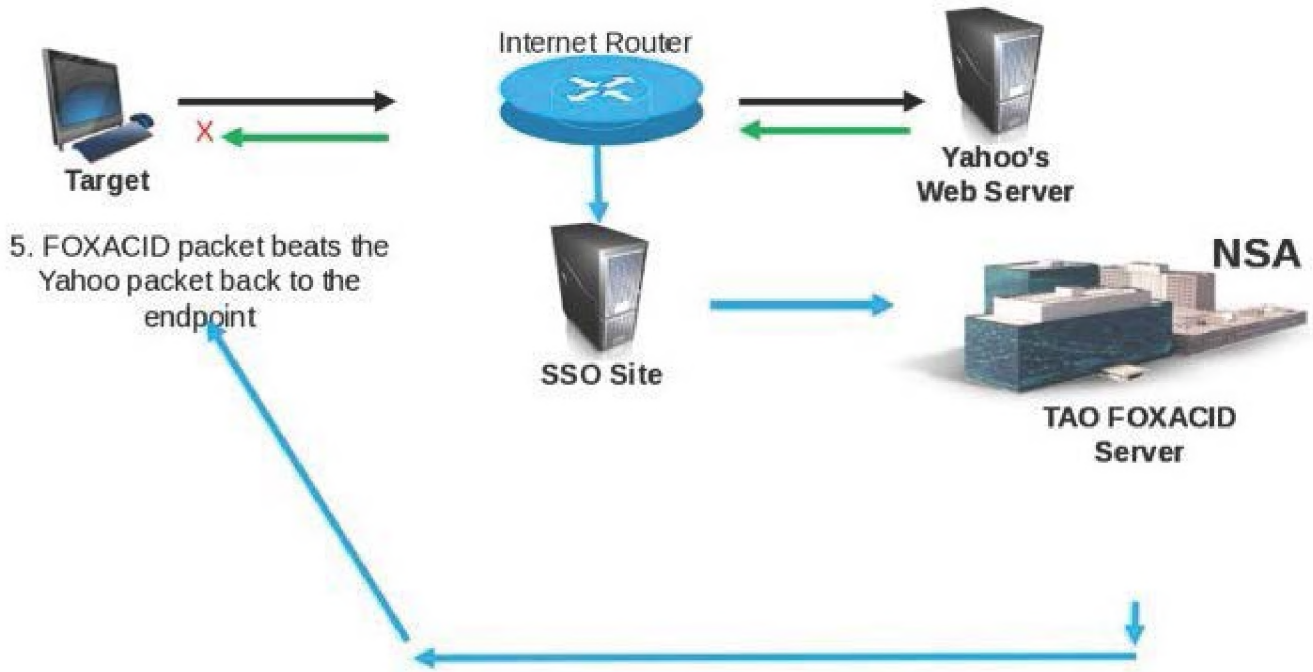
What is QUANTUM?

QUANTUM Generic Animation – High Level of How It Works



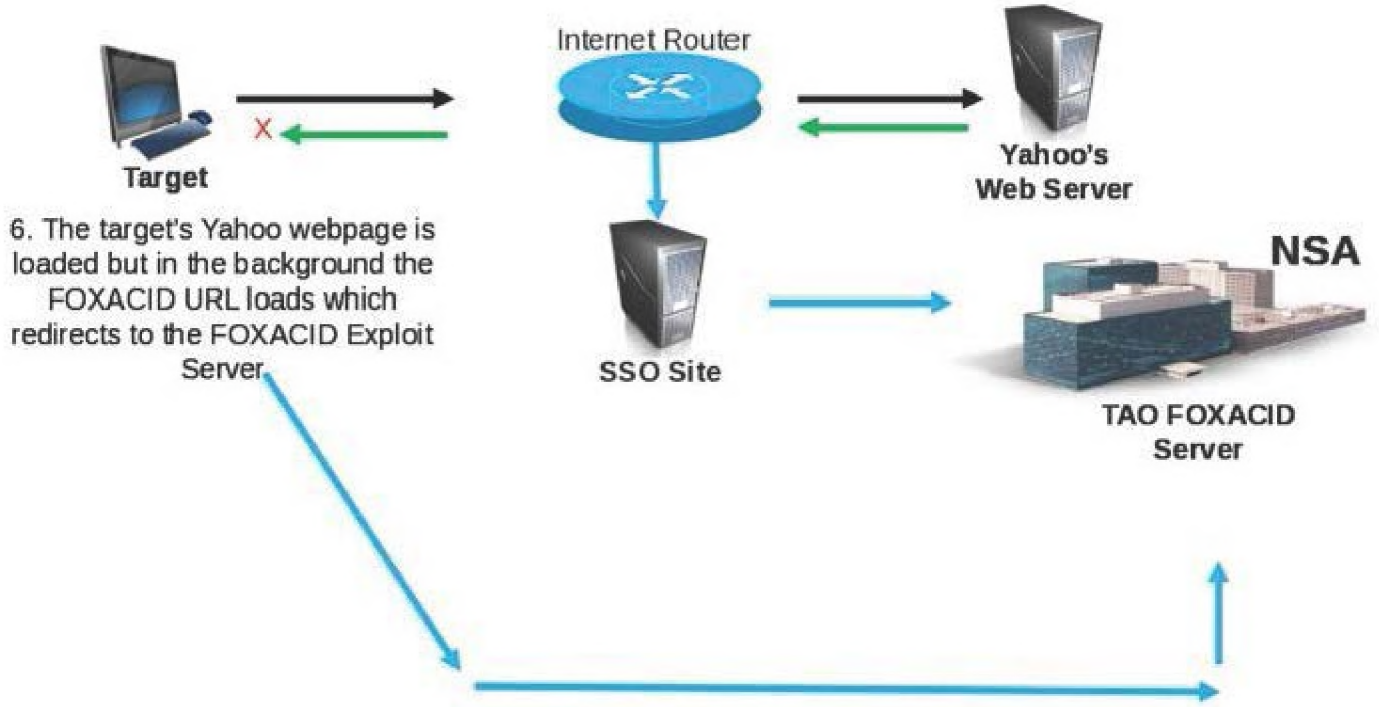
What is QUANTUM?

QUANTUM Generic Animation – High Level of How It Works



What is QUANTUM?

QUANTUM Generic Animation – High Level of How It Works



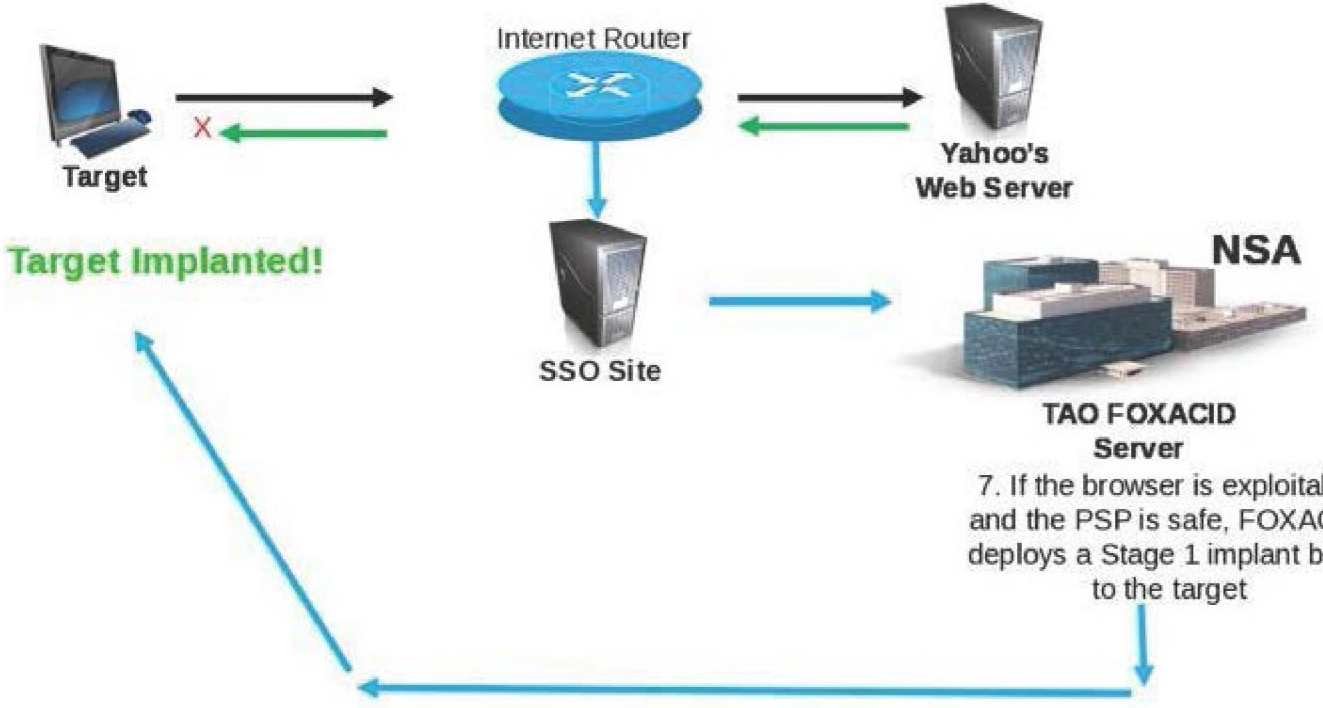
What is QUANTUM?

QUANTUM Generic Animation – High Level of How It Works

7. If the browser is exploitable and the PSP is safe, FOXACID deploys a Stage 1 implant back to the target

What is QUANTUM?

QUANTUM Generic Animation – High Level of How It Works



QUANTUM Capabilities – NSA

(TS//SI//REL) NSA QUANTUM has the *greatest* success against <yahoo>, <facebook>, and Static IP Addresses. New QUANTUM realms are often changing, so check the GO QUANTUM wiki page or the QUANTUM SpySpace page to get more up-to-date news.

NSA QUANTUM is capable of targeting the following realms:

- IPv4_public
- alibabaForumUser
- doubleclickID
- emailAddr
- rocketmail
- hi5Uid
- hotmailCID
- linkedin
- mail
- mailruMrcu
- msnMailToken64
- mailruMrcu
- msnMailToken64
- qq
- facebook
- simbarUuid
- twitter
- yahoo
- yahooBcookie
- ymail
- youTube
- WatcherID

QUANTUMTHEORY – GCHQ

If a Partnering Agreement Form (PAF) is set up with GCHQ for the CNO project, then the R&T Analyst can utilize GCHQ QUANTUMTHEORY to include additional capabilities such as:

- ALIBABA
- AOL
- BEBO_EMAIL
- DOUBLE_CLICK
- FACEBOOK_CUSER
- GOOGLE_PREFID
- GMAIL
- HI5
- HOTMAIL
- LINKEDIN
- MAIL_RU
- MICROSOFT_MUID
- MICROSOFT_ANONA
- RAMBLER
- RADIUS
- SIMBAR
- TWITTER
- YAHOO_B
- YAHOO_L/Y
- YANDEX_EMAIL
- YOUTUBE
- IP Address

More information on: https://wiki.gchq/[redacted]/QUANTUM_BISCUIT

If you cannot get to the link try: http://[redacted]

QUANTUM SIGDEV – QFDs

(TS//SI//REL) Find all Selectors associated to your target (Yahoo, Yahoo B Cookies, Facebook, Hotmail, etc) using Marina, NSA or GCHQ QFDs.

NSA SATC QFDs:

ALTEREGO QFD:

GCHC

Queried Selector	Alternate Selector	Queried Selector Degree	Alternate Selector Degree	Intersection	Score (1-100)
[redacted]<itue.164>	[redacted]<facebook>	4	5	2	40
[redacted]<itue.164>	[redacted]<imsi>	6	2	2	60
[redacted]<itue.164>	[redacted]<yahoo>	67	439	61	59

DOGCOLLAR QFD:

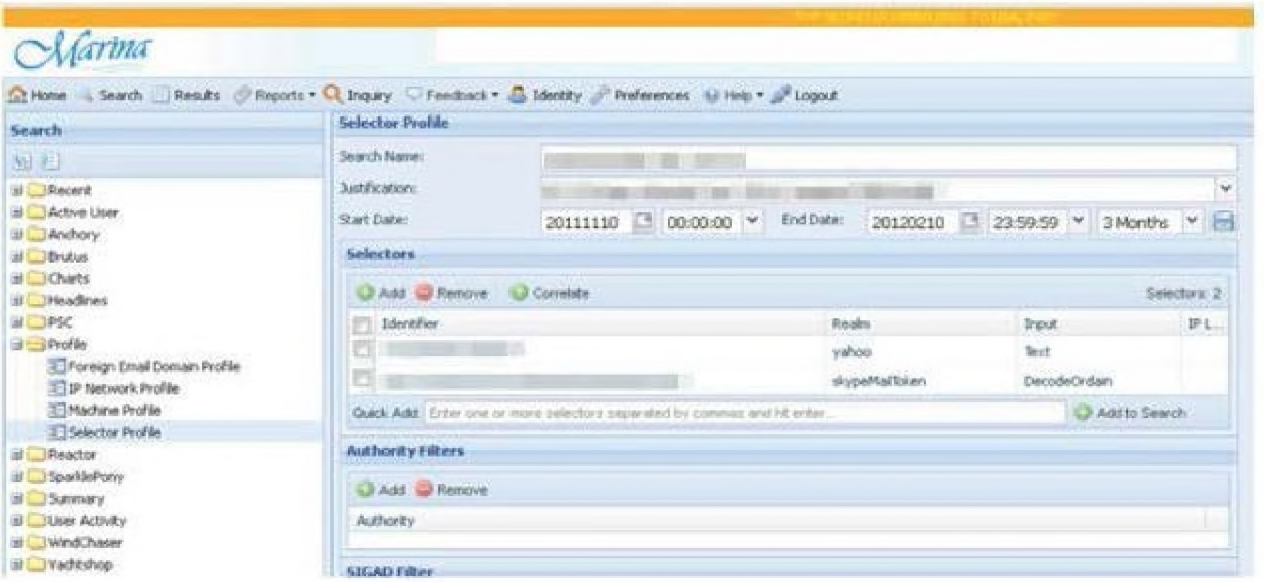
Selector	Type	Enrichment Value	Observations	First Seen Date	Last Seen Date
[redacted]<facebook>	DISPLAY_NAME	[redacted]	429	2012/05/24	2013/03/27

Skip to Step 5 once you have all of your selectors…

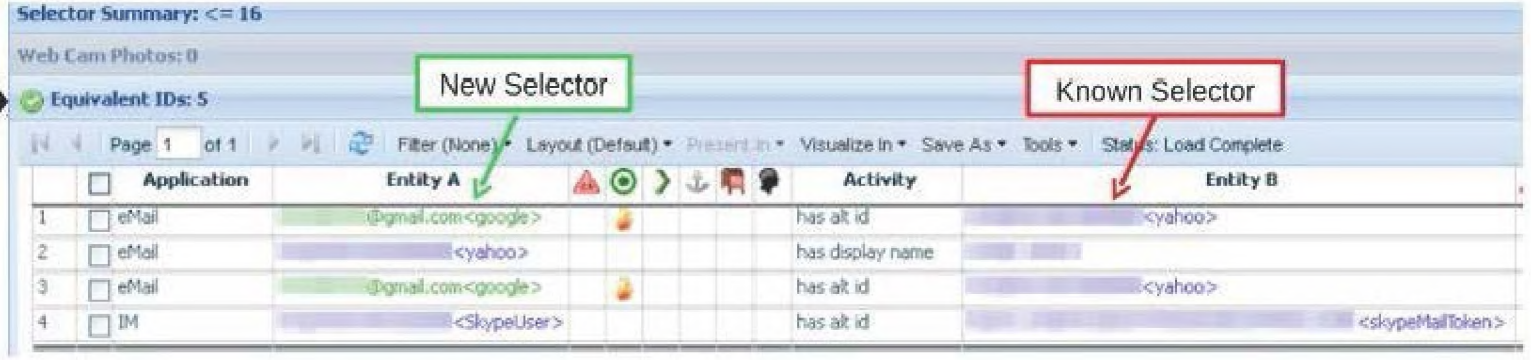
QUANTUM SIGDEV – Marina

Step 1: **Skip to Step 5 if you used the QFDs to identify alternate selectors**

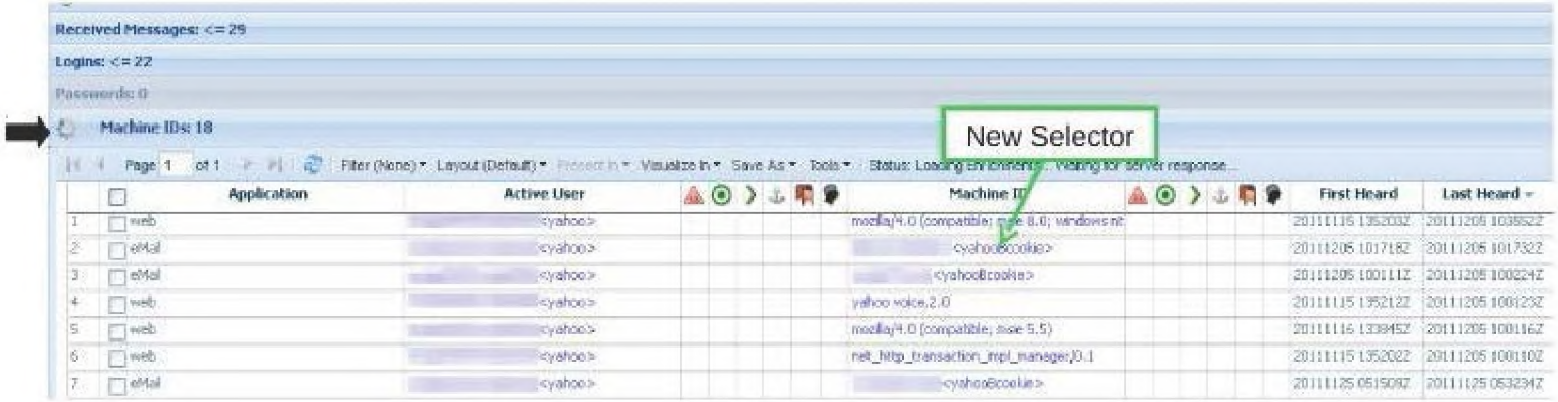
4 (TS//SI//REL) If you do not use the GCHQ or NSA QFDs you can use Marina. Run a Marina *Selector/Identifier Profile (Federated)* search for a 3 month range to look for additional selectors.



4 (TS//SI//REL) Once the query finishes, look at the *Equivalent IDs* section. This will show you other selectors that your target is using. This is determined by linking content (logins/email registrations/etc). It is worth verifying that these are indeed selectors associated to your target. NSA QUANTUM works best against <yahoo> and <facebook>. Although, it is worth making note of a <gmail> selector for possible GCHQ QUANTUM support or for your own notes.

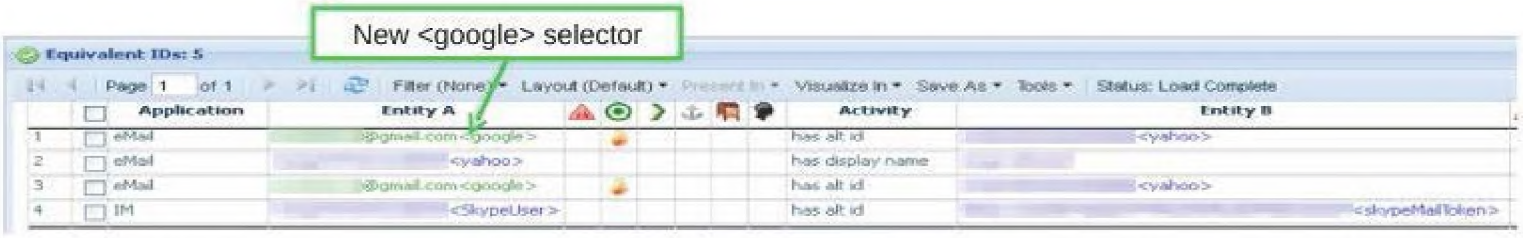


4 (TS//SI//REL) If your search was on a <yahoo> email address, then click on Machine IDs and look for a recent <yahooBcookie>. YahooBcookie's are unique to a specific computer and can hold other <yahoo> addresses that are being logged into on that computer as long as the user does not clear browser cookies. If you see multiple <yahooBcookie> pick the most recent *Last Heard* date. Also higher the *Num Heard* is, the more likely that selector does not change.



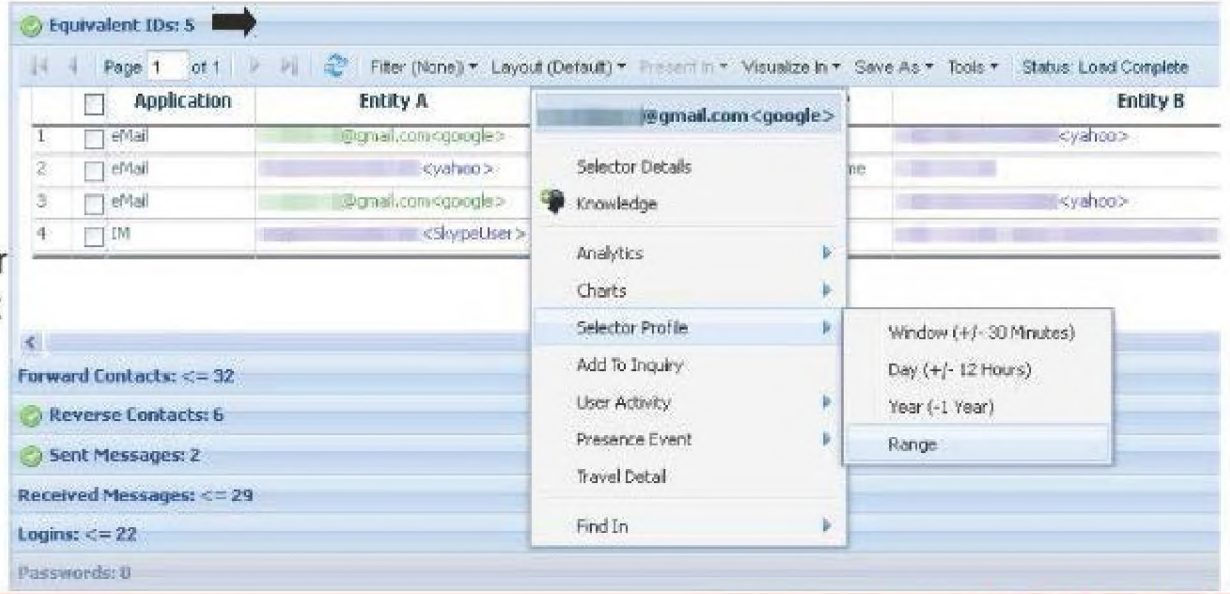
Unique Selectors Found:

1. [redacted]<yahoo> **(Known Selector)**
2. [redacted]@gmail.com<google> **(New Selector)**
3. [redacted]<yahooBcookie> **(New Selector)**

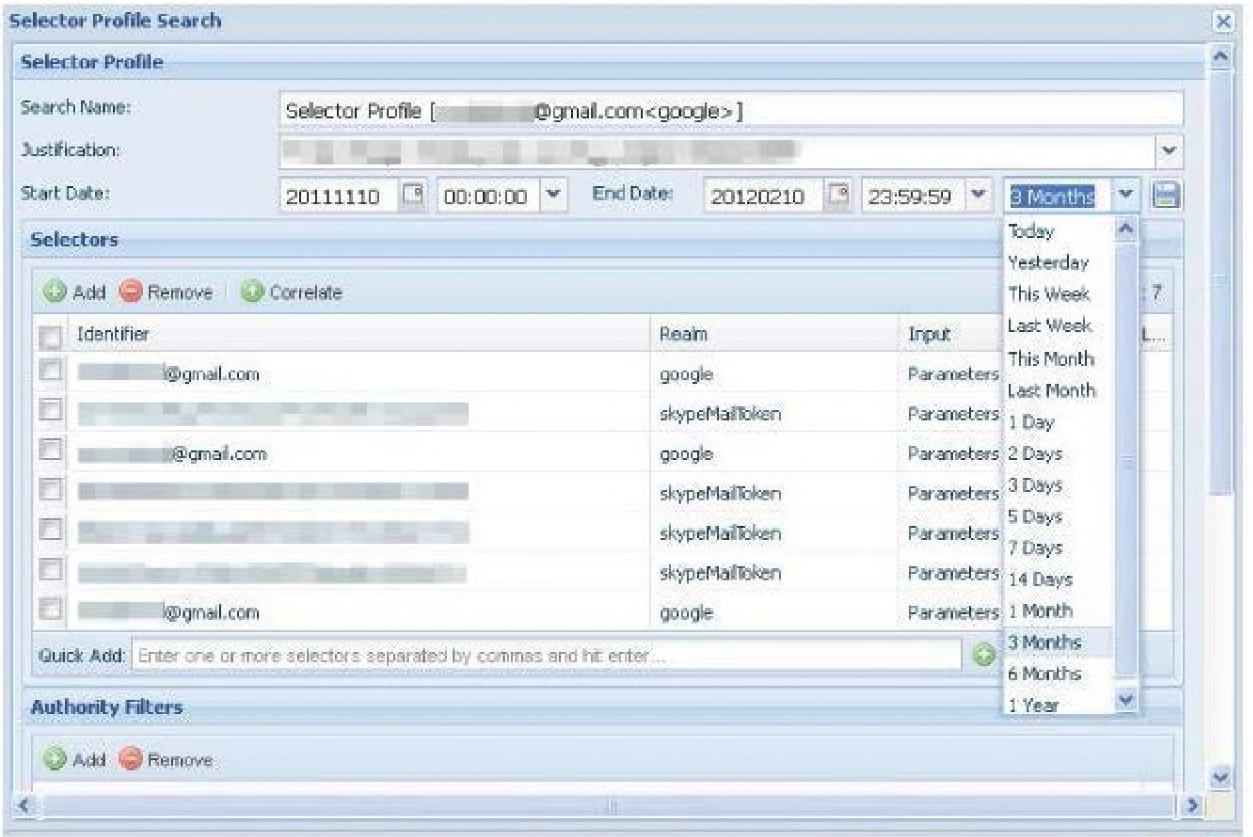


1. (TS//SI//REL) Since [redacted]@gmail.com<google> is a new selector, you will want to do a Marina Selector Profile query on it to see if there are additional accounts associated to the target. Remember NSA QUANTUM cannot target the <google> selector.

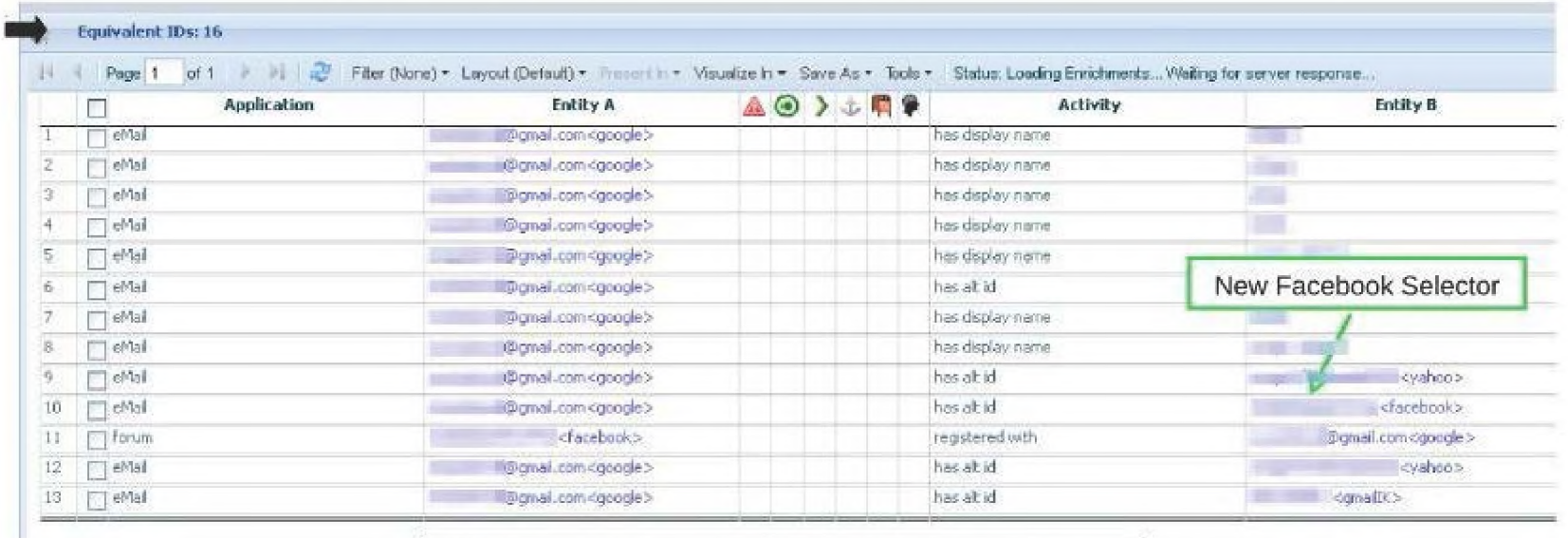
2. (TS//SI//REL) You can do this by clicking on the selector, scroll down to Selector Profile, and click Range.



4 (TS//SI//REL) Change the query to search for the last 3 Months and click SUBMIT



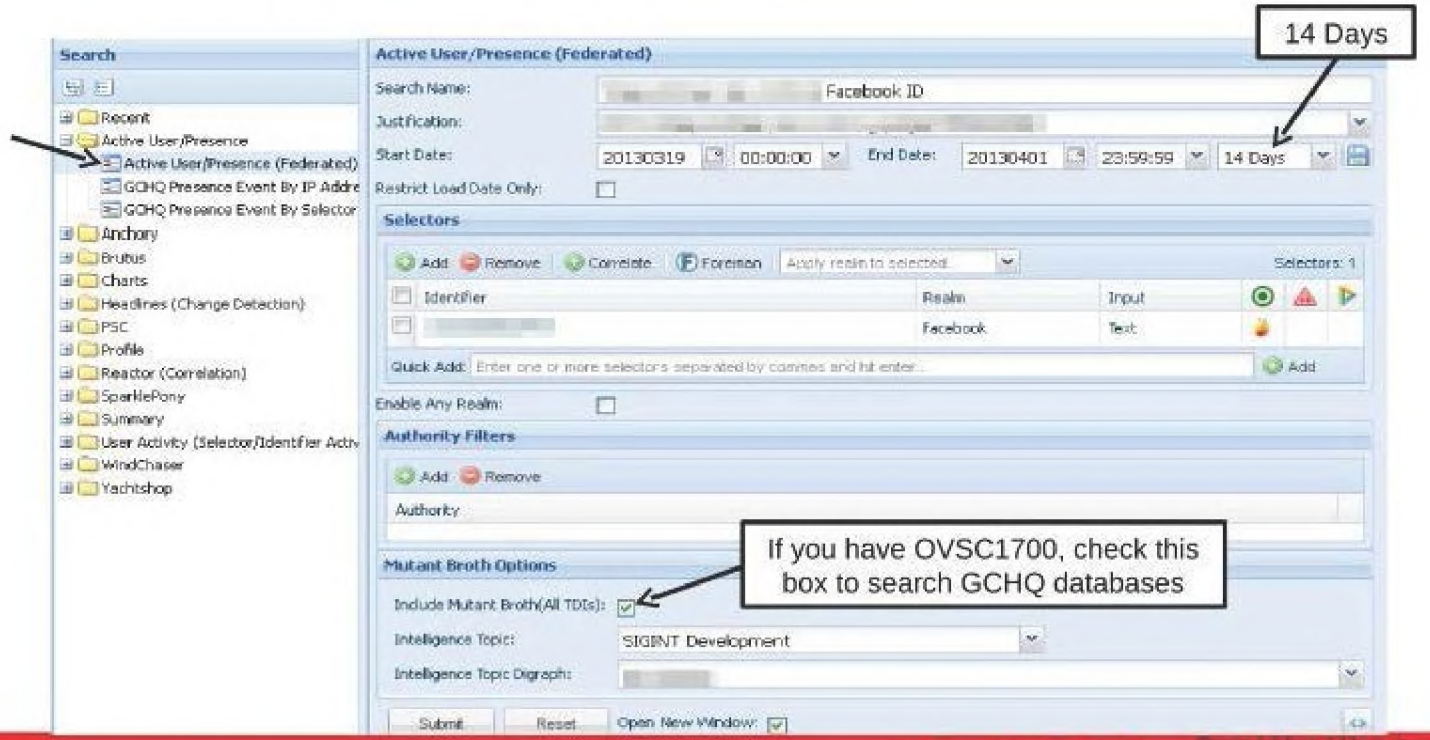
4 (TS//SI//REL) Once the query finishes, look at the Equivalent IDs section and make note of any new <yahoo>, <hotmail>, <yahooBcookie>, and <facebook> selectors and do the same process to identify additional selectors.



All Unique Selectors Found From Both Searches:

1. [redacted]<yahoo> **(Known Selector)**
2. [redacted]@gmail.com<google> **(New Selector)**
3. [redacted]<yahooBcookie> **(New Selector)**
4. [redacted]<facebook> **(New Selector)**

1. (TS//SI//REL) Once you have a list of your selector(s), you will want to look at each one separately to check for the likelihood of successfully exploiting your target via NSA QUANTUM. We are checking to see if the target itself is seen at US-[redacted] and if it is active.
2. (TS//SI//REL) First we want to run a Marina *Active User/Presence (Federated)* search on [redacted]<facebook> for the past 14 days.



- (TS//SI//REL) You will either have results or not have results. The key is to look at the SIGAD for the results and if the SIGAD is capable of doing QUANTUM then you most likely have a vulnerable target! To check for SIGADs that NSA and GCHQ QUANTUM can target, type GO QUANTUM in your browser. If GCHQ QUANTUM is needed, then work with your R&T Analyst to follow the appropriate steps on the wiki to set up a PAF.

- (TS//SI//REL) You will want to look at the Marina results and make note of the most frequent SIGAD/IP CIDR for each *Active User/Presence (Federated) query*

1) Selector

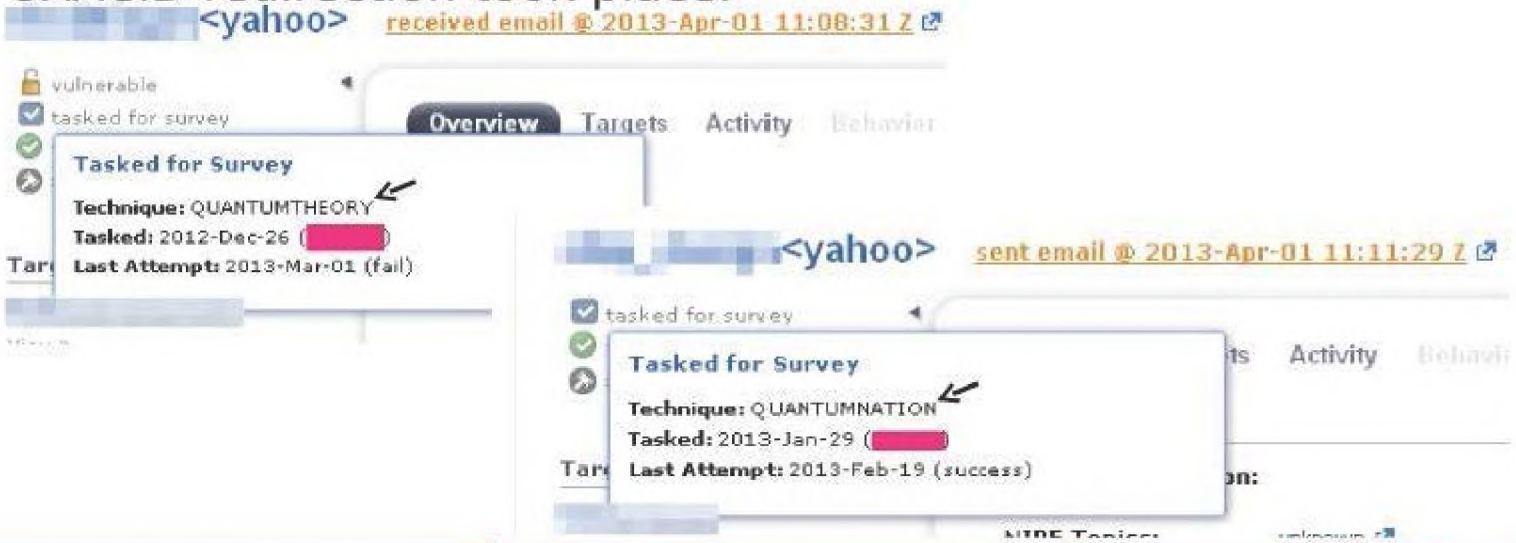
a) *SIGAD*

b) *Active User IP CIDR* – The CIDR will be added to the TLN's Whitelist.

-A TLN's Whitelist is a list containing the IP CIDRs your target uses. It is where the FOXACID server will only continue with exploitation if the external IP Address of the target/redirection is on the Whitelist for the TLN your R&T Analyst requests.

Is My Selector Tasked for QUANTUM?

If you sent your R&T analyst a selector to task for QUANTUMTHEORY and you want to see if it has been tasked yet, you can enter the selector in Target Profiler and if you see “tasked for survey” and the Technique to be QUANTUMTHEORY or QUANTUMNATION then it is tasked! You can also see when the last FOXACID redirection took place.



QUANTUMNATION

QUANTUMNATION uses new TAO CNE tradecraft and automation to drive broad scale initial access, specifically an SSG cloud-analytic to identify selectors in SSO passive collection that are viable for end-point access, and the use of lightweight CNE implants to obtain initial access and survey data delivered to the TOPI offices via corporate SIGINT repositories. For More Information on QUANTUMNATION check the QUANTUMNATION wiki page

Target Profiler now shows if a selector is vulnerable to a QUANTUM exploit. If your target is valid for QUANTUMNATION, A "Vulnerable" link in Target Profiler will appear. Simply click the link that sends an email to request QUANTUMNATION tasking.

Note: QUANTUMNATION and standard QUANTUM tasking results in the same exploitation technique. The main difference is QUANTUMNATION deploys a stage 0 implant and is able to be submitted by the TOPI. Any ios device will always get VALIDATOR deployed.

- (TS//SI//REL) Once you have a selector, SIGAD, and IP CIDR, you are ready to start the process for a FOXACID TLN and Tag request.
- (TS//SI//REL) Depending on the teams, either an R&T analyst or the Branch Chief can create a TLN (Twisty Lobby Number). Contact your Branch Chief for information on creating a TLN for each selector you want to target.
- (TS//SI//REL) Note: You will need 1 TLN and 1 FOXACID Tag per selector you task with QUANTUM.

Step 8:

- (TS//SI//REL) Once you have a TLN, you will need to submit a FOXACID Tag request.
- (TS//SI//REL) Go to https:/ .nsa/cgi-bin/ and fill out the appropriate information in the top and within the body of the ticket update this information accordingly. Here is an example:
  - CT or Non-CT: Non-CT
  - Second Party/Partnering: No
  - Country Region/Type:
  - FISA Target: No
  - Type of Op: QUANTUM
  - Utilizing WPTT: No
  - Project Name:
  - TLN: 12345 **Insert Your TLN**
  - IP Range: **Insert Your Active User IP CIDR / WHITELIST**
  - MAC Addresses: Unknown
  - Payload Requested: Val
  - Start Date: 20130401
  - POCs:
  - MSQ Support: No

- (TS//SI//REL) Once the ticket is completed, you will receive an email with the FOXACID Tag for your TLN.
- (TS//SI//REL) Go to https://[redacted].nsa.ic.gov[redacted]/index.php and fill out the appropriate information in the form to task your selector and tag for QUANTUM.
- (TS//SI//REL) Once your selector is tasked for QUANTUM you will see the status changed to complete.
- (TS//SI//REL) The last step it to monitor the TLN in FOXSEARCH https://[redacted].nsa[redacted] to look for redirections and update the plugins or WHITELIST if needed.
- (TS//SI//REL) De-task your QUANTUM request when you hook your target!

- If you have any questions or comments about this presentation, please send an email to [redacted] at [redacted]@nsa.ic.gov