



# Email Address vs User Activity

24 June 2009

Derived From: NSA/CSSM 1-52  
Dated: 20070108  
Declassify On: 20291123

DERIVED FROM: NSA/CSSM 1-52



# Email Addresses

- The Email Address search allows you to search on:
  - Full Email Address
    - Do not search on/wildcard JUST the username, always include a specific domain
    - Foreign-hosted domains (e.g. @cnc.cn)
- The query searches within bodies of emails, webpages and documents for....(you guessed it)...Email Addresses
  - To, From, CC, BCC lines..
  - “Contact Us” pages on websites
  - Signature blocks



# Email Address

- Email Addresses are found in many parts of traffic

A screenshot of a network analysis tool's interface showing an email header. The tool has three tabs: "DNI Display" (selected), "Raw Data", and "DNI Format". The email header fields are: Subject: RE: Malaysia Tax; From: [redacted]; To: [redacted]; Cc: [redacted]; Date: Tue Jun 23 12:41:25 GMT 2009. A red oval highlights the From, To, and Cc fields. Below the header, a file attachment is visible: "01.jpg (12018 bytes)".

| DNI Display   Raw Data   DNI Format |                              |
|-------------------------------------|------------------------------|
| Subject:                            | RE: Malaysia Tax             |
| From:                               | [redacted]                   |
| To:                                 | [redacted]                   |
| Cc:                                 | [redacted]                   |
| Date:                               | Tue Jun 23 12:41:25 GMT 2009 |
| 01.jpg (12018 bytes)                |                              |

XKEYSCORE has picked up traffic with email addresses in it..



# Email Address

DNI Display Raw Data DNI Format

Subject: **RE: Malaysia Tax**

From: [REDACTED]

To: [REDACTED]

Cc: [REDACTED]

Date: Tue Jun 23 12:41:25 GMT 2009

Attachments: @image001.jpg (12013 bytes);

X-KEYSCORE C2C Session Viewer

Session 19 of 18

| Datetime            | Case Notation   | From IP                         | To IP                      | From Port | To Port | Protocol | Len |
|---------------------|-----------------|---------------------------------|----------------------------|-----------|---------|----------|-----|
| 2009-06-23 12:41:28 | PRPA07550000000 | 198. [REDACTED] (United States) | 219. [REDACTED] (Malaysia) | 39247     | 25      | tcp      | 486 |

Session Header (3) Attachments (5) **Meta (10)**

attribute\_info.txt **email\_addresses.txt** tech.html application\_id.xml appproc.asdf xks\_snippet.txt phone\_number.html

fingerprints.xml user\_activity.xml ip\_lc\_trie.txt

email\_addresses.txt FORMATTER AUTO

Using TXT formatter

[REDACTED]

XKEYSCORE parses out everything it 'thinks' is an email address, so don't be fooled by mis-hits



# Creating Email Address Queries

- Enter usernames and domains into query

Search: Email Addresses

Query Name:

Justification:

Additional Justification:

Miranda Number:

Datetime:  Start:   Stop:

Email Username:

@Domain:

Subject:

Multiple usernames from SAME domain can be OR'd



# Creating Email Address Queries

- BE VERY CAREFUL of OR'ing domains

Search: Email Addresses

Query Name:

Justification:

aqi in iran sample

Additional Justification:

Miranda Number:

Datetime:

1 Day

Start:

2009-06-23

00:00

Stop:

2009

Email Username:

badguy or baddude1 or badguysemail

@Domain:

yahoo.com or hotmail.com

Subject:

When working with multiple domains, create separate Email Address queries for each. i.e. Group your queries by domain names.



Multiple domains means either badguy@yahoo.com or badguy@hotmail.com. Are both your targets?



# Email Address

- Sample Search: baku@huawei.com

## Search: Email Addresses

Query Name:

Justification:

Additional Justification:

Miranda Number:

Datetime:

Start:

00:00

St

Email Username:

@Domain:



# Email Address

■ Email Addresses are found in many parts of traffic

DNI Display Raw Data DNI Format

+ HTTP Header Information

Content Type: HTTP/HTML

Services

Fax: 0061-2-94118533

**Vienna, Austria**

Ezone Office Building, 4th Floor/ Top 7, Ernst-Melchior-Gasse 20, 1020 Vienna, Austria

Tel: 0043-1-31199999

**Baku, Azerbaijan**

Caspian Plaza Centre ,block 610-611, J.Jabbarly St., Baku Azerbaijan, Az1065

Tel: 0099412-510-5644/5744/5844

Fax: 0099412-510-5944

E-mail: [baku@huawei.com](mailto:baku@huawei.com)

Results here are from someone viewing a website that contained the email address

**Bahrain, Bahrain**  
Building 647, Road 2811Seef District 428Kingdom of Bahrain

Tel: 00973-17568708

Fax: 00973-17568701

**Bahrain, Bahrain**  
Villa NO.1, Mohamedia Garden, Gate NO.36,Road No.3431,Block No.334,Bahrain

Tel: 00974-3443296/00973-9580085

**Dhaka, Bangladesh**

R M Centere(2nd Floor),101, gulshan Avenue Gulshan Model

Tel: Dhaka 1213 Bangladesh

**Minsk, Belarus**

Korolya str.,51, floor-2, office-28, Minsk,Belarus

Tel: 00375 17 2049002



# User Activity Query



- User Activity query is based on APPROC collection (such as chat, webmail, etc)
- Allows more flexible search criteria than Email Address query
  - Can search on: Cookies, numeric logins (e.g. web forums & OSN), VoIP selectors, webcam first images, Webmail profile information from registration (birthdays), general usernames



# Creating User Activity Queries

- The fields in a User Activity query can be confusing

Datetime:  Start:  11:00 Stop: 20

Search For:

Search Value:

Realm:

Attribute Type:

Attribute Value:

Activity:

Source:

IP Address:  From

Enter target selectors/identifiers here:

- Phone No
- Cookie
- Username/EMAD (then add REALM)
-



# Creating User Activity Queries

- The fields in a User Activity query can be confusing

| Search For | Search Value     | Attribute Type | Attribute Value  |
|------------|------------------|----------------|--|
| username   | [REDACTED]@yahoo | communicants   | [REDACTED] saifdes ziad197                                   |
| username   | [REDACTED]@yahoo | contact_list   | 0920273966 999999 a_salty a_t_love_me a                      |
| username   | [REDACTED]@yahoo | direction      | server-to-client   |
| username   | [REDACTED]@yahoo | from           | [REDACTED]   |
| username   | [REDACTED]@yahoo | previous_user  | Notice partial email addresses in the "Search Value" field.. |
| username   | [REDACTED]@yahoo | raw_metadata   |  |
| username   | [REDACTED]@yahoo | to             | [REDACTED]   |
| username   | [REDACTED]@yahoo | user_realm     | emailAddr  |
| username   | [REDACTED]@yahoo | yahoo          | [REDACTED]   |
| username   | [REDACTED]       | emailAddr      | [REDACTED]@yahoo   |
| username   | [REDACTED]@yahoo | app_provider   | YMSG   |

# Creating User Activity Queries



- Scenario:

You have a target's email address:

- [REDACTED]@hotmail.com
  - Known: One email address
  - Unknown: Alternate ID's, IPs, Location, Photo, etc... (lots of stuff)

Where do we begin?



# I want to....

- I have an Email Address and want to see if it's being collected?
  - Do an **Email Address** query on username and domain

|                 |   |
|-----------------|---|
| Email Username: | <input type="text" value="baku"/>       |
| @Domain:        | <input type="text" value="huawei.com"/> |

- Do a **User Activity** query on the email address in the "Selector Value"

|               |   |
|---------------|---|
| Search Value: | <input type="text" value="baku@huawei*"/> |
|---------------|---|



# I want to....

- I have a Cookie and want to see what other accounts access this computer
  - Do TWO separate **User Activity** query on the cookies

1.

Attribute Value:

| Search For | Search Value     | Attribute Type | Attribute Value |
|------------|------------------|----------------|-----------------|
| username   | [REDACTED]@yahoo | yahooBcookie   | dg8q0od4u0i4    |
| username   | [REDACTED]@yahoo | B_cookie       | dg8q0od4u0i4    |
| username   | [REDACTED]@yahoo | B_cookie       | dg8q0od4u0i4    |
| username   | [REDACTED]@yahoo | yahooBcookie   | dg8q0od4u0i4    |
| username   | [REDACTED]@yahoo | yahooBcookie   | dg8q0od4u0i4    |
| username   | dg8q0od4u0i4     | B_cookie       | dg8q0od4u0i4    |
| username   | [REDACTED]@yahoo | B_cookie       | dg8q0od4u0i4    |
| username   | [REDACTED]@yahoo | B_cookie       | dg8q0od4u0i4    |
| username   | [REDACTED]@yahoo | yahooBcookie   | dg8q0od4u0i4    |
| username   | [REDACTED]@yahoo | yahooBcookie   | dg8q0od4u0i4    |
| username   | [REDACTED]@yahoo | B_cookie       | dg8q0od4u0i4    |

Brings back THESE results...

Notice redundancy.. So you MAY miss traffic if you select "B\_cookie" or "yahooBcookie" (don't know why)

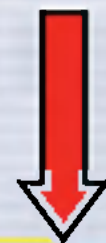


# I want to....

- I have a Cookie and want to see what other accounts access this computer
  - Do TWO separate **User Activity** query on the cookies

2.

Search value:



Brings back THESE results...

| Search For | Search Value  | Attribute Type | Attribute Value  |
|------------|---------------|----------------|------------------|
| username   | dg8q0od4u0li4 | yahoo          | [REDACTED]@yahoo |
| username   | dg8q0od4u0li4 | yahoo          | [REDACTED]@yahoo |
| username   | dg8q0od4u0li4 | yahoo          | [REDACTED]@yahoo |
| username   | dg8q0od4u0li4 | yahoo          | [REDACTED]@yahoo |
| username   | dg8q0od4u0li4 | yahoo          | [REDACTED]@yahoo |
| username   | dg8q0od4u0li4 | yahoo          | [REDACTED]@yahoo |
| username   | dg8q0od4u0li4 | yahoo          | [REDACTED]@yahoo |
| username   | dg8q0od4u0li4 | yahoo          | [REDACTED]@yahoo |
| username   | dg8q0od4u0li4 | yahoo          | [REDACTED]@yahoo |
| username   | dg8q0od4u0li4 | yahoo          | [REDACTED]@yahoo |

Notice redundancy.. So you MAY miss traffic if you select "B\_cookie" or "yahooBcookie" (don't know why)



# I want to....

- I have a Cookie and want to see what other accounts access this computer
  - Do a Marina query on the cookie as well (why not)?

Specify Date Range  to

(YYYYMMDD [hhmmss]):

for User Activity by...  that...  the value(s)...

when it is reached, return...  ? (100,000 raw metadata result limit)

where value is...  active user ?  in user\_a or user\_b column ?

filter by...     ?

---

\*Enrichment Options:  All  None  Selected

Query Justification (optional):





# I want to....

- I have a Cookie and want to see what other accounts access this computer
  - Do a Marina query on the cookie as well (why not)?

| USER_A     | ACTIVITY                     | USER_B                      | COOKIE                      |
|------------|------------------------------|-----------------------------|-----------------------------|
| [REDACTED] | <yahoo> seen with machine ID | dg8q0od4u0li4<yahooBcookie> | dg8q0od4u0li4<yahooBcookie> |
| [REDACTED] | <yahoo> seen with machine ID | dg8q0od4u0li4<yahooBcookie> | dg8q0od4u0li4<yahooBcookie> |
| [REDACTED] | <yahoo> seen with machine ID | dg8q0od4u0li4<yahooBcookie> | dg8q0od4u0li4<yahooBcookie> |



# I want to....

- So let's put the cookie query all together...
  - Between Marina and XKS, I should have an idea of all the accounts..
    - Results pulling on dg8q0od4u0li4 as a Search Value

| Search For | Search Value  | Attribute Type | Attribute Value             |
|------------|---------------|----------------|-----------------------------|
| username   | dg8q0od4u0li4 | yahoo          | [REDACTED]@yahoo            |
| username   | dg8q0od4u0li4 | yahoo          | [REDACTED]@yahoo            |
| username   | dg8q0od4u0li4 | raw metadata   | <commEventSummary> <appProc |

- Plus my Marina results

| USER_A            | ACTIVITY             | USER_B                      | COOKIE                      |
|-------------------|----------------------|-----------------------------|-----------------------------|
| [REDACTED]@yahoo> | seen with machine ID | dg8q0od4u0li4<yahooBcookie> | dg8q0od4u0li4<yahooBcookie> |
| [REDACTED]@yahoo> | seen with machine ID | dg8q0od4u0li4<yahooBcookie> | dg8q0od4u0li4<yahooBcookie> |
| [REDACTED]@yahoo> | seen with machine ID | dg8q0od4u0li4<yahooBcookie> | dg8q0od4u0li4<yahooBcookie> |

RESULTS: Three users on the a computer..



# I want to....

- I have an IP address and want to know what users/accounts are collected in that network? (I.E. a Café's IP address, or mail/web server for an organization)

- Do an **Email Address** query on the IP address

|                 |   |
|-----------------|---|
| Email Username: | <input type="text"/>  |
| @Domain:        | <input type="text"/>  |
| Subject:        | <input type="text"/>  |
| IP Address:     | <input type="text" value="██████████"/> From <input type="button" value="v"/> |

- Do a **User Activity** query on the IP address

|                 |   |
|-----------------|---|
| Search For      | <input type="text"/>                    |
| Search Value    | <input type="text"/>                    |
| Realm           | <input type="text"/>                    |
| Attribute Type  | <input type="text"/>                    |
| Attribute Value | <input type="text"/>                    |
| Activity        | <input type="text"/>                    |
| Source          | <input type="text"/>                    |
| IP Address:     | <input type="text" value="██████████"/> |



# Moral of the story

- Email Address query looks for the @ symbol in traffic
- User Activity search allows you to query on more than just an email address