Email Address vs User Activity

24 June 2009
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 Addresses are found in many parts of traffic.

XKEYSCORE has picked up traffic with email addresses in it.
Subject: RE: Malaysia Tax

From: [Redacted]

To: [Redacted]

Cc: [Redacted]

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

Attachments: [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: 1 Day
Start: 2009-06-23 00:00
Stop: —

Email Username: badguy or baddude! or badguyemail
@Domain: yahoo.com
Subject: 

Multiple usernames from SAME domain can be OR’d
Creating Email Address Queries

BE VERY CAREFUL of OR’ing domains

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 Addresses are found in many parts of traffic.
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
The fields in a User Activity query can be confusing.

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.

<table>
<thead>
<tr>
<th>Search For</th>
<th>Search Value</th>
<th>Attribute Type</th>
<th>Attribute Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>username</td>
<td>@yahoo</td>
<td>communicates</td>
<td>saifdes ziad197</td>
</tr>
<tr>
<td>username</td>
<td>@yahoo</td>
<td>contact_list</td>
<td>966 999999 a_salty_a_f_1ove_hes a_</td>
</tr>
<tr>
<td>username</td>
<td>@yahoo</td>
<td>direction</td>
<td>server-to-client</td>
</tr>
<tr>
<td>username</td>
<td>@yahoo</td>
<td>from</td>
<td></td>
</tr>
<tr>
<td>username</td>
<td>@yahoo</td>
<td>previous_user</td>
<td></td>
</tr>
<tr>
<td>username</td>
<td>@yahoo</td>
<td>raw_metadata</td>
<td></td>
</tr>
<tr>
<td>username</td>
<td>@yahoo</td>
<td>to</td>
<td></td>
</tr>
<tr>
<td>username</td>
<td>@yahoo</td>
<td>user_realm</td>
<td></td>
</tr>
<tr>
<td>username</td>
<td>@yahoo</td>
<td>yahoo</td>
<td></td>
</tr>
<tr>
<td>username</td>
<td>@yahoo</td>
<td>emailAddr</td>
<td></td>
</tr>
<tr>
<td>username</td>
<td>@yahoo</td>
<td>app_provider</td>
<td></td>
</tr>
</tbody>
</table>

Notice partial email addresses in the “Search Value” field.
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:** baku  
  **@Domain:** huawei.com

- Do a User Activity query on the email address in the “Selector Value”

  **Search 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: dg8q0od4u0li4

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: `dg8q0dd4u0li4`

Brings back THESE results...

<table>
<thead>
<tr>
<th>Search For</th>
<th>Search Value</th>
<th>Attribute Type</th>
<th>Attribute Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>username</td>
<td>dg8q0dd4u0li4</td>
<td>yahoo</td>
<td>yahoo</td>
</tr>
<tr>
<td>username</td>
<td>dg8q0dd4u0li4</td>
<td>yahoo</td>
<td>yahoo</td>
</tr>
<tr>
<td>username</td>
<td>dg8q0dd4u0li4</td>
<td>yahoo</td>
<td>yahoo</td>
</tr>
<tr>
<td>username</td>
<td>dg8q0dd4u0li4</td>
<td>yahoo</td>
<td>yahoo</td>
</tr>
<tr>
<td>username</td>
<td>dg8q0dd4u0li4</td>
<td>yahoo</td>
<td>yahoo</td>
</tr>
<tr>
<td>username</td>
<td>dg8q0dd4u0li4</td>
<td>yahoo</td>
<td>yahoo</td>
</tr>
<tr>
<td>username</td>
<td>dg8q0dd4u0li4</td>
<td>yahoo</td>
<td>yahoo</td>
</tr>
<tr>
<td>username</td>
<td>dg8q0dd4u0li4</td>
<td>yahoo</td>
<td>yahoo</td>
</tr>
</tbody>
</table>

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)?
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)?

<table>
<thead>
<tr>
<th>USER A</th>
<th>ACTIVITY</th>
<th>USER B</th>
<th>COOKIE</th>
</tr>
</thead>
<tbody>
<tr>
<td>yahoo</td>
<td>seen with machine ID dg8q0od4u0li4</td>
<td>yahoo</td>
<td>dg8q0od4u0li4</td>
</tr>
<tr>
<td>yahoo</td>
<td>seen with machine ID dg8q0od4u0li4</td>
<td>yahoo</td>
<td>dg8q0od4u0li4</td>
</tr>
<tr>
<td>yahoo</td>
<td>seen with machine ID dg8q0od4u0li4</td>
<td>yahoo</td>
<td>dg8q0od4u0li4</td>
</tr>
</tbody>
</table>
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

<table>
<thead>
<tr>
<th>Search For</th>
<th>Search Value</th>
<th>Attribute Type</th>
<th>Attribute Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>username</td>
<td><code>dg8q0od4u0li4</code></td>
<td>yahoo</td>
<td></td>
</tr>
<tr>
<td>username</td>
<td><code>dg8q0od4u0li4</code></td>
<td>yahoo</td>
<td></td>
</tr>
<tr>
<td>username</td>
<td><code>dg8q0od4u0li4</code></td>
<td>raw metadata</td>
<td><code>&lt;commEventSummary&gt;</code></td>
</tr>
</tbody>
</table>

Plus my Marina results

<table>
<thead>
<tr>
<th>USER_A</th>
<th>ACTIVITY</th>
<th>USER_B</th>
<th>COOKIE</th>
</tr>
</thead>
<tbody>
<tr>
<td>[redacted]</td>
<td><code>seen with machine ID dg8q0od4u0li4&lt;yahooBcookie&gt;</code></td>
<td><code>dg8q0od4u0li4&lt;yahooBcookie&gt;</code></td>
<td><code>dg8q0od4u0li4&lt;yahooBcookie&gt;</code></td>
</tr>
<tr>
<td>[redacted]</td>
<td><code>seen with machine ID dg8q0od4u0li4&lt;yahooBcookie&gt;</code></td>
<td><code>dg8q0od4u0li4&lt;yahooBcookie&gt;</code></td>
<td><code>dg8q0od4u0li4&lt;yahooBcookie&gt;</code></td>
</tr>
<tr>
<td>[redacted]</td>
<td><code>seen with machine ID dg8q0od4u0li4&lt;yahooBcookie&gt;</code></td>
<td><code>dg8q0od4u0li4&lt;yahooBcookie&gt;</code></td>
<td><code>dg8q0od4u0li4&lt;yahooBcookie&gt;</code></td>
</tr>
</tbody>
</table>

RESULTS: Three users on the a computer..
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

- Do a User Activity query on the IP address
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