

Reconnaissance

User Agents:

Hypothesis:

User Agent Strings may provide insight into an adversary that they may not have intended to show.

Here are some questions to think about that may help as we conduct our hunt:

- What data sources (sourcetypes) are needed to view user agent strings?
 - When were specific user agent strings seen?
 - What IP addresses where user agent strings seen from?
 - Are any of the user agent strings anomalous? That is are there any that are excessively short or long or from systems that would be unexpected?
 - Focus your hunt in the month of August 2017
-
- We can start by searching the stream:http sourcetype, which is our web data captured off the wire, and look for all web traffic where the site referenced is our corporate web site www.froth.ly. We can then use the stats command and generate a count grouped by http_user_agent, the field name for user agent strings, and sort that output by count from largest to smallest.

```
index=botsv2 sourcetype=stream:http site=www.froth.ly  
| stats count by http_user_agent  
| sort - count
```

- After inspecting the results, we can find one result that seems foreign or unknown to us.
[Mozilla/5.0 \(X11; U; Linux i686; ko-KP; rv: 19.1br\) Gecko/20130508 Fedora/1.9.1-2.5.rs3.0 NaenaraBrowser/3.5b4](#)
- Upon further investigating about the User Agent, we find some non-Western European characters, a code of ko-KP and a browser we are not familiar with.
- If we search some of these less familiar values in the user agent string, we can find out that ko-KP is the browser language code for North Korea and when we search for NaenaraBrowser, we can see that it is a North Korean web browser.

```
Mozilla/5.0 (X11; U; Linux i686; ko-KP; rv: 19.1br) Gecko/20130508 Fedora/1.9.1-2.5.rs3.0 NaenaraBrowser/3.5b4
```



Naenara 3 on Fedora Linux

Here's detailed information about it:

Simplified readout

Clear, human readable descriptions of the software & platform

Simple Software String

[Naenara 3 on Fedora Linux](#)

Simple Sub-description

Simple Operating Platform

Software extras

Extra things this User agent announces.

Detected Addons

Software capabilities

Extra Info

[X11 Window System](#)

Extra Info Table

[Hardware Architecture: i686](#)

Software

Information about the web software

Software

[Naenara 3](#)

Software Name

[Naenara](#)

Software Name Code

[naenara](#)

Software Version

3

Software Version (full)

3.5b4

Layout Engine Name

[Gecko](#)

Layout Engine Version

20130508

Software Type

[browser -> web-browser](#)

Hardware Type

[computer](#)

Operating System

Information about the Operating System

Operating System

[Fedora Linux](#)

Operating System Name

[Linux](#)

Operating System Name Code

[linux](#)

Operating System Flavour

[Fedora](#)

Operating System Version

Operating System Version (full)

Operating System Frameworks

Misc

Miscellaneous Information


Operating Platform

- Now that we have identified a suspicious user agent, we can use the stats command and look for source and destination pairs that are referencing this string. We see three external IPs using this user agent string targeting two distinct systems at Frothly.

| | | | | |
|--|---|--------------|-----------------|-----------|
| index=botsv2 sourcetype=stream:http "Mozilla/5.0 (X11; U; Linux i686; ko-KP; rv: 19.1br) Gecko/20130508 Fedora/1.9.1-2.5.rs3.0 NaenaraBrowser/3.5b4" stats count by src dest | | | during Aug 2017 | 🔍 |
| ✓ 83 events (8/1/17 12:00:00.000 AM to 9/1/17 12:00:00.000 AM) No Event Sampling ▾ Job ▾ ■ ↶ ↷ ⏏ ⏴ ⏵ ⚙ Smart Mode ▾ | | | | |
| Events Patterns Statistics (3) Visualization | | | | |
| 20 Per Page ▾ ↗ Format Preview ▾ | | | | |
| src ▾ | ✎ | dest ▾ | ✎ | count ▾ ✎ |
| 136.0.0.125 | | 172.31.4.249 | | 8 |
| 136.0.2.138 | | 172.31.4.249 | | 24 |
| 85.203.47.86 | | 172.31.6.251 | | 51 |

- Upon researching the Asset Center, we can confirm that 172.31.4.249 is a DNS server called 'gacrux'.
- Using OSINT tools to dig deeper, we find that this server is hosted using RIPE.NET which is a European Coordination Center for handing out IP addresses. Now using Cymru, we can find the ASN connected with RIPE.NET.

Team Cymru IP to ASN Lookup v1.0


[\[Team Cymru\]](#)
[\[ASN Lookup docs\]](#)
[\[IP Information\]](#)

Family: ☒ IPv4 ☐ IPv6 Methods: ☒ whois ☐ peer-whois
Flags: ☐ prefix ☐ cc ☐ registry ☐ allocated ☐ nottruncate ☐ verbose

Insert your IP or ASN in the textbox above.

IPv4 [OPTIONAL COMMENT]
Eg. '4.2.2.2 2004-12-10 11:33:21 GMT'

AS#
Eg. 'AS23028'

IPv6 [OPTIONAL COMMENT]

```

--- snip snip ---
2001:5c0:8fff:ffe::ff6 2004-12-10 11:32:01 GMT
2001:5c0:8fff:ffe::ff7 2004-12-10 11:33:21 GMT
--- snip snip ---

```

Both IPv4 and IPv6 addresses are supported.
However, only one address family is permitted
per query. In other words, you may NOT intermix
IPv4 and IPv6 addresses.

Executing commands. Please be patient!

v4.whois.cymru.com

The server returned 2 line(s).

| AS | IP | AS Name |
|--------|--------------|--|
| 133752 | 85.203.47.86 | LEASEWEB-APAC-HKG-10 Leaseweb Asia Pacific pte. ltd., HK |

What Have we Learned?

1. User Agent String of North Korean origin visited www.froth.ly
 - Mozilla/5.0 (X11; U; Linux i686; ko-KP; rv: 19.1br) Gecko/20130508 Fedora/1.9.1-2.5.rs3.0 NaenaraBrowser/3.5b4
2. IP address of browser : 85.203.47.86
3. ASN : 133752
4. Visitor used Express VPN in HongKong to connect www.froth.ly.
5. Two additional IP addresses used the same user agent to connect to the site.
136.0.0.125 and 136.0.2.138

Public Web Visibility

Hypothesis:

PRE- Search Open Websites/Domains

Can we identify Publicly available company information that an adversary may be accessing

Here are some questions to think about that may help as we conduct our hunt:

- From an adversary perspective, where can we find information about our target?
- Did specific user agent strings access company content?
Mozilla/5.0 (X11; U; Linux i686; ko-KP; rv: 19.1br) Gecko/20130508 Fedora/1.9.1-2.5.rs3.0 NaenaraBrowser/3.5b4
- What IP addresses accessed company content?
- What kinds of company information is available from our website and other places to understand more about us?

- If we start to explore our http data, we can pivot to any number of interesting fields that were extracted at search time. One of those fields is http_content_type. This field is used to indicate the mime type in the event.

New Search Save As Create Table View Close

index=botsv2 sourcetype=stream:http site=www.froth.ly http_user_agent="Mozilla/5.0 (X11; U; Linux i686; ko-KP; rv: 19.1br) Gecko/20130508 Fedora/1.9.1-2.5.rs3.0 NaenaraBrowser/3.5b4" during Aug 2017 Q

! The following error(s) occurred while the search ran. Therefore, search results might be incomplete. [Show errors](#).

✓ 51 events (8/1/17 12:00:00.000 AM to 9/1/17 12:00:00.000 AM) No Event Sampling Job || ■ ↶ ↷ ⬇ Smart Mode

Events (51) Patterns Statistics Visualization

Format Timeline Zoom Out Zoom to Selection Deselect 1 day per column

< Hide Fields All Fields

SELECTED FIELDS

- a host 1
- a http_content_type 7
- a source 1
- a sourcetype 1

INTERESTING FIELDS

- a action 2
- a app 1
- # bytes 42
- # bytes_in 39
- # bytes_out 37
- a dest 1
- a dest_ip 1

http_content_type ×

7 Values, 100% of events Selected Yes No

Reports

- Top values
- Top values by time
- Rare values

Events with this field

| Values | Count | % |
|---|-------|---------|
| text/html; charset=iso-8859-1 | 30 | 58.824% |
| text/javascript | 9 | 17.647% |
| text/css | 7 | 13.725% |
| text/html; charset=UTF-8 | 2 | 3.922% |
| application/vnd.openxmlformats-officedocument.spreadsheetml.sheet | 1 | 1.961% |
| image/jpeg | 1 | 1.961% |
| image/png | 1 | 1.961% |

- We can see that, one of the MIME types is a office document. Spreadsheet. Upon clicking that, we can see that company_contacts.xlsx file has been downloaded on August 5th

timestamp: 2017-08-05T08:15:48.785770Z
transport: tcp
uri_path: /files/company_contacts.xlsx

What Have we Learned?

1. company_contacts.xlsx was downloaded.
2. It was downloaded on 8/5/17 1:15:49.707 AM.