Synergising Network Analysis Tradecraft

Network Tradecraft Advancement Team (NTAT)
* What is the NTAT?

* 2011 – 2012 work and accomplishments
Tradecraft

• “The development of methods, techniques, algorithms and processes in order to generate Intelligence, and developing the ability to apply this knowledge either manually or through automation. Tradecraft is developed from experience, research, intuition and by the reapplication and redefinition of existing techniques. Industrial-Scale Tradecraft involves data on a large scale.”

Network Tradecraft

• Usable knowledge about how to acquire intelligence FROM the network
The NTAT

* Create **repeatable**, **sustainable** & **shareable** tradecraft to enable network analysis

* Facilitate knowledge collaboration and interchange across the 5-Eyes SIGDEV community

TOP SECRET//SI
The Process

Stage 1 = Fact Finding

Stage 2 = Define Focus (based on Fact Finding)

Stage 3 = Develop Tradecraft

Stage 4 = Document Tradecraft

Stage 5 = Test Documented Tradecraft and Refine
* Technological convergence – where voice and data services interact with each other on a single device

* Tradecraft to enable the targeting of handsets in telephony space and CNE exploitation in IP space

* Improved algorithms for mobile gateway identification and implementation of these algorithms
* 2 weeks
* CSE, DSD, GCHQ
* Virtually, via chat room, NSA & GCSB
* Focus on data, techniques & analytic outcomes

https://wiki.dsd/twiki/
DSD Workshop
Outcomes

Technique developed to identify wide variety of potential converged data, unique for specific country or mobile network operator

Ø potentially lead to convergence correlation dataset to help profile targets on-line activity

Documentation of techniques to identify specific components of raw HTTP activity that alludes to the browsing, downloading and installation of smartphone applications

Ø identified the presence of application servers for mobile network operators and geographical areas

DSD implementation of mobile gateway identification analytic based on FRETTING YETI

Ø three agencies now running the same analytic provides a richer dataset of mobile gateways

CRAFTY SHACK trial

Ø NTAT now using CRAFTY SHACK for tradecraft documentation

TOP SECRET//SI
## XKS Microplugin: Samsung Protocol

<table>
<thead>
<tr>
<th>User-Agent</th>
<th>Device_ID</th>
<th>HTTP_User-Agent</th>
<th>Latest_Message</th>
<th>Message_Type</th>
<th>Mht</th>
<th>Network_Type</th>
<th>Dell_VERSION</th>
<th>send_Retcode</th>
<th>send_Reason</th>
<th>Protocol</th>
<th>Protocol</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>AUI</td>
<td>GT-I9100</td>
<td>SAMSUNG Android</td>
<td>2100-0</td>
<td>checkAppUpgrade Request</td>
<td>10</td>
<td>0</td>
<td>2.6.064</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>GT-I9100</td>
<td>SAMSUNG Android</td>
<td>2300-0</td>
<td>checkAppUpgrade Request</td>
<td>01</td>
<td>0</td>
<td>3.0.021</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>GT-I9100</td>
<td>SAMSUNG Android</td>
<td>2300-0</td>
<td>checkAppUpgrade Request</td>
<td>01</td>
<td>0</td>
<td>3.0.021</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>GT-I9100</td>
<td>SAMSUNG Android</td>
<td>2300-0</td>
<td>checkAppUpgrade Request</td>
<td>01</td>
<td>0</td>
<td>3.0.021</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>GT-I9100</td>
<td>SAMSUNG Android</td>
<td>2300-0</td>
<td>checkAppUpgrade Request</td>
<td>01</td>
<td>0</td>
<td>3.0.021</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>GT-I9100</td>
<td>SAMSUNG Android</td>
<td>2300-0</td>
<td>checkAppUpgrade Request</td>
<td>01</td>
<td>0</td>
<td>3.0.021</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>GT-I9100</td>
<td>SAMSUNG Android</td>
<td>2300-0</td>
<td>checkAppUpgrade Request</td>
<td>01</td>
<td>0</td>
<td>3.0.021</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>GT-I9100</td>
<td>SAMSUNG Android</td>
<td>2300-0</td>
<td>checkAppUpgrade Request</td>
<td>01</td>
<td>0</td>
<td>3.0.021</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>GT-I9100</td>
<td>SAMSUNG Android</td>
<td>2300-0</td>
<td>checkAppUpgrade Request</td>
<td>01</td>
<td>0</td>
<td>3.0.021</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### TOP SECRET//SI
CSE Workshop
February 2012

* 2 weeks
* CSE, DSD, GCHQ, GCSB, NSA – everyone wanted to experience a Canadian winter!
* Build on the work started at DSD

Winter Nirvana
The Reality!
Refinement of XKS fingerprints to identify mobile bearers, Samsung and Android Marketplace servers
   Ø 17 XKS fingerprints deployed

Documentation of analytics in CRAFTY SHACK
   Ø These analytics are now being implemented across the 5 Eyes

Proving the tradecraft actually works!
   Ø Scenario to test the tradecraft and analytics – Op IRRITANT HORN
Op IRRITANT HORN
Op IRRITANT HORN
Does the tradecraft work?

* Another Arab Spring (only this time, different countries)
* Goal: identify aggregation points for the mobile networks in the countries of interest using the tradecraft developed during the workshops
* Did it work? YES -> the team was able to identify connections from the countries to application and vendor servers in non 5-Eyes countries
* So what? We found some servers....
  Ø Potential MiTM
  Ø Effects
  Ø Harvesting data at rest
  Ø Harvesting data in transit
Finding mobile application & vendor update servers
Finding mobile application & vendor update servers

Congo

Senegal

Sudan

france  android-market.l.google.com
france  android-market.l.google.com
france  android-market.l.google.com
france  android-market.l.google.com
france  android-market.l.google.com

cuba    store.cubava.cu
cuba    store.cubava.cu
senegal  srv_applis.sar.sn

morocco boungeontelevision.com
switzerland download-force.com
bahamas  supportapple.com
cuba    store.cubava.cu
netherlands mobile.ero-advertising.com
russia  lady.marketgid.info

TOP SECRET//SI
### Identify Servers communicating with a Mobile network

**SEES** | **CSEC** | **DSD** | **OCHQ** | **GCSB** | **NSA** | **Factbox**
---|---|---|---|---|---|---

**Metadata**

What does the tradecraft achieve?
- This tradecraft will provide a list of servers that have been seen communicating with a mobile network.

In what situations would this tradecraft be most useful?
- To identify mobile application servers for a specific network.
- To identify any server that may be useful for collection purposes.

Describe any problems, caveats, or things to watch out for.
- The list of servers returned depends on the the IP range and collection sources utilized. Success of this tradecraft may require additional research to identify other IP ranges or requesting other agencies to check their collection to identify different servers.

Links that can help you to implement this tradecraft

- [SEES](#) | [CSEC](#) | [DSD](#) | [OCHQ](#) | [GCSB](#) | [NSA](#) | [Factbox](#)

#### Inputs:
- **Ontology/Network block**: Ontology/Network block.
- **Ontology/address**: Ontology/address.

#### Outputs:
- **Ontology/Network block**: Ontology/Network block.
- **Ontology/address**: Ontology/address.
- **Ontology/hostname**: Ontology/hostname.
- **Ontology/Identifier**: Ontology/Identifier.
- **Ontology/Organization**: Ontology/Organization.
- **Ontology/Direction**:
- **Ontology/Location**:
- **Ontology/Geographic select**: Ontology/Geographic select.

#### Invokes Tradecraft:
- Find public IPv4 space used by Mobile Devices and Related Servers on the Internet.
- Finding Mobile Internet Gateways.

#### Alternatives:
- Identify Servers communicating with a Mobile network.

### 6 SEES Tradecraft Steps (document underlying analytic, do not include tools)

1. **Find IP ranges** or individual addresses identified as being related to mobile network communications.
2. **Obtain geolocation information** and network ownership information for each IP address. This should include Network Owner name, Carrier name, ARIN, ARIN Name, Country Code, City, Postal Code, and anything related details that your system can collect.
3. **Obtain Internet communication events related to the IP address**. These events should include include packet source information, To IP, From IP, TCP/UDP, and HTTP User-Agent.
4. **Sort the results and dump them**. This depends on your collection sources.
5. **Filter out server communications** that are IP addresses that aren't useful. Further analysis is needed to identify the non-useful nodes (e.g., email, DNS). Use Nessus or similar.
6. **Check the TCP/UDP field**.
   - If Server is a Client, grab the To IP information.
   - If Client is a Server, grab the To IP information.
   - If Server is a Server, grab both the To and From IP information.
7. **Look for unusual suspicious activity**.
8. **Sort and develop** based on Server IP information. TCP/UDP direction info is no longer needed.
9. **Obtain geolocation information and network ownership information for each Server IP**. This is done for servers that are not in the original IP blocks.
10. **Remove any servers that are not useful. This may include 5-caps servers**.

#### Comments:
- [Show comments](#)
- [Last updated 12/2013](#)

**Category**: Tradecraft
Identifying servers communicating with an MNO

TOP SECRET//SI
Profiling mobile application servers

This tool should accept a CSV file of mobile app server KPIs and perform a reverse DNS lookup to obtain the IP addresses of the app servers. For each IP address, Geo-location and Network information (ATLAS) Data Range, IP Range, and app server details are analyzed. The Geo-location and Network Information are used to filter the events based on the geo and network details. The events are then filtered to obtain the unique TDI events, and the app server details are added to these events. The results are then filtered further to obtain the final list of events for each app server with the geo and network details of the client's access points.

TOP SECRET//SI
Profiling mobile application servers
Profiling mobile application servers

Results based on mobile application servers seen in CSE collection
We have a list of the most popular smartphones for Warid Congo customers and their IMSIs

TOP SECRET//SI
Success Stories

* UCWeb mobile browser identification
  * Discovered by GCHQ analyst during DSD workshop

* Chinese mobile web browser – leaks IMSI, MSISDN, IMEI and device characteristics
* Led to discovery of active comms channel from

(S//SI//REL TO USA, FVEY) The CONVERGENCE team helped discover an active communication channel originating from [redacted] that is associated with the [redacted] as they are known within the [redacted] hierarchy area of responsibility is for covert activities in Europe, North America, and South America. The customer [redacted] leveraged a **Convergence Discovery capability that enabled the discovery of a covert channel associated with smart phone browser activity in passive collection.** The covert channel originates from users who use UCBrowser (mobile phone compact web browser). The covert channel leaks the IMSI, MSISDN, Device Characteristics, and IMEI back to server(s) in [redacted]. Initial investigation has determined that perhaps malware can be associated when the covert channel is established. [redacted] covert exfil activity identifies SIGINT opportunity where potentially none may have existed before. Target offices that have access to X-KEYSCORE can search within this type of traffic based on their IMSI or IMEI to determine target presence.
<table>
<thead>
<tr>
<th>State</th>
<th>ID</th>
<th>Datetime</th>
<th>Highlights</th>
<th>Browser Version</th>
<th>Email Address</th>
<th>Handset Model</th>
<th>MSI</th>
<th>Global Title</th>
<th>Platform</th>
<th>Active UserIF</th>
<th>Casenotation</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>2012-05-13 02:29:20</td>
<td></td>
<td>8.6.5.5.7</td>
<td>ti21movies</td>
<td>nokia50-1</td>
<td></td>
<td>82799909000</td>
<td>java</td>
<td>82799909000</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>2012-05-13 06:00:59</td>
<td></td>
<td>8.6.3.107</td>
<td>ti21movies</td>
<td>nokia50-1</td>
<td></td>
<td>82799909000</td>
<td>java</td>
<td>82799909000</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>4</td>
<td>2012-05-13 19:38:11</td>
<td></td>
<td>7.8.3.103</td>
<td></td>
<td>HTC A510e</td>
<td></td>
<td>82799909000</td>
<td>android</td>
<td>82799909000</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>2</td>
<td>2012-05-14 12:29:53</td>
<td></td>
<td>8.8.4.121</td>
<td></td>
<td>NokiaE72-1</td>
<td></td>
<td>82799909000</td>
<td>sis</td>
<td>82799909000</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>5</td>
<td>2012-05-14 16:46:06</td>
<td></td>
<td>8.8.4.121</td>
<td>mmobimastil</td>
<td>NokiaX6-08</td>
<td></td>
<td>82799909000</td>
<td>sis</td>
<td>82799909000</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>5</td>
<td>2012-05-15 18:29:19</td>
<td></td>
<td>8.8.4.121</td>
<td>mmobimastil</td>
<td>NokiaX6-08</td>
<td></td>
<td>82799909000</td>
<td>sis</td>
<td>82799909000</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>7</td>
<td>2012-05-15 20:02:56</td>
<td></td>
<td>8.8.4.121</td>
<td>mmobimastil</td>
<td>NokiaX6-08</td>
<td></td>
<td>82799909000</td>
<td>sis</td>
<td>82799909000</td>
<td></td>
</tr>
</tbody>
</table>

TOP SECRET//SI
Vision of Success

* Shared convergence database with numerous different sources, methods & tradecraft feeding into it
* Ultimately correlating telephony and Internet TDIs with some degree of confidence
Synergising Network Analysis Tradecraft

Network Tradecraft Advancement Team (NTAT)
Synergising Network Analysis Tradecraft

Network Tradecraft Advancement Team (NTAT)
Overview

* What is the NTAT?

* 2011 – 2012 work and accomplishments
Tradecraft

- "The development of methods, techniques, algorithms and processes in order to generate intelligence, and developing the ability to apply this knowledge either manually or through automation. Tradecraft is developed from experience, research, intuition and by the reapplication and redefinition of existing techniques. Industrial-Scale Tradecraft involves data on a large scale."

Network Tradecraft

- Usable knowledge about how to acquire intelligence FROM the network.
The NTAT

- Create repeatable, sustainable & shareable tradecraft to enable network analysis

- Facilitate knowledge collaboration and interchange across the 5-Eyes SIGDEV community
The Process

Stage 1 = Fact Finding

Stage 2 = Define Focus (based on Fact Finding)

Stage 3 = Develop Tradecraft

Stage 4 = Document Tradecraft

Stage 5 = Test Documented Tradecraft and Refine

TOP SECRET!!
Network Convergence Tradecraft

* Technological convergence – where voice and data services interact with each other on a single device

* Tradecraft to enable the targeting of handsets in telephony space and CNE exploitation in IP space

* Improved algorithms for mobile gateway identification and implementation of these algorithms
DSD Workshop
November 2011

* 2 weeks
* CSE, DSD, GCHQ
* Virtually, via chat room, NSA & GCSB
* Focus on data, techniques & analytic outcomes

https://wiki.dsd/twiki
DSD Workshop Outcomes

Technique developed to identify wide variety of potential converged data, unique for specific country or mobile network operator

- potentially lead to convergence correlation dataset to help profile targets on-line activity

Documentation of techniques to identify specific components of raw HTTP activity that alludes to the browsing, downloading and installation of smartphone applications

- identified the presence of application servers for mobile network operators and geographical areas

DSD implementation of mobile gateway identification analytic based on FRETTING YETI

- three agencies now running the same analytic provides a richer dataset of mobile gateways

CRAFTY SHACK trial

- NTAT now using CRAFTY SHACK for tradecraft documentation

TOP SECRET//SI
CSE Workshop
February 2012

- 2 weeks
- CSE, DSD, GCHQ, GCSB, NSA – everyone wanted to experience a Canadian winter!
- Build on the work started at DSD

* Winter Nirvana!
The Reality!
CSE Workshop Outcomes

Refinement of XKS fingerprints to identify mobile bearers, Samsung and Android Marketplace servers
- 17 XKS fingerprints deployed

Documentation of analytics in CRAFTY SHACK
- These analytics are now being implemented across the 5 Eyes

Proving the tradecraft actually works!
- Scenario to test the tradecraft and analytics – Op IRRITANT HORN

TOP SECRET//SI
Op IRRITANT HORN
Does the tradecraft work?

- Another Arab Spring (only this time, different countries)
- Goal: identify aggregation points for the mobile networks in the countries of interest using the tradecraft developed during the workshops
- Did it work? YES -> the team was able to identify connections from the countries to application and vendor servers in non 5-Eyes countries
- So what? We found some servers....
  - Potential MITM
  - Effects
  - Harvesting data at rest
  - Harvesting data in transit

MiTM – exploit the application server and use it as a MiTM platform for handset exploitation

Effects – exploitation of the application servers could make it possible to provide selective misinformation to the targets handsets

Harvesting data at rest – exploitation of the applications servers could provide access to a wealth of information at rest. The amount and usefulness of this information depends on the application in question

Harvesting data in transit – mobile applications servers often send and receive data that SIGINT agencies find useful (e.g. the Samsung protocol sending client and handset details to a server in Germany)
The results above are from a tradecraft to find servers of applications and vendor updaters servers from given countries. The rationale behind this is to identify servers that target within those countries might visit which could be exploited by CNE to push a phone implant capability.

The tradecraft relies upon 5 tuple data seen from the mobile gateways from target countries and to servers which have matching 'key words' in the hostname. The results above could then be scoped for CNE to see if they would be valid boxes to use an access platform.
The results above are from a tradecraft to find servers of applications and vendor updaters servers from given countries. The rationale behind this is to identify servers that target within those countries might visit which could be exploited by CNE to push a phone implant capability.

The tradecraft relies upon 5 tuple data seen from the mobile gateways from target countries and to servers which have matching 'key words' in the hostname. The results above could then be scoped for CNE to see if they would be valid boxes to use an access platform.
Identifying servers communicating with an MNO
Profiling mobile application servers
Profiling mobile application servers

- Results based on mobile application servers seen in CSE collection
- We have a list of the most popular smartphones for Warid Congo customers and their IMSIs

TOP SECRET/SSI
Success Stories

* UCWeb mobile browser identification
  * Discovered by GCHQ analyst during DSD workshop

* Chinese mobile web browser – leaks IMSI, MSISDN, IMEI and device characteristics
Led to discovery of active comms channel from [redacted]

(S//SI//REL TO USA, FVEY) The CONVERGENCE team helped discover an active communication channel originating from [redacted] that is associated with the [redacted] as they are known within the [redacted] hierarchy area of responsibility is for covert activities in Europe, North America, and South America. The customer [redacted] leveraged a Convergence Discovery capability that enabled the discovery of a covert channel associated with smartphone browser activity in passive collection. The covert channel originates from users who use UCBrowser (mobile phone compact web browser). The covert channel leaks the IMSI, MSISDN, Device Characteristics, and IMEI back to server(s) in [redacted]. Initial investigation has determined that perhaps malware can be associated when the covert channel is established. [redacted] covert exfiltration activity identified SIGINT opportunity where potentially none may have existed before. Target offices that have access to [redacted] KEYSOURCE can search within this type of traffic based on their IMSI or IMEI to determine target presence.
<table>
<thead>
<tr>
<th>Time</th>
<th>Hostname</th>
<th>Path</th>
<th>Size</th>
<th>User</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>2003-01-26 00:00:00</td>
<td>localhost</td>
<td>/</td>
<td>0 B</td>
<td>root</td>
<td>active</td>
</tr>
<tr>
<td>2003-01-26 00:00:01</td>
<td>localhost</td>
<td>/index.html</td>
<td>0 B</td>
<td>root</td>
<td>active</td>
</tr>
<tr>
<td>2003-01-26 00:00:02</td>
<td>localhost</td>
<td>/</td>
<td>0 B</td>
<td>root</td>
<td>active</td>
</tr>
<tr>
<td>2003-01-26 00:00:03</td>
<td>localhost</td>
<td>/</td>
<td>0 B</td>
<td>root</td>
<td>active</td>
</tr>
<tr>
<td>2003-01-26 00:00:04</td>
<td>localhost</td>
<td>/</td>
<td>0 B</td>
<td>root</td>
<td>active</td>
</tr>
</tbody>
</table>

TOP SECRET/SI
Vision of Success

- Shared convergence database with numerous different sources, methods & tradecraft feeding into it
- Ultimately correlating telephony and Internet TDI's with some degree of confidence
Synergising Network Analysis Tradecraft

Network Tradecraft Advancement Team (NTAT)