



# (U//FOUO) SPINALTAP: Making Passive Sexy for Generation Cyber

[REDACTED], R1, [REDACTED]  
[REDACTED], F77, [REDACTED]  
[REDACTED], F77, [REDACTED]



# SPINALTAP

- Extracts selectors from TAO/SFC/GCHQ boxes that should also appear in passive collection
- Translates selectors from active context to passive context
- Creates fingerprints to label passive collection related to endpoint-derived selectors
- Automated
- Scalable



# SPINALTAP



endpoint/related/WICKEDAMP11/user\*  
 endpoint/related/WICKEDAMP11/network\*  
 endpoint/related/WICKEDAMP11/machineID\*  
 endpoint/related/WICKEDAMP11/cypher\_key\*  
 endpoint/related/WICKEDAMP11/attached\_device\*



Serial numbers  
Hostmacs

usernames

IMEIs  
UDIDs  
Browser tags  
usernames

machineIDs

Computer System	
Manufacturer	Gateway
Model	M-68841
Domain	WORKG
Domain Role	Standalo

COUDBTAD	
A:	
C: <1>	
D: <32>	
E:	
F:	
G:	
H:	

Key Name	
hkey_local_machine\catalogs\	
hkey_local_machine\catalogs\	
hkey_local_machine\software\	
hkey_local_machine\software\	
hkey_local_machine\software\	

user@yahoo[2].1290074506.txt	
user@yahoo[2].1290074506.txt	
user@yahoo[2].1290074506.txt	
98	csB
10	ya csp41md5ip9n1Gb
40	10 yahoo.com/
30	40 1024
93	30 4099842048
30	93 30195537
	30 934331712
	30048403





# Selector Types

## Machine IDs

- **Cookies**
  - Hotmail GUIDs
  - Google prefIDs
  - YahooBcookies
  - mailruMRCU
  - yandexUid
  - twitterHash
  - ramblerRUID
  - facebookMachine
  - doubleclickID
- **Serial numbers**
- **Browser tags**
  - Simbar
  - ShopperReports
  - SILLYBUNNY
- **Windows Error IDs**
- **Windows Update IDs**

## Attached Devices

- **IMEIs for Phones**
  - Apple IMEIs
  - Nokia IMEIs
- **UDIDs**
  - Apple UDIDs
- **Bluetooth?**
  - Device Name
  - Device Address

## Cipher Keys

- **Cipher Keys uniquely identified to a user**
  - ejKeyID

## Network

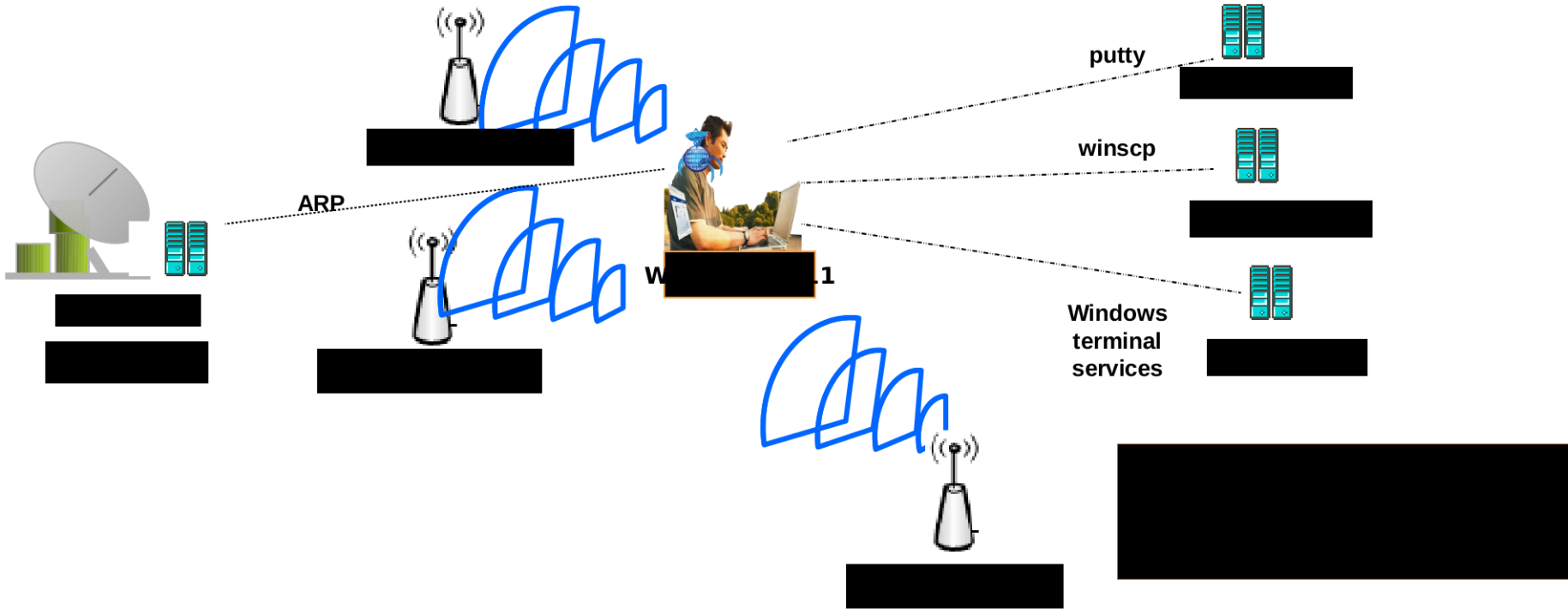
- **Wireless MACs**
- **VSAT MACs and IPs**

## User Leads

- **User selectors from Cookies, Registry, and Profile Folders**
  - msnpassport
  - google
  - yahoo
  - Youtube
  - Skype
  - Paltalk
  - Fetion
  - QQ
  - hotmailCID
- **STARPROC-identified active users**





# Network Level Selectors





# Active/Passive Map

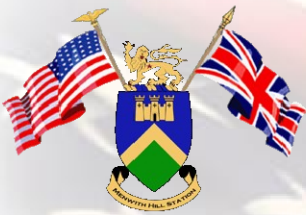
1. XKS Fingerprints parse files collected from endpoint accesses and feed active\_passive\_map microplugin
2. Micro-plugin feeds SPINALTAP Database / GUI
3. SPINALTAP Database generates fingerprints

 CNE  
 Active Passive Map

Input Source:

Filter	relationship_type	relationship_value	Count
<input type="checkbox"/>	serial_number_dell		2
<input type="checkbox"/>	windowsupdateGUID		2
<input type="checkbox"/>	windowsupdateGUID		2
<input type="checkbox"/>	windowsupdateGUID		2
<input type="checkbox"/>	yahooUser		2
<input type="checkbox"/>	yahooUser		2
<input type="checkbox"/>	yahooUser		2
<input type="checkbox"/>	yahooUser		2
<input type="checkbox"/>	yahooUser		2
<input type="checkbox"/>	yahooUser		2
<input type="checkbox"/>	yahooUser		2
<input type="checkbox"/>	realm_mid_GooglePREF		1
<input type="checkbox"/>	realm_mid_GooglePREF		1

Analysts can query microplugin to see what selectors have been extracted for their target projects



# Sample Lifecycle: DARKSCREW46

[Redacted]

S [Redacted] s:  
A [Redacted] p

## Machine Info

**DARKSCREW/DARKSCREW46** ▾

Last Collection[limit 3 listed]:

[2012-02-12](#)

[2012-02-08](#)

[2012-02-06](#)

[List All Collection](#)

[Categorized Collection](#)

relationship_type	relationship_value	Input Source
serial_number_lenovo	L3PW286	DARKSCREW46
hotmailGUID	0574A0786A9C6AD13CCDA29F6E9C6A60	DARKSCREW46
hotmailGUID	10F3D90D305A6CAA3939DBEA345A6CC3	DARKSCREW46
hotmailGUID	277D434B01A0648503DE419705A064E0	DARKSCREW46
doubleclickID	22bcd6191801009a	DARKSCREW46
doubleclickID	22fd816a5401001b	DARKSCREW46
facebookMachine	e0yyTZC6VhXJBTsemghlfZ	DARKSCREW46
GooglePREFID	3064562fddcfcfd52	DARKSCREW46
GooglePREFID	59035ab896c931e1	DARKSCREW46
GooglePREFID	5f234c7ac7381e2f	DARKSCREW46
hotmailGUID	E9C7006D5F1F49D683EBF805FE18FE17	DARKSCREW46
yahooBcookie	2amrd0t7h2hcs	DARKSCREW46

[endpoint/related/DARKSCREW46/user/nsa/cne/yahooUser](#)

Fm IP	To IP	Sigad	Application Type
[Redacted]	[Redacted]	DS-200X	mail
[Redacted]	[Redacted]	DS-200X	chat
[Redacted]	[Redacted]	DS-200X	chat

[Redacted]

[Redacted]



# Improving CNE Collection

- Pushed for routine, standardized collection of artifacts containing useful selectors to support SPINALTAP
  - Registry: additions to SIGDEV survey to collect new registry keys and values
  - Files: broad, repeated cookie collection via additions to SIGDEV survey
  - Directories: dirwalks already standardized, no changes necessary





# SPINALTAP Fingerprints

- 31168 active fingerprints
- Fingerprints for 722 projects
  - 488 TAO CNE projects
  - 7 GCHQ CNE projects
  - 227 SFC Forensics projects
- Fingerprints for 6188 unique machines

attached_device fingerprints	1102
user fingerprints	23173
machineID fingerprints	5599
cipher_key fingerprints	1293

NSA TAO fingerprints	29361
NSA SFC fingerprints	1745
GCHQ CNE fingerprints	61

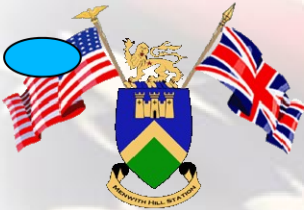
**endpoint/related/<BOXNAME>/<id\_class>/<agency\_owner>/<source>/<id\_type>**

.....

endpoint/related/STONEHENGE18/user/nsa/cne/skypeHash

endpoint/related/DEADDRUMMER10/machineID/gchq/cne/simbar

endpoint/related/FREEFLOWERPEOPLE1/attached\_device/nsa/forensic/appleUDID



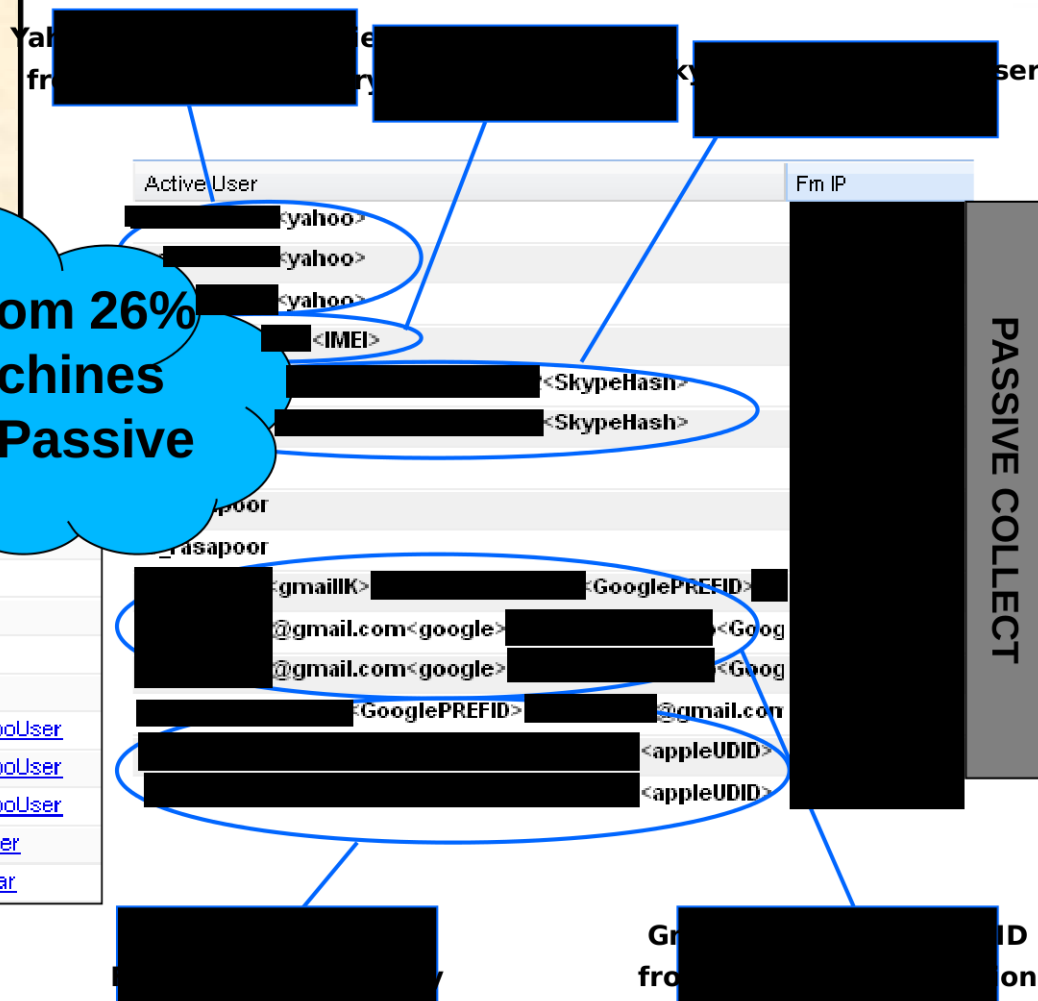
# SPINALTAP Fingerprint Hits

Since activated July 2011:

- Hits from 2087 unique fingerprint hits (7%)
- Hits from 1619 unique boxes (26%)
- 8395 box/id type/sigad combination

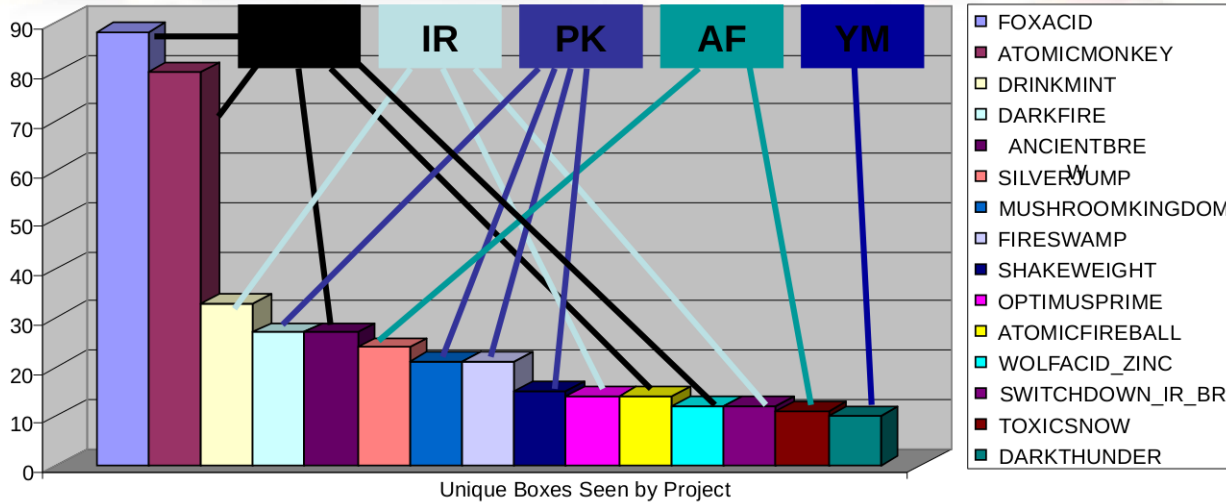
**Selectors from 26% of TAO Machines are seen in Passive**

Sigad	AppID (+Fingerprints)
UKJ-260D	<a href="#">endpoint/related/SILVERJULI</a>
USJ-759A	<a href="#">endpoint/related/SILVERJULI</a>
UKJ-260D	<a href="#">endpoint/related/SILVERJULI</a>
UKC-302A	<a href="#">endpoint/related/SLYNINJA15</a>
UKJ-260D	<a href="#">endpoint/related/SLYWMZARD16/user/nsa/cne/yahooUser</a>
UKJ-260G	<a href="#">endpoint/related/SLYWMZARD16/user/nsa/cne/yahooUser</a>
UKJ-260D	<a href="#">endpoint/related/SLYWMZARD21/user/nsa/cne/skypeuser</a>
UKJ-260D	<a href="#">endpoint/related/SPARTANFURY16/user/nsa/cne/skypeuser</a>
DS-300	<a href="#">endpoint/related/STRAITLACED554/user/nsa/cne/yahooUser</a>
DS-300	<a href="#">endpoint/related/SWITCHDOWN_IR_BR152/user/nsa/cne/yahooUser</a>
DS-300	<a href="#">endpoint/related/SWITCHDOWN_IR_BR245/user/nsa/cne/yahooUser</a>
DS-300	<a href="#">endpoint/related/SWITCHDOWN_IR_BR246/user/nsa/cne/yahooUser</a>
UKC-302A	<a href="#">endpoint/related/THIEVESQUARTER25/user/nsa/cne/yahooUser</a>
DS-300	<a href="#">endpoint/related/WATERCASKET103/machineID/nsa/cne/simbar</a>



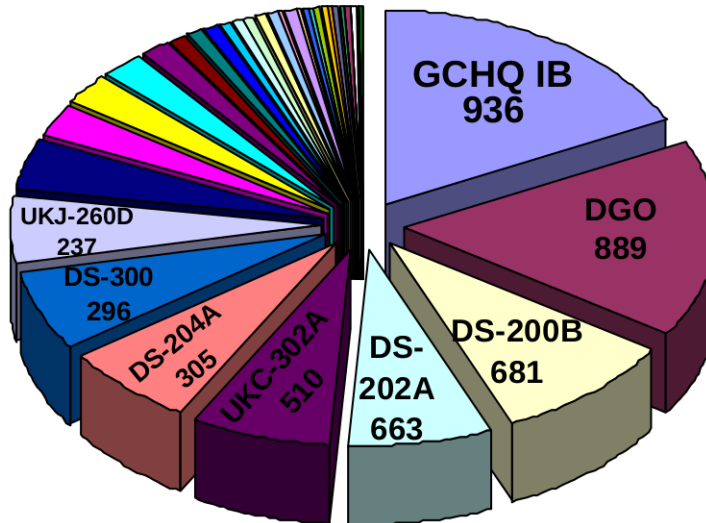


# Hits by Project/Site



**Unique Machines  
Seen by Project  
(Top 15 projects)**

**Unique Machines  
seen by SIGAD**



**1619 unique machines seen  
At 68 different sigads  
Using 31 different ID types**



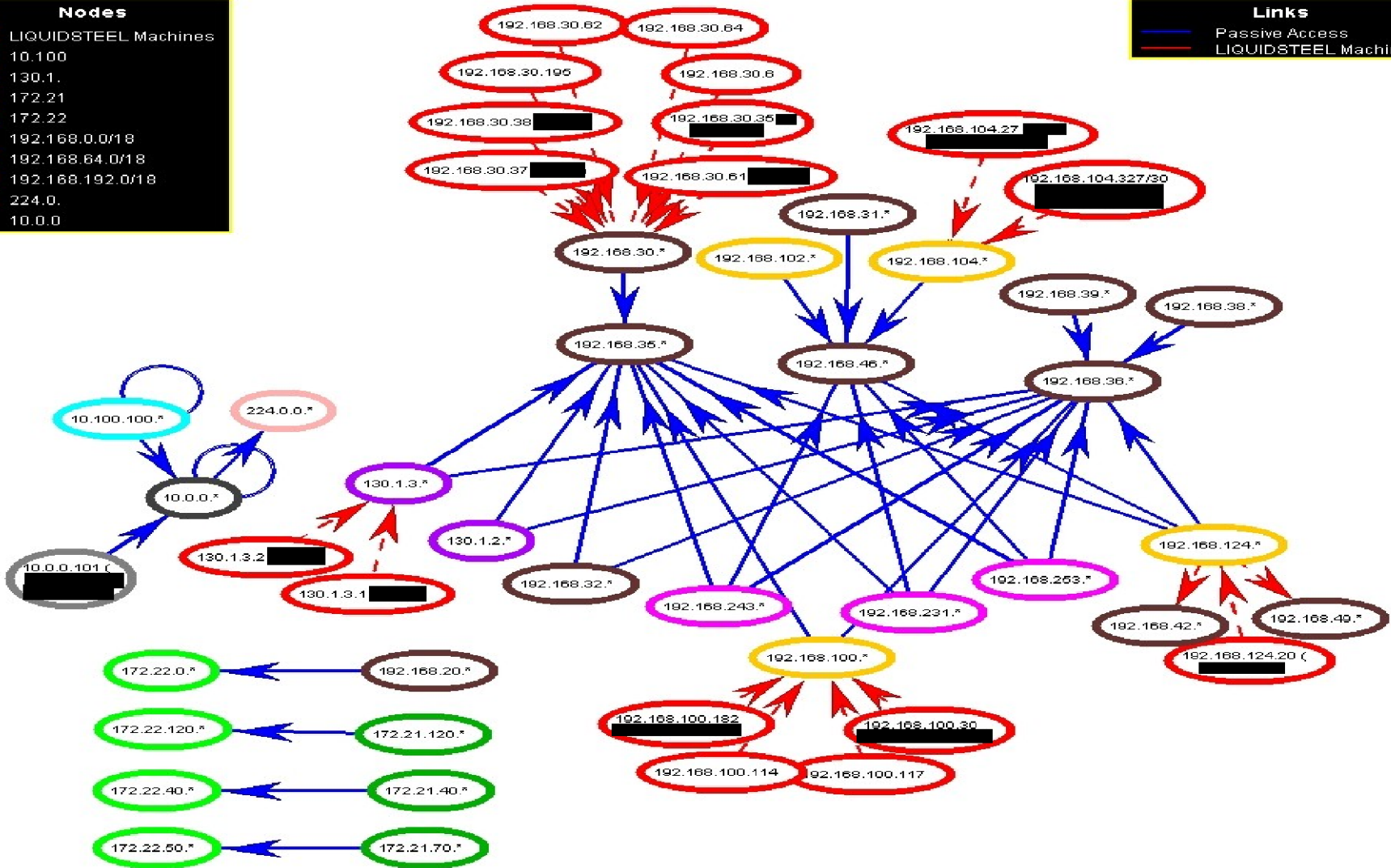
# Application: Exfil Opportunities

**Nodes**

Red	LIQUIDSTEEL Machines
Cyan	10.100
Magenta	130.1.
Green	172.21
Light Green	172.22
Brown	192.168.0.0/18
Yellow	192.168.64.0/18
Pink	192.168.192.0/18
Light Pink	224.0.
Grey	10.0.0

**Links**

Blue arrow	Passive Access
Red arrow	LIQUIDSTEEL Machines





# Application: Bearer Prioritization

<a href="#">Home</a> <a href="#">All Questions</a> <a href="#">All CASNs</a> <a href="#">Survey CASNs</a> <a href="#">ASPHALT CASNs</a> <a href="#">Snap CASNs</a>					
Show <input type="text" value="50"/> entries <input type="button" value="Refresh"/> <span style="float: right;">First</span>					
id	topic	weight	run_interval	valid_length	description
	*spinal*				
113	SPINALTAP	50	1	30	Case notation gets points for each type correlation seen each CNE project

SPINALTAP		
Show <input type="text" value="25"/> entries <input type="button" value="Refresh"/> <span style="float: right;">First</span>		
casn	sigad	casn_total_score
2CBAB00000M0286	USJ-759A	166778
E9DCJ00000M0000	USJ-759A	84634
E9DHL00000M0000	USJ-759A	76044
5BBAK00000MID04	USJ-759	18723
B0BAJ00000M0000	USJ-759A	35249
E9DFT00000M0000	USJ-759A	115091
G6BAD00000M0100	USJ-759A	27832
5BBAK00000M0000	USJ-759A	26019
NFH116400280000	USJ-759	150
NFDJG00000M4147	USJ-759A	27580
NFH111717504144	USJ-759A	19874

casn	fingerprint
2CBAB00000M0286	cne_related/ANCIENTBREW115/user/nsa/yahooUser
2CBAB00000M0286	cne_related/CHOCOLATESHIP2/user/nsa/email
2CBAB00000M0286	cne_related/CUDDLYBADGER16/user/nsa/yahooUser
2CBAB00000M0286	cne_related/DARKTHUNDER64/user/nsa/yahooUser
2CBAB00000M0286	cne_related/DISTORTAFFECT1/user/nsa/yahooUser
2CBAB00000M0286	cne_related/DRINKMINT158/user/nsa/yahooUser
2CBAB00000M0286	cne_related/DRINKMINT195/user/nsa/yahooUser
2CBAB00000M0286	cne_related/DRINKMINT322/user/nsa/yahooUser
2CBAB00000M0286	cne_related/DRINKMINT350/user/nsa/yahooUser
2CBAB00000M0286	cne_related/DRINKMINT384/user/nsa/yahooUser
2CBAB00000M0286	cne_related/DRINKMINT410/user/nsa/yahooUser
2CBAB00000M0286	cne_related/DRINKMINT420/user/nsa/yahooUser



# Application: Target Relationships

## Histogram Grid ✕

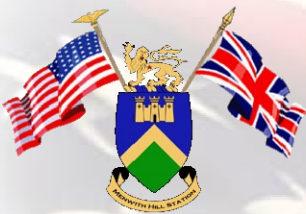
Page 1 of 1 ↩ ↪ ↻ Clear Selection Export Interactive Mode

Filter	Input Source	Count
<input type="checkbox"/>	WOLFACID_PRECIOUS5	82
<input type="checkbox"/>	DOUBLETAP23	45
<input type="checkbox"/>	DOUBLETAP14	33
<input type="checkbox"/>	WOLFACID_URANIUM1	24
<input type="checkbox"/>	WOLFACID_IODINE1	16
<input type="checkbox"/>	WOLFACID_PRECIOUS4	13
<input type="checkbox"/>	WOLFACID_ARGON8	12
<input type="checkbox"/>	WOLFACID_IRON10	12
<input type="checkbox"/>	ATOMICFOG40	8
<input type="checkbox"/>	OFFICELINEBACKER105	8
<input type="checkbox"/>	OFFICELINEBACKER90	8
<input type="checkbox"/>	DOUBLETAP11	7
<input type="checkbox"/>	WOLFACID_BARIUM49	7

## ejkeyid

Help Actions Reports View Map View **FILTERS:** 🗃️ 🔍

	<input type="checkbox"/>	State	ID	Datetime	Highlights	AppID (+Fingerprints)
1	<input type="checkbox"/>	✉	<a href="#">255</a>	2011-12-14 23:53:00		<a href="#">dnt_payload/file_cne/technique/unitedrake_cyber/cyberquest/cno_activity_dnt_payload/header_parsed_encryption/</a>
2	<input type="checkbox"/>	✉	<a href="#">214</a>	2011-05-20 18:41:00		<a href="#">dnt_payload/file_cne/technique/unitedrake_cyber/cyberquest/cno_activity_dnt_payload/header_parsed_encryption/</a>
3	<input type="checkbox"/>	✉	<a href="#">215</a>	2011-05-20 20:08:00		<a href="#">dnt_payload/file_cne/technique/unitedrake_cyber/cyberquest/cno_activity_dnt_payload/header_parsed_encryption/</a>
4	<input type="checkbox"/>	✉	<a href="#">438</a>	2011-11-03 18:31:00		<a href="#">dnt_payload/file_cne/technique/unitedrake_cyber/cyberquest/cno_activity_dnt_payload/header_parsed_encryption/</a>
5	<input type="checkbox"/>	✉	<a href="#">85</a>	2011-11-30 21:42:00		<a href="#">dnt_payload/file_VPII/Site to Site_VPII/More_Setup_titles_subjects_or_filenames_ccne/Discovery/MobileTerms c</a>
6	<input type="checkbox"/>	✉	<a href="#">243</a>	2011-10-25 19:59:00		<a href="#">dnt_payload/file_cne/technique/danderspritz_cyber/cyberquest/cno_activity_dnt_payload/header_parsed_encryptio</a>
7	<input type="checkbox"/>	✉	<a href="#">244</a>	2011-10-25 20:00:00		<a href="#">dnt_payload/file_cne/technique/danderspritz_cyber/cyberquest/cno_activity_dnt_payload/header_parsed_encryptio</a>
8	<input type="checkbox"/>	✉	<a href="#">257</a>	2011-10-25 20:07:00		<a href="#">dnt_payload/file_cne/technique/danderspritz_cyber/cyberquest/cno_activity_dnt_payload/header_parsed_encryptio</a>



# Application: Selector Discovery

Home MyXKS Admin Users Search Workflow Central Results Fingerprints Tagging Statistics Tasking Map Help

**Note: Icons on this page represent categories of services (e.g. web searches, VoIP, browsers) provided by established commercial firms. They do NOT identify targeted firms.**

**IP Address:** [Redacted] **Country:** PK **Start:** 2012-04-27 14:46:46 **Duration:** 3 min(s) **Casenotation(s):** PKCSE039L001 PKCSE039K00 **High**  
**HHFP:** 13c8eea4 **City:** KARACHI **Stop:** 2012-04-27 14:49:21 **Sigad(s):** UKC-302A **Active User(s):** [Redacted]

**Fingerprint**

- defeat/atrouter/yahoo/insider/client\_ad\_get
- defeat/atxs/yahoo/insider/client\_ad\_get
- endpoint/related/atomicmonkey372/machineid/nsa/cne/simbar
- mail/webmail/yahoo

**Active Accounts**

User	[Redacted] <yahooBcookie>
------	---------------------------

**Web Sites Visited**

Type	Page Title/Host	Count
host	insider.msg.yahoo.com	1
host	us.adserver.yahoo.com file://C:\Documents%20an...	1

**Web Searches**

**Targets: Content Hits**

**Device Information**

Client IP	Client GEO	Leaker IP
[Redacted]	PK, KARACHI (24.87, 67...	

**Active Accounts**

User	Role	State
[Redacted] <yahooBcoo...	unknown	active

Topic Hits  
Browsers  
User Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)

Images  
VOIP  
SSH  
SSL

REENABLE

Application: ~~Mitigate~~ ~~Lost~~ Collect

active_user_id	id_type	machine_name	q_technique	sigad	opportunity_type	unique_cour
	yahooUser	TOXICSNOW72	QDIRK	USJ-759A	CONFIRMED	26
	yahooUser	ATOMICMONKEY380	QDIRK	USJ-759A	POTENTIAL	5
	yahooUser	SLYNINJA150	QDIRK	USJ-759A	POTENTIAL	4
	yahooUser	SLYNINJA150	QDIRK	USJ-759A	CONFIRMED	27
	yahooUser	SLYNINJA151	QDIRK	USJ-759A	CONFIRMED	3
	yahooUser	MUSHROOMKINGDOM143	QDIRK	USJ-759A	CONFIRMED	2
	yahooUser	ATOMICMONKEY200	QDIRK	USJ-759A	UNKNOWN	1
	facebook	OFFICELINEBACKER21	QBISCUIT	DS-300	CONFIRMED	2
	yahooUser	SWTCHDOWN_IR_BR154	QBISCUIT	DS-300	UNKNOWN	1
	yahooUser	SPARTANFURY35	QBISCUIT	DS-300	CONFIRMED	2
	yahooUser	OPTIMUSPRIME222	QBISCUIT	DS-300	UNKNOWN	2
	yahooUser	SPARTANFURY64	QBISCUIT	DS-300	UNKNOWN	33
	facebook	STRAITLACED435	QBISCUIT	DS-300	UNKNOWN	3
	yahooUser	WATERCASKET88	QBISCUIT	DS-300	UNKNOWN	11
	yahooUser	SPARTANFURY35	QBISCUIT	DS-300	UNKNOWN	2
	facebook	DOUBLETAP27	QBISCUIT	DS-300	POTENTIAL	2
	yahooUser	WATERCASKET103	QBISCUIT	DS-300	UNKNOWN	6
	yahooUser	WATERCASKET27	QBISCUIT	DS-300	UNKNOWN	15
	yahooUser	OPTIMUSPRIME353	QBISCUIT	DS-300	CONFIRMED	11
	yahooUser	SPARTANFURY35	QBISCUIT	DS-300	POTENTIAL	1
	yahooUser	OPTIMUSPRIME353	QBISCUIT	DS-300	UNKNOWN	7
	yahooUser	OPTIMUSPRIME353	QBISCUIT	DS-300	POTENTIAL	9
	yahooUser	SPARTANFURY35	QBISCUIT	DS-300	CONFIRMED	1
	yahooUser	SPARTANFURY45	QBISCUIT	DS-300	CONFIRMED	14





# Application: ~~Mitigate~~ ~~Lost~~ Collect

- Combine XKEYSCORE Map/Reduce Results (QTM Opportunities) with GMPLACE Callback Analytics (Lost Implants)

QUANTUM\_Database / urQuantumReenable Last updated: Thu May 31 09:57:24 +0000 2012

Show  entries

Refresh

active_user_id	from_port	to_port	id_type	machine_name	opportunity_type	q_technique	sigad	last_callback
	5050	3139	yahooUser	ATOMICMONKEY108	UNKNOWN	QBISCUIT	US-3171	2012-04-08T10:42:30.000+00:00
	80	45527	yahooUser	DARKFIRE1086	POTENTIAL	QBISCUIT	US-3171	2012-04-04T03:16:14.000+00:00
	80	4687	yahooUser	ATOMICMONKEY496	POTENTIAL	QBISCUIT	US-3171	2012-04-08T10:37:00.000+00:00
	65080	80	facebook	DARKFIRE1082	CONFIRMED	QDIRK	US-3171	2012-04-13T06:32:17.000+00:00
	33966	80	yahooUser	ATOMICMONKEY496	CONFIRMED	QDIRK	US-972U	2012-04-08T10:37:00.000+00:00
	15577	80	yahooUser	COBALTGUPPY36	CONFIRMED	QBISCUIT	US-3171	2012-04-16T10:31:57.000+00:00



# Future Work

- Further automate extraction, fingerprint creation (currently weekly)
- Provide access to SPINALTAP DB via GUI
- Support for new ID types
  - MAC addresses
  - Expansion of SFC related fingerprints
  - Expansion of 2nd Party CNE related fingerprints
- Deprecation/Expiration of fingerprints
- Improve private network identification
- Provide as enrichment source to other tools



# Hits – All Projects

YELLOWFAN  
WOLFACID\_ZINC  
WOLFACID\_TIN  
WOLFACID\_LEAD  
WOLFACID\_JUPITER  
WOLFACID\_IRON  
WOLFACID\_CHILI  
WOLFACID\_BARIUM  
WOLFACID\_ARGON  
WOLFACID\_ANISE  
WITHEREDFRUIT  
WILDCHOCOBO  
WAXCHIP  
WATERWINGS  
WATERCASKET  
VEILEDMAGIC  
UPPERMUTANT  
UMBRAGESPIDER  
TROPICALSTORM  
TOXICSNOW  
TOTALDAGGER  
TOADYTEAL  
THIEVESQUARTER  
SWITCHDOWN\_IR\_CD  
SWITCHDOWN\_IR\_BR  
SWITCHDOWN\_IR\_AW  
STRAITLACED  
STEELSKY\_GOLF  
STEELSKY\_FOXTROT  
STEELSKY\_ECHO  
STEELSKY\_DELTA  
SPIKEYFARM  
SPARTANFURY  
SNAPKEY  
SLYWIZARD  
SLYSNOW  
SLYNINJA  
SKYJACKBRAD  
SILVERJUMP  
SILENT\_TONGUES  
SHATTEREDSHIELD  
SHAKEWEIGHT  
SHADYNINJA  
SCARFSLOOP  
SANDPALACE  
ROLLEDHAT  
PRETZELDOG  
PLUMREVOLVER  
PHANTOMSTARFISH  
PARLAYBUFFET  
OPTIMUSPRIME

OFFICEQUARTERBACK  
OFFICELINEBACKER  
OBSCUREBLAZE  
NATIVEFLORA  
NAPALAN  
MUSHROOMKINGDOM  
MIRACLEMAX  
MILKSTEAK  
MIDNIGHTSCORPION  
MICEFUR  
MAXRANKLE  
MAGNUMOPUS\_CC  
MAGNUMOPUS  
LUTEUSASTRO  
KUKRISTEEL  
KOOPATROOPA  
KIDSHIP\_AA  
JEEPFLA\_MARKET  
JEEPFLA  
JEALOUSJOKER  
JAVAFRESCO  
INDEPENDENCEPIE  
IMPUREHOLSTER  
ICEBLOCK  
HORSEWRAP  
HASTYCOBRA  
HAMMERBROTHERS  
GOODMONKEY  
FURRYEWOK  
FREEWOODENSTICK  
FREEWINDSHEAR  
FREEWINDCLOUD  
FREEWHEELNUT  
FREEWHEELCOVER  
FREEWAYPOINT  
FREEWAVECREST  
FREEWATERTOWER  
FREEWATERTANK  
FREEWATERGLASS  
FREEWATERBED  
FREEWARRIORPAINT  
FREEVINYLMESH  
FREETWINBEE  
FREETRUEPINBALL  
FREETROUTSTREAM  
FREETRICKYKICK  
FREETINYTANK  
FREETIMESHARE  
FREETIMELEGEND  
FREETICKETBOOTH

FREETHUNDERCLOUD  
FREETESTSHEET  
FREETANKSTAND  
FREESTORAGEROOM  
FREESTONESHIP  
FREESTATEWARD  
FREESPEEDTRAP  
FREESPACEFLIGHT  
FREESNOWSHOVEL  
FREESNOWCLOUD  
FREESMOKESCREEN  
FREESMALLSPACE  
FREESLOWFAST  
FREESINEWAVE  
FREESHORTPASS  
FREESHORTCARD  
FREESEADADDY  
FREESCREENDOOR  
FREESCHOOLLOCKER  
FREESASHCORD  
FREESALTTRUCK  
FREESAFEKEY  
FREEROCKSONG  
FREERIPPINGBLADE  
FREERIGHTWHALE  
FREERIDEAROUND  
FREEREDSTAIN  
FREEREDSHIRT  
FREEREDMARKER  
FREEREDERASER  
FREEREDBEER  
FREERAVENTICKET  
FREERAINCLOUD  
FREEPULLCHAIN  
FREEPUFFYCLOUD  
FREEPOWERFAILURE  
FREEPOSTMARK  
FREEPONGPLAYER  
FREEPLASTICCASE  
FREEPINEPLANK  
FREEPICCLEBRINE  
FREEPAINTBALL  
FREEOUTRUN  
FREEOLDBIKE  
FREEOILPAINT  
FREEOILLEAK  
FREEOBLIQUECASE  
FREENIGHTTRAIN  
FREENAVYBLUE

FREEMINTJELLY  
FREEMINETUNNEL  
FREEMETALSHARD  
FREEMETALFILE  
FREEMETALCRATE  
FREEMARBLEBASIN  
FREELOLLYPOP  
FREELINEDOWN  
FREELIKESAME  
FREELIFERAFT  
FREELEADSINGER  
FREELEADSHOT  
FREELANDLINE  
FREEKNOCKOUT  
FREEKINGSPAWN  
FREEKIDPOOL  
FREEJETFUEL  
FREEHOOPDREAM  
FREEHOOKHANDLE  
FREEHOMEBASE  
FREEHAVEFUN  
FREEGLUESTRIP  
FREEGLASSTUBE  
FREEGEMSTONE  
FREEFRIEZEFRESCO  
FREEFLOWCHART  
FREEFLATFIBER  
FREEFILEDELETE  
FREEFIBERBOARD  
FREEFASTCAR  
FREEFAMILYTIE  
FREEENERGYTAX  
FREEEMUFARM  
FREEDOVETAIL  
FREEDOMECPOLA  
FREEDOGCRATE  
FREEDISKBRAKE  
FREEDISCOVERY  
FREEDIRTYTRICK  
FREEDETOURSIGN  
FREEDADBATTERY  
FREEDATALOSS  
FREEDARKSUIT  
FREECRUSHEDDISK  
FREECREEKMOOR  
FREECORNMAZE  
FREECORNHUSK  
FREECOLDTEA  
FREECLEARTAPE  
FREECHESSBOARD

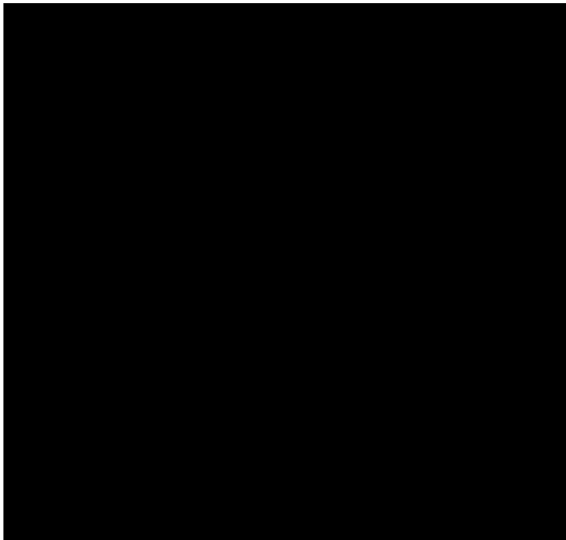
FREECHERRYCOLA  
FREECEMENTBLOCK  
FREECATBOX  
FREECANESUGAR  
FREECANALOCK  
FREEBUTTERCLOUD  
FREEBRASSBRUSH  
FREEBLUEMAT  
FREEBLOWNTURBO  
FREEBLOODYWOLF  
FREEBLACKCLOUD  
FREEBITTERCLOUD  
FREEBIGBOSS  
FREEBEACHTREE  
FREEBATTLEZONE  
FREEBALLROOM  
FREEBADRENT  
FREEBADFIBER  
FREEBACKGAMMON  
FREEARCADEZONE  
FREEAIRFARE  
FREEACIDRAIN  
FRANTICDANCER  
FOXBASE  
FOXACID  
FIRESWAMP  
FIREEATER  
FIREBRUSH  
EMPTYMOCHA  
ELECTRONSWORD  
EFFABLELAMBDA  
EDITIONHAZE  
DRUMBEAT  
DRINKMINT\_AA  
DRINKMINT  
DOUBLETAP  
DISTORTAFFECT  
DIRTDIVER  
DETASSELANJICE  
DEPUTYSHIP  
DARKTHUNDER  
DARKSCREW  
DARKRAZOR  
DARKRAVEN  
DARKINTENT  
DARKHELMET  
DARKFIRE  
CYGNUSOLOR  
CUDDLYBADGER  
CRYPTICSENTINEL

CRISPSWARE  
COCOAMELTDOWN  
COBALTGUPPY  
CHOCOLATESHIP  
CAFFEINECRASH  
BULLETTTOOTH  
BROKENTHOUGHT  
BLOODDIAMOND  
BLACKMESA  
BLACKAMETHYST  
BEEFCAKE  
BEDOUISTRIKE  
BACKSNARF  
AZTECTOMB  
ATOMICSTRIKE  
ATOMICPUNCH  
ATOMICMONKEY  
ATOMICFOG  
ATOMICFIREBALL  
ATOMICCANNON  
ARMOREDCONDOR  
APACHERIVER  
ANCIENTBREW  
AFTERYARDARM  
AFTERWINDBLOWN  
AFTERWAYBACK  
AFTERTREEFORM  
AFTERTANKERTRUCK  
AFTERSHORTRUN  
AFTERRICHGEAR  
AFTERLASTTEAM  
AFTERGASSTATION  
AFTERCLIFFDIVE  
AFTERBOOTSOLE  
ACRIDMINI  
ABSOLINEDELTA  
AARDVARKSTAKE



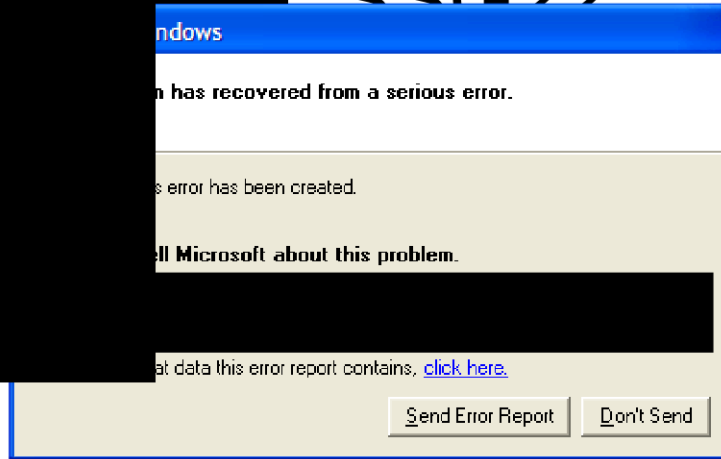
# Contributions

- 
- 
- 
- 
- 
- 



S32361

SSG22



S31322



# Windows Error Reports

- Windows crash reports in passive:
  - Identify application crashes on TAO targets
    - Another data point to correlate active/passive collection
    - Identify applications of interest on TAO machines
  - Track 4th Party tools
    - Crashes from attributed .dlls identify targets of foreign CNE
    - Analytics may be able to highlight suspicious processes



# Windows Error Reports

**Detailed error and target system info for troubleshooting, tracking, and maintenance**

Event Type	Exception Code	Exception Offset	Fault Module Timestamp	Count
APPCRASH	c0000005	01cb3aa6	411096b4	8
APPCRASH	c0000005	01903aa6	411096b4	6
APPCRASH	c0000005	03573aa6	411096b4	6
APPCRASH	c0000005	047b3aa6	411096b4	6
APPCRASH	c0000005	01bf3aa6	411096b4	4
APPCRASH	c0000005	03993aa6	411096b4	2
BEX	00653aa6	c0000005	411096b4	2
BEX	01e13aa6	c0000005	411096b4	2
BEX	01f63aa6	c0000005	411096b4	2
BEX	03083aa6	c0000005	411096b4	2
BEX	03bd3aa6	c0000005	411096b4	2
BEX	0ca13aa6	c0000005	411096b4	2

System Manufacturer	System Product Name	BIOS Version	Count
FUJITSU SIEMENS	AMILO Pro V2040	R01-A1B	30
Hewlett-Packard	Presario CQ56 Notebook PC	F.05	14
TOSHIBA	SATELLITE U500	1.50	6
TOSHIBA	Satellite C640	1.50	3
		PRG3110H.86A.0065.20	2
Hewlett-Packard	HP Mini 110-3700	F.23	2
TOSHIBA	Satellite L300	1.40	2
TOSHIBA	Satellite L635	1.40	2
TOSHIBA	Satellite P105	V3.30	2
Dell Inc.	OptiPlex 755	A09	1
System manufacturer	System Product Name	0701	1

Application Version	OS Version	Count
8.0.7600.16800	6.1.7600.2.00010100.0.0.1.16385	30
8.0.7600.16869	6.1.7600.2.00010300.0.0.11.16385	14
8.0.7600.16385	6.1.7600.2.00010100.0.0.1.16385	8
8.0.7600.16839	6.1.7600.2.00010300.0.0.3.16385	6
8.0.7600.16869	6.1.7600.2.00010300.0.0.3.16385	3
8.0.7600.16869	6.1.7600.2.00010100.0.0.1.16385	2
8.0.7601.17514	6.1.7601.2.00010100.1.0.48.17514	2

IE8

Windows 7



# Crashes on TAO Targets

Value Name ▲	Value Type	Display Content
errorport	REG_SZ	WindowsErrorReportingServicePort
machineid	REG_SZ	34F9B1DE-9D71-4009-AE54-65C45C1F876F
maxqueuesizepercentage	REG_DWORD	00000001
purgethresholdvalueinkb	REG_DWORD	0000000A
servicetimeout	REG_DWORD	0000EA60

Registry keys from  
CNE

Error report in passive

GET /StageOne/Generic/BEX/iexplore\_exe/8\_0\_7601\_17514/4ce79912/IEBHO\_dll\_unloaded/0\_0\_0\_0/4e4178b9/603f1430/c0000005/00000008.htm?LCID=3081 &OS=6.1.7601.2.00010100.1.0.1.17514 &SM=Hewlett-Packard &SPN=HP Pavilion dm3 Notebook PC &BV=F.03 &MID=34F9B1DE-9D71-4009-AE54-65C45C1F876F HTTP/1.1

Connection: Keep-Alive  
User-Agent: MSDW  
Host: watson.microsoft.com

Passive access to  
CNE target

Application Name	Sigad	Casnotation	Fm IP	Count ▼
iexplore.exe	USJ-759A	E9DCJ00000M0000		32
AcroRd32.exe	USJ-759A	E9DCJ00000M0000		1
Flash Games.exe	USJ-759A	E9DCJ00000M0000		1



# Windows Error Reports

- Similar work completed for Windows Update
  - April 2012:
    - 2827 Windows Update and Windows Error IDs from endpoints
    - 17 CNE Machines found in Passive (8 for the first time, for other 9 it's the first time with MachineID)
- Crashes from 4th party Tools
  - At least one crash report from a likely 4th party found
  - Ingesting into The Cloud for Whizbang! analytics
    - Crashes from target networks
    - Crashes of uncommon .dlls
    - Crashes of known 4th party .dlls





# But Also...

- Windows crash reports in passive:
  - Reveal crashes of TAO tools on targets
    - Troubleshoot problems with TAO tools
    - Identify OPSEC issues from repeated crashes

Datetime	Application Name	Fault Module Name
2012-01-19 11:57:45	iexplore.exe	.dll_unloaded
2012-01-19 11:57:45	iexplore.exe	.dll_unloaded
2012-01-19 11:57:45	iexplore.exe	.dll_unloaded
2012-01-19 07:44:28	iexplore.exe	.dll_unloaded
2012-01-19 11:57:45	iexplore.exe	.dll_unloaded
2012-01-19 18:57:11	iexplore.exe	.dll_unloaded
2012-01-19 18:57:47	iexplore.exe	.dll_unloaded
2012-01-19 18:58:39	iexplore.exe	.dll_unloaded
2012-01-19 18:59:48	iexplore.exe	.dll_unloaded
2012-01-19 20:03:23	iexplore.exe	.dll_unloaded

.dll unique to TAO  
VALIDATOR first-stage  
implant



# Aftermath

- Setup automated workflow for TAO VALIDATOR team to receive daily updates
- 10-30 crashes per day
- In a month ~30 machines
- Pinpointed to:
  - VALIDATOR 8.2.5.1
  - VALIDATOR 12
  - Win 7 32bit
- TAO/ROC Mission Directors deciding way forward



QUESTIONS?



# SIGINT FORENSICS CENTER

(S//REL) *Tracking Courier Use of  
Secure Digital Cards*

SIGDEV Conference 2012  
The overall classification of this briefing is:

**TOP SECRET//COMINT//REL FVEY**

Derived From: NSA/CSSM 1-52 Dated: 20070108 Declassify On: 20320108

# (U//FOUO) SD Cards

(U//FOUO) Small

(U//FOUO) Convenient

(U//FOUO) Common

(S//REL) Used by targets

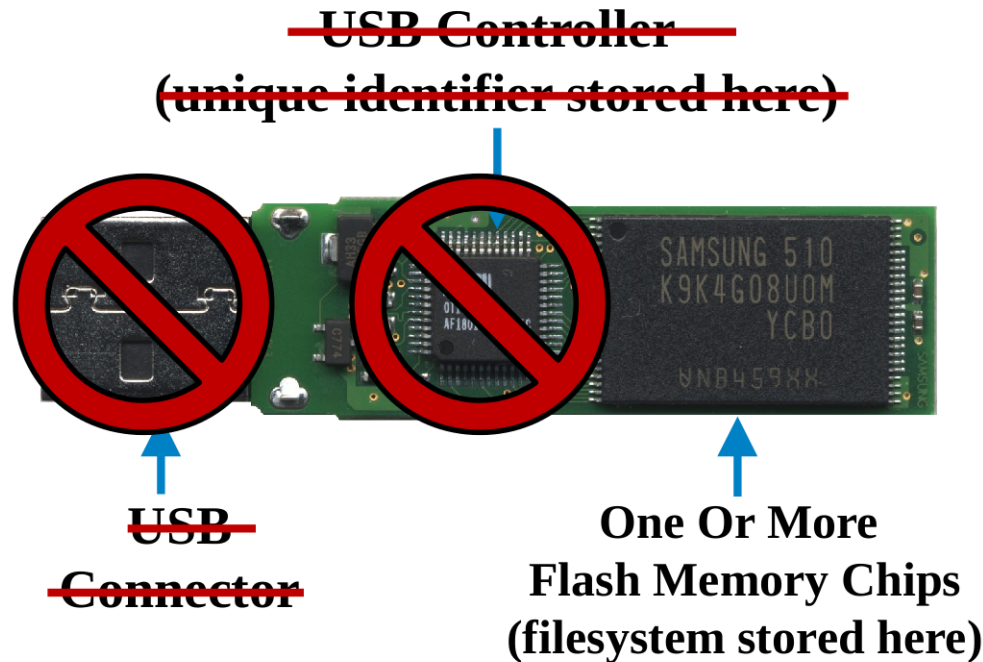


# (S//REL) Tracking SD Cards: The

## Problem

(U//FOUO) No USB Controller

(U//FOUO) FAT Filesystem



(S//REL) The solution: Volume Identification

(U//FOUO) VSN: Volume Serial Number

(U//FOUO) VL: Volume Label

**Actual Values:**

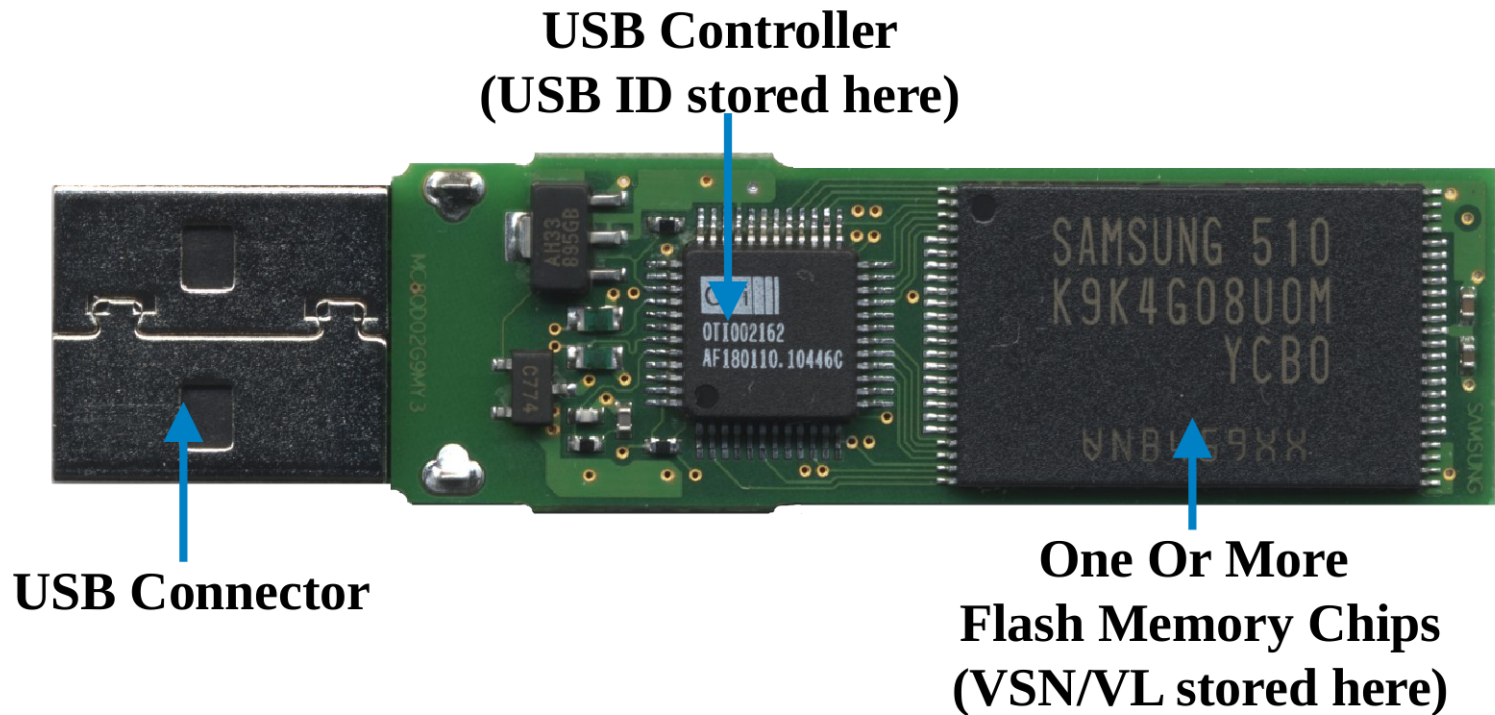
Usama	728c0200
Nokia N73	a7bec691
Google_earth	65ba457d

C

*Located in the boot sector of a volume*

*\*CDs and DVDs also contain VSN/VLs*

# (S//REL) Unique USB Identification

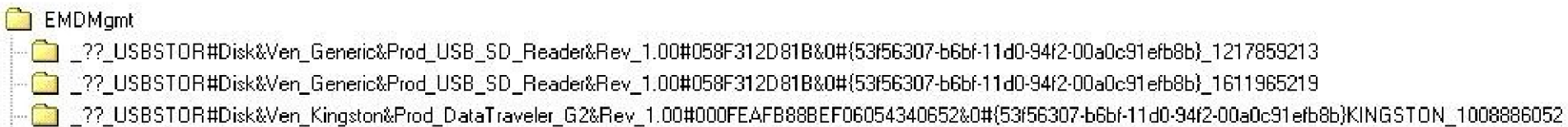






## (S//REL) VSN/VL Sources

- (S//REL) Filesystem/Volume boot sector
- (S//REL) Windows Registry
  - (S//REL) Vista/7 provide comprehensive history



- (S//REL) XP provides VSN for “last mounted”
- (S//REL) LNK files
  - (S//REL) Identify VSN/VL, device type (CD, removable media, etc)



## (S//REL) VSN/VLs & UBL

(S//REL) Published report (S/OO/SFC/3-12)

(S//REL) Identification information identified for  
36 devices not seized during UBL raid  
16 Missing devices

6 Connected via SD Reader

5 via USB

5 unknown

(S//REL) Determined uniqueness & first  
connect date



# (U//FOUO) Developing a Solution

(TS//SI//REL)



(TS//SI//REL) **Automated solutions between seized media & CNE media via JOLLYROGER**

(TS//SI//REL)



(U//FOUO) Questions?

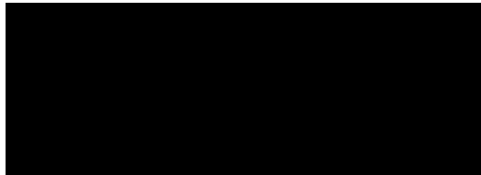
# NSA SIGINT Forensics Center



**“GO SFC”**

# QUANTUMFALCON

## Summarization to support QUANTUM Targeting



## Overview

### Challenges

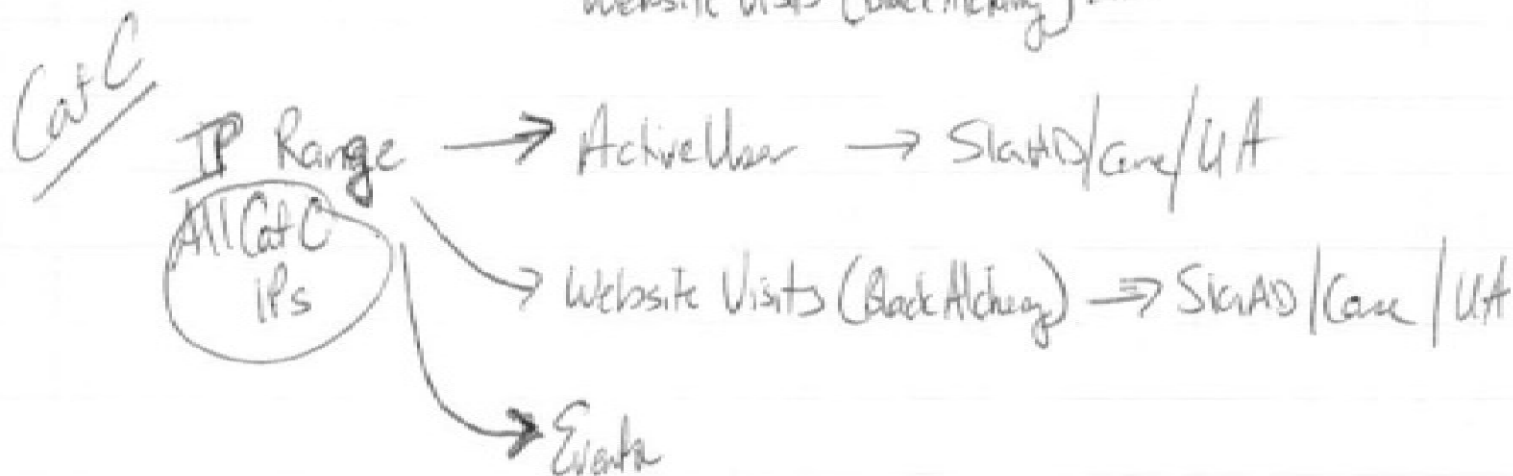
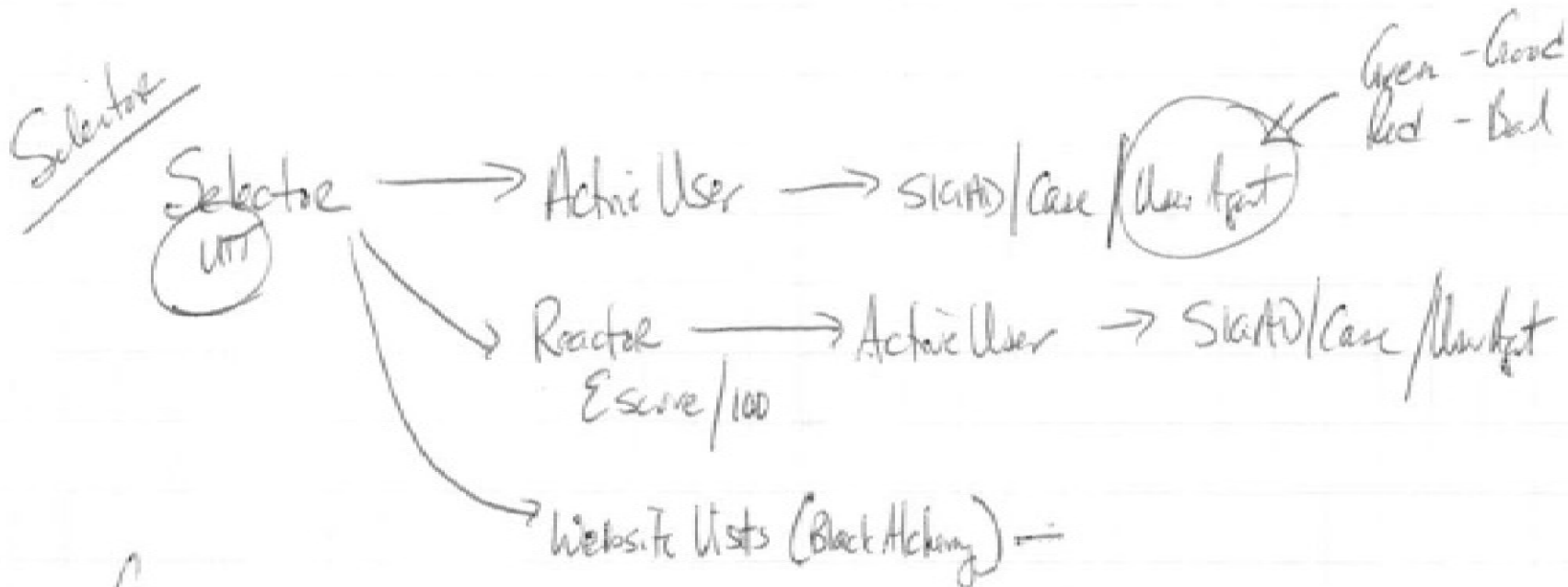
- Triage selectors for potential QUANTUM targeting
- Enrich with strongly correlated selectors
- Possible manually with MARINA with multiple queries (no workflows)

## Overview

### Solution

- Cloud analytic developed to support targeting
- Map/Reduce ideal for counting activity
- Using corporate resources to perform activities
  - Seed selector list – INQUIRY service
  - Summary of ASDF data already on GHOSTMACHINE
  - REACTOR E score data inside ASDF records (User = User Atom)
  - UTT sent daily to GHOSTMACHINE

# The Napkin





# What does it look like?

Selector	AltID	UTTCategory	SIGAD	CASENOTATION	IPDirecti	From	FromASN	To	ToASN	#TRSI	#DaysSec	La
100000227785040<facebook>		6587:FGS2A4	US-972U	AF.QXAP0S000000	C->S	AF	38742	US	32934	1	1	20
100000227785040<facebook>		6587:FGS2A4	US-972U	AF.QXAP0S	C->S	AF	38742	US	32934	1	1	20
100000603891507<facebook>			UKC-302A	PKCSE035K000H0D0	C->S	PK	45595	US	26101	2	1	20
100000603891507<facebook>			UKC-302A	PKCSE035L000H0D0	C->S	PK	45595	US	26101	2	2	20
100000677501875<facebook>			UKC-302A	PKCSE068A000H0D0	C->S	PK	45595	BG	32934	1	1	20
100000677501875<facebook>			UKC-302A	PKCSE068A000H0D0	C->S	PK	45595	US	32934	8	2	20
100000677501875<facebook>			UKC-302A	PKCSE068A000H0D0	S->C	US	32934	PK	45595	1	1	20
100000692006670<facebook>		60:S2A13	USD-1079	H5V035343960000	S->C	US	32934	SG	7700	9	2	20
100000727045165<facebook>		1860:S2A63 238C	UKC-302A	PKCSE035L000H0D0	C->S	PK	45595	US	26101	2	1	20
100000727045165<facebook>		1860:S2A63 238C	UKC-302A	PKCSE039K000H0D0	C->S	PK	45595	US	14778	66	2	20
100000727045165<facebook>		1860:S2A63 238C	UKC-302A	PKCSE039K000H0D0	C->S	PK	45595	US	36646	28	3	20
100000727045165<facebook>		1860:S2A63 238C	UKC-302A	PKCSE039L000H0D0	C->S	PK	45595	US	14778	81	4	20
100000727045165<facebook>		1860:S2A63 238C	UKC-302A	PKCSE039L000H0D0	C->S	PK	45595	US	36646	40	4	20
100000820627286<facebook>			USJ-759A	5BDAZ0000M0000	S->C	BG	32934	IQ	16212	26	1	20
100000820627286<facebook>			USJ-759A	5BDAZ0000M0000	S->C	US	32934	IQ	16212	215	4	20
100000820627286<facebook>			USJ-759	5BDAZ0000MID03	C->S	IQ	16212	BG	32934	36	3	20
100000820627286<facebook>			USJ-759	5BDAZ0000MID03	C->S	IQ	16212	US	32934	70	4	20
100001442593682<facebook>		2783:F74	US-966A	E2H115434620000	S->C	US	8075	XX	-	531	6	20
100001442593682<facebook>		2783:F74	US-966A	E2H115434620000	null	-	-	-	-	9	1	20
100001442593682<facebook>		2783:F74	US-966A	E2H1154346000TD	C->S	XX	-	IE	32934	5	1	20
100001442593682<facebook>		2783:F74	US-966A	E2H1154346000TD	C->S	XX	-	US	32934	2	1	20
100001442593682<facebook>		2783:F74	US-966A	E2H115434620000	S->C	IE	32934	XX	-	49	4	20
100001442593682<facebook>		2783:F74	US-966A	E2H115434620000	S->C	US	32934	XX	-	50	6	20
100001450912744<facebook>			UKC-302A	PKCSE035K000H0D0	C->S	PK	45595	US	26101	2	2	20
100001450912744<facebook>			UKC-302A	PKCSE035L000H0D0	C->S	PK	45595	US	26101	1	1	20
100001751863833<facebook>			UKC-302A	PKCSE035K000H0D0	C->S	AF	55330	US	26101	1	1	20
100001751863833<facebook>			US-968Z	K5H110900004144	S->C	US	32934	AF	23649	5	1	20
100002135632573<facebook>		2381:SV 4318:S2	UKC-302A	PKCSE072A000H0D0	C->S	PK	45595	US	32934	5	1	20
100002135632573<facebook>		2381:SV 4318:S2	UKC-302A	PKCSE072A000H0D0	S->C	US	32934	PK	45595	1	1	20

# What does it look like?

Selector	AltID	SIGAD	CASENOTATION	IPDirecti	FromIP	From	ToIP	To	#TRSI	#DaysSec
100000227785040<facebook>		US-972U	AF.QXAP0S000000	C->S		AF		US	1	
100000227785040<facebook>		US-972U	AF.QXAP0S	C->S		AF		US	1	
100000692006670<facebook>		USD-1079	H5V035343960000	S->C		US		SG	1	
100000692006670<facebook>		USD-1079	H5V035343960000	S->C		US		SG	3	
100000692006670<facebook>		USD-1079	H5V035343960000	S->C		US		SG	5	
100000820627286<facebook>		USJ-759A	5BDAZ00000M0000	S->C		US		IQ	152	
100000820627286<facebook>		USJ-759A	5BDAZ00000M0000	S->C		US		IQ	35	
100000820627286<facebook>		USJ-759A	5BDAZ00000M0000	S->C		BG		IQ	26	
100000820627286<facebook>		USJ-759A	5BDAZ00000M0000	S->C		US		IQ	9	
100000820627286<facebook>		USJ-759A	5BDAZ00000M0000	S->C		US		IQ	19	
100000820627286<facebook>		USJ-759	5BDAZ00000MID03	C->S		IQ		US	5	
100000820627286<facebook>		USJ-759	5BDAZ00000MID03	C->S		IQ		US	34	
100000820627286<facebook>		USJ-759	5BDAZ00000MID03	C->S		IQ		US	24	
100000820627286<facebook>		USJ-759	5BDAZ00000MID03	C->S		IQ		BG	2	
100000820627286<facebook>		USJ-759	5BDAZ00000MID03	C->S		IQ		BG	31	
100000820627286<facebook>		USJ-759	5BDAZ00000MID03	C->S		IQ		BG	3	
100000820627286<facebook>		USJ-759	5BDAZ00000MID03	C->S		IQ		US	2	
100000820627286<facebook>		USJ-759	5BDAZ00000MID03	C->S		IQ		US	3	
100000820627286<facebook>		USJ-759	5BDAZ00000MID03	C->S		IQ		US	1	
100000820627286<facebook>		USJ-759	5BDAZ00000MID03	C->S		IQ		US	1	
100001442593682<facebook>		US-966A	E2H115434620000	S->C		US		XX	8	
100001442593682<facebook>		US-966A	E2H115434620000	S->C		US		XX	1	
100001442593682<facebook>		US-966A	E2H115434620000	S->C		US		XX	63	
100001442593682<facebook>		US-966A	E2H115434620000	S->C		US		XX	4	
100001442593682<facebook>		US-966A	E2H115434620000	S->C		US		XX	127	
100001442593682<facebook>		US-966A	E2H115434620000	S->C		US		XX	17	
100001442593682<facebook>		US-966A	E2H115434620000	S->C		US		XX	28	
100001442593682<facebook>		US-966A	E2H115434620000	S->C		US		XX	90	
100001442593682<facebook>		US-966A	E2H115434620000	S->C		US		XX	21	
100001442593682<facebook>		US-966A	E2H115434620000	S->C		US		XX	1	
100001442593682<facebook>		US-966A	E2H115434620000	S->C		US		XX	1	
100001442593682<facebook>		US-966A	E2H115434620000	S->C		US		XX	24	
100001442593682<facebook>		US-966A	E2H115434620000	S->C		US		XX	6	
100001442593682<facebook>		US-966A	E2H115434620000	S->C		US		XX	9	
100001442593682<facebook>		US-966A	E2H115434620000	S->C		US		XX	1	
100001442593682<facebook>		US-966A	E2H115434620000	S->C		US		XX	61	
100001442593682<facebook>		US-966A	E2H115434620000	S->C		US		XX	1	
100001442593682<facebook>		US-966A	E2H115434620000	S->C		US		XX	1	
100001442593682<facebook>		US-966A	E2H115434620000	S->C		US		XX	10	

Hits CaseNotationCounts IPHits

1105 of 31950 records found

Average: 10060205.58 Count: 14378 Sum: 44466108682

100%

**Issues****Questions**