(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

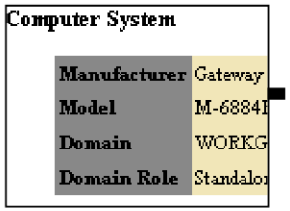
endpoint/related/WICKEDAMP11/user*
endpoint/related/WICKEDAMP11/network*
endpoint/related/WICKEDAMP11/machineID*
endpoint/related/WICKEDAMP11/cypher_key*
endpoint/related/WICKEDAMP11/attached_device*

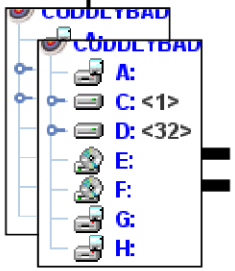
Serial numbers
Hostmacs

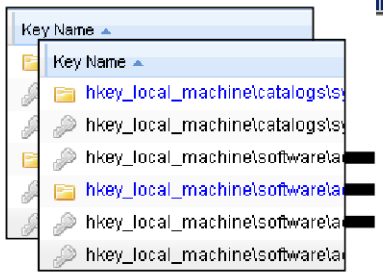
usernames

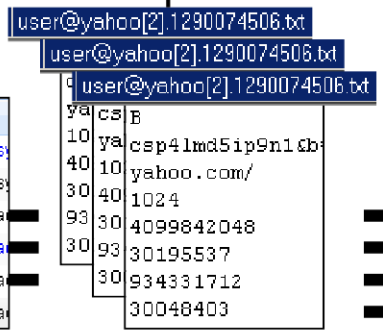
IMEIs
UDIDs
Browser tags
usernames

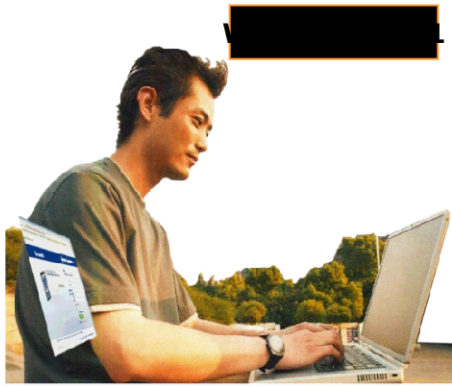
machineIDs











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

User Leads

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

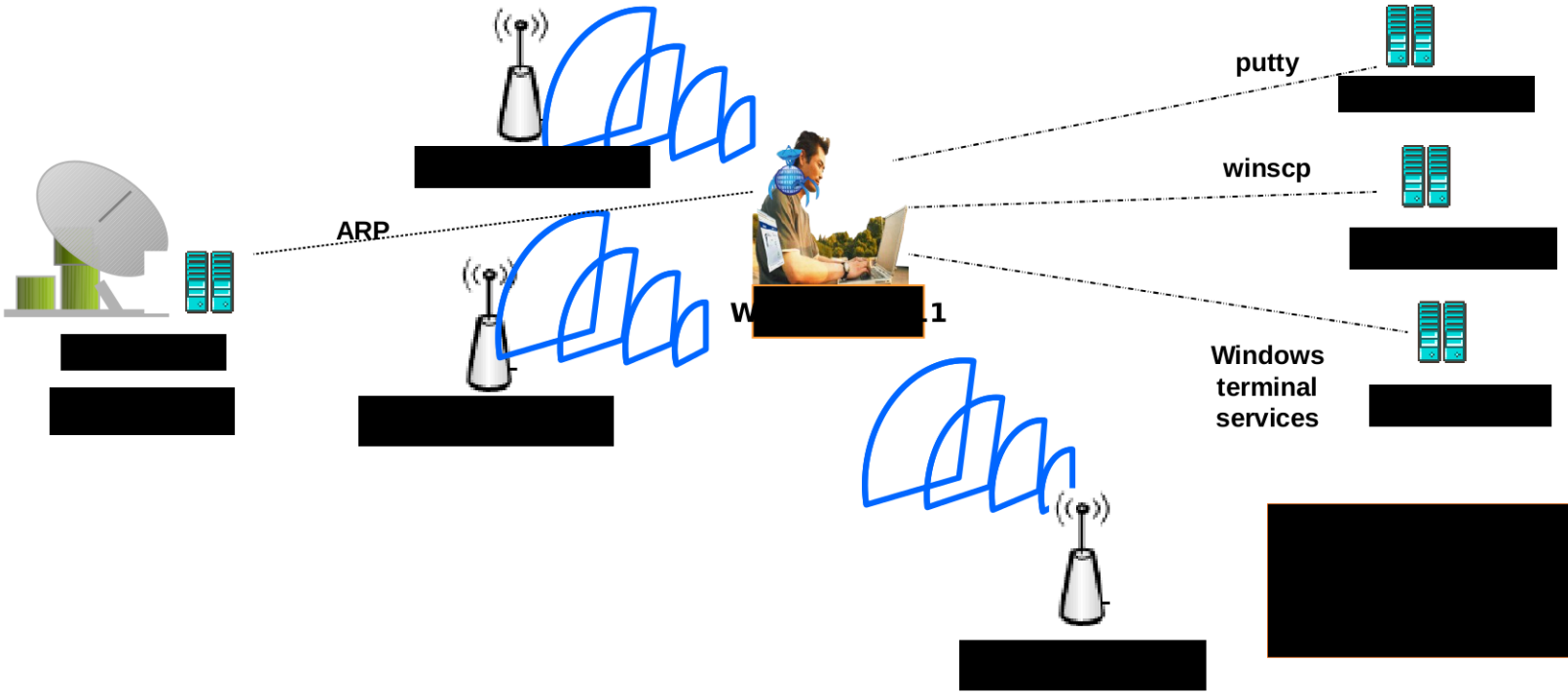
Network

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

Network Level Selectors

[redacted]

[redacted]

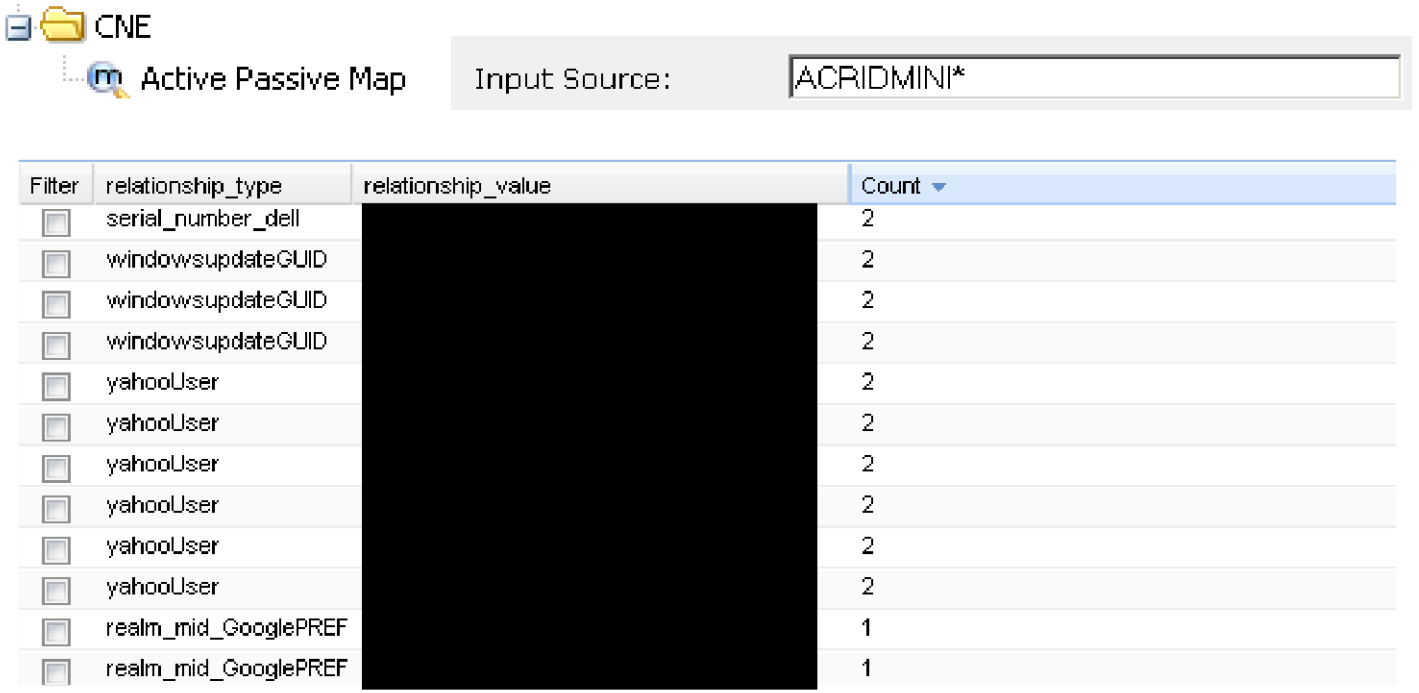


[redacted]

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

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



Sample Lifecycle: DARKSCREW46

[redacted]

Machine Info

DARKSCREW/DARKSCREW46

Last Collection[limit 3 listed]:

- 2012-02-12
- 2012-02-08
- 2012-02-06

List All Collection

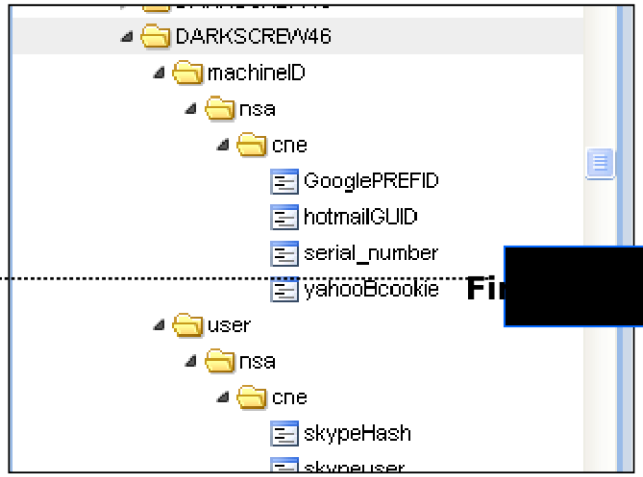
Categorized Collection

[redacted]

relationship_type	relationship_value	Input Source
serial_number_lenovo	L3PVV286	DARKSCREW46
hotmailGUID	0574A0786A9C6AD13CCDA29F6E9C6A60	DARKSCREW46
hotmailGUID	10F3D90D305A6CAA3939DBEA345A6CC3	DARKSCREW46
hotmailGUID	277D434B01A0648503DE419705A064E0	DARKSCREW46
doubleclickID	22bcd6191801009a	DARKSCREW46
doubleclickID	22fd816a5401001b	DARKSCREW46
facebookMachine	e0yyTZC6VhXJBtTsemghIlfZ	DARKSCREW46
GooglePREFID	3064562fddcfcd52	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]		DS-200X	mail
		DS-200X	chat
		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

*Last updated 11

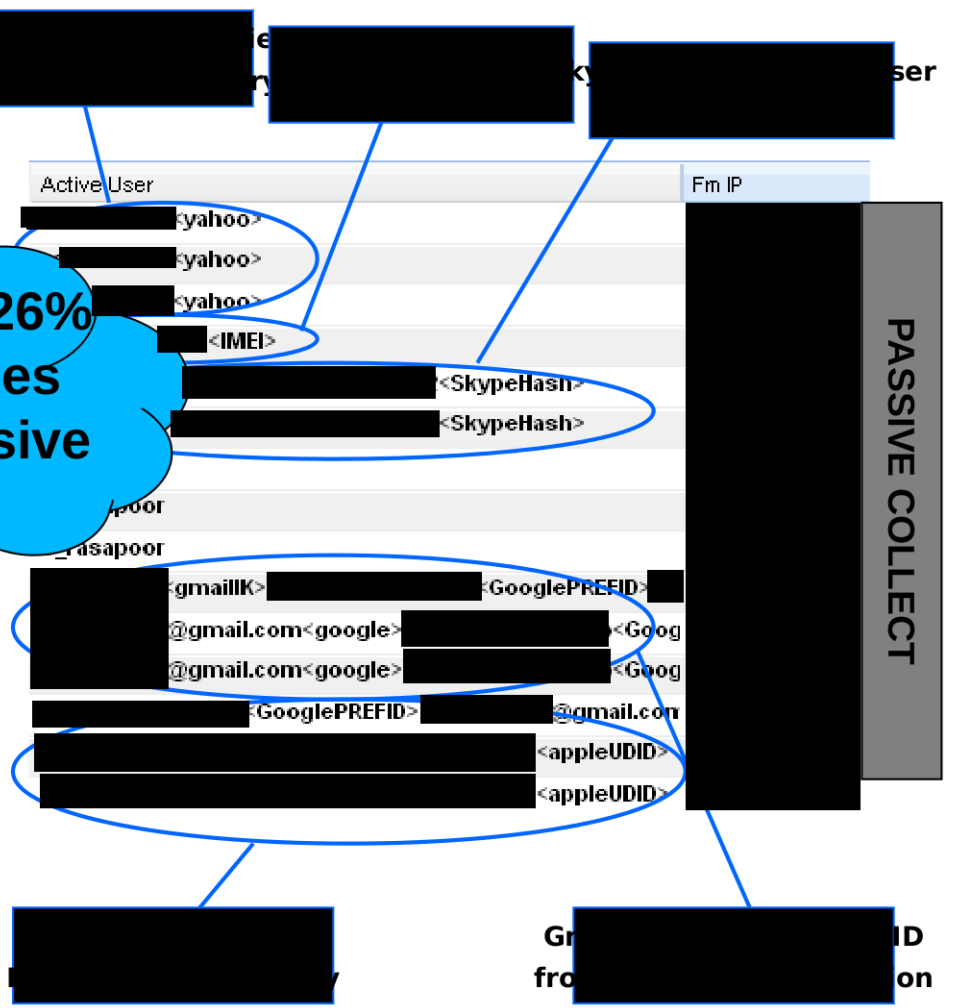
SPINALTAP Fingerprint Hits

Since activa[redacted] July 2011:

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

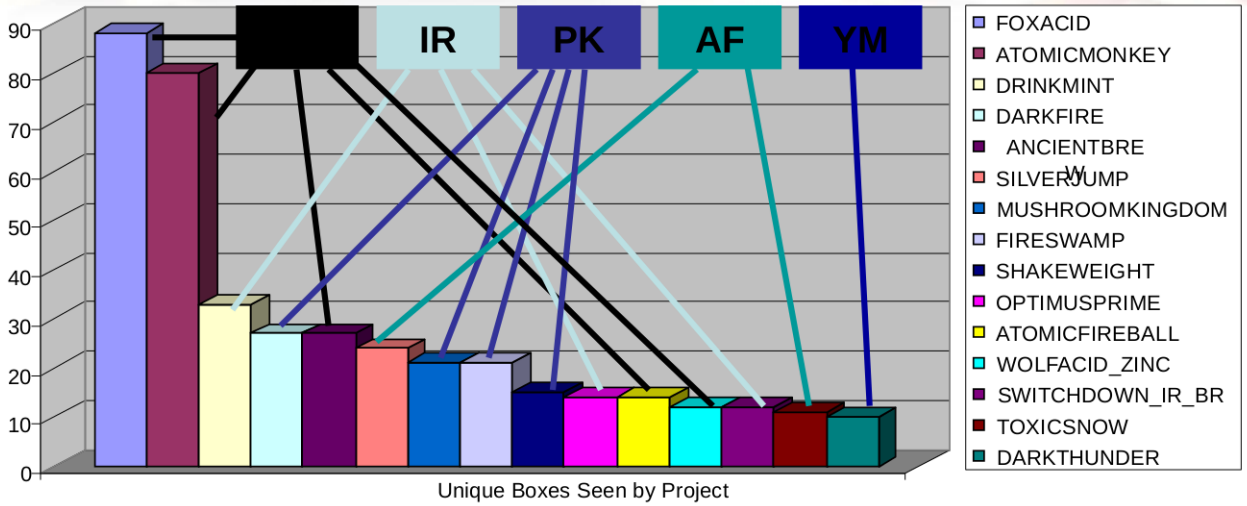
Selectors from 26% of TAO Machines are seen in Passive

Sigad	AppID (+Fingerprints)
UKJ-260D	endpoint/related/SIL[redacted]
USJ-759A	endpoint/related/SILVE[redacted]
UKJ-260D	endpoint/related/SILVERJU[redacted]
UKC-302A	endpoint/related/SLYNINJA15[redacted]
UKJ-260D	endpoint/related/SLYWIZARD16/user/nsa/cne/[redacted]
UKJ-260G	endpoint/related/SLYWIZARD16/user/nsa/cne/yahooUser
UKJ-260D	endpoint/related/SLYWIZARD21/user/nsa/cne/skypeuser
UKJ-260D	endpoint/related/SPARTANFURY16/user/nsa/cne/skypeuser
DS-300	endpoint/related/STRAITLACED554/user/nsa/cne/yahooUser
DS-300	endpoint/related/SWITCHDOWN_IR_BR152/user/nsa/cne/yahooUser
DS-300	endpoint/related/SWITCHDOWN_IR_BR245/user/nsa/cne/yahooUser
DS-300	endpoint/related/SWITCHDOWN_IR_BR246/user/nsa/cne/yahooUser
UKC-302A	endpoint/related/THIEVESQUARTER25/user/nsa/cne/yahooUser
DS-300	endpoint/related/WATERCASKET103/machineID/nsa/cne/simbar



*Last updated 11

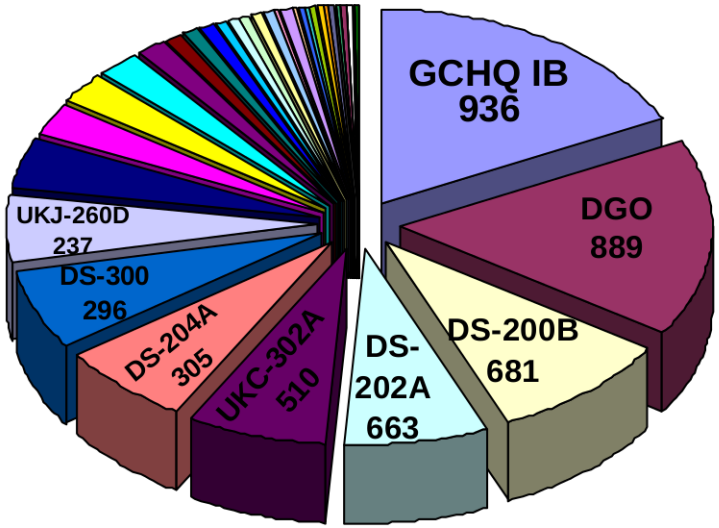
Hits by Project/Site



Unique Machines Seen by Project

(Top 15 projects)

Unique Machines seen by SIGAD

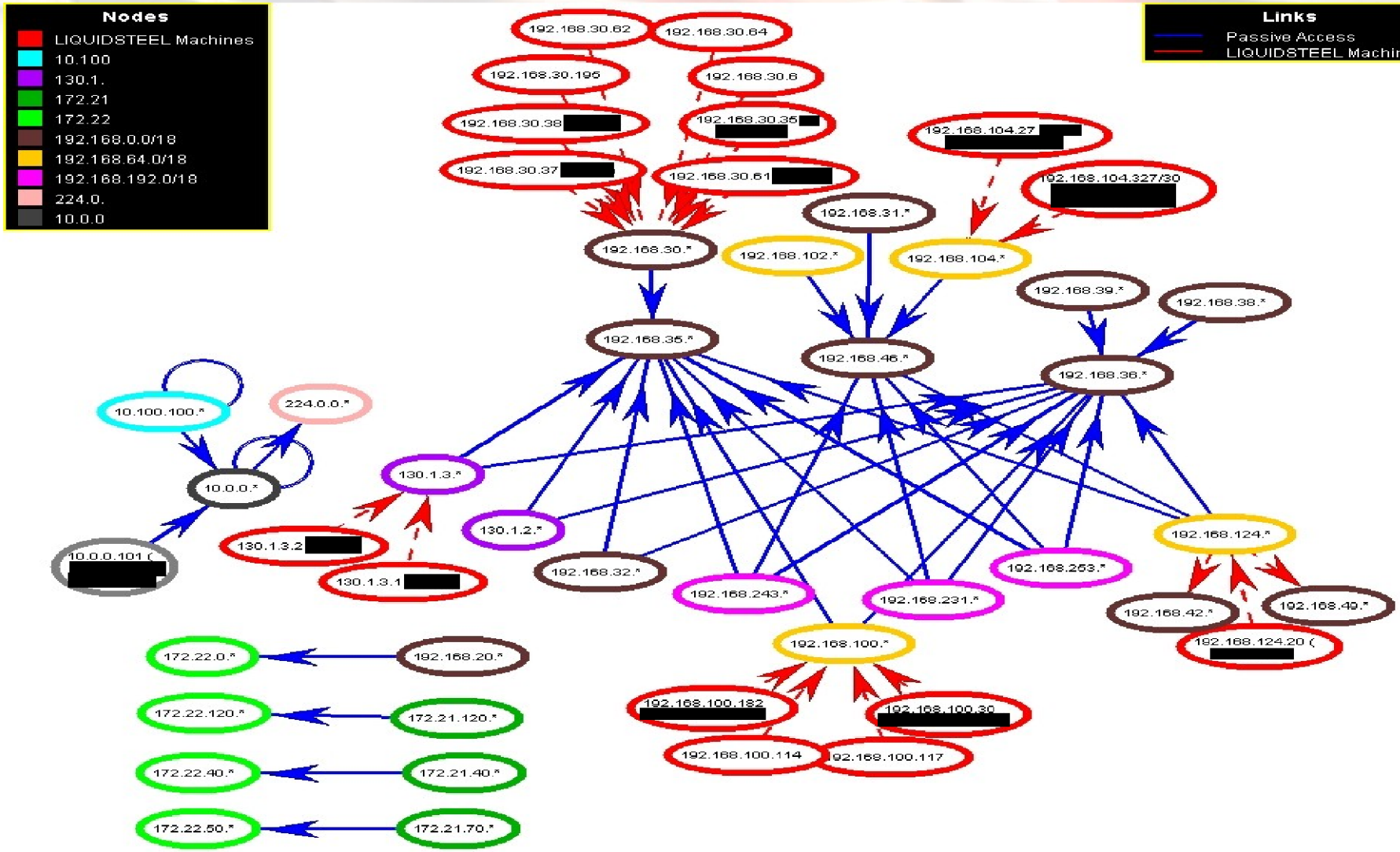


1619 unique machines seen

At 68 different sigads

Using 31 different ID types

Application: Exfil Opportunities



Application: Bearer Prioritization

Home | All Questions | All CASNs | Survey CASNs | ASPHALT CASNs | Snap CASNs

Show 50 entries | Refresh | First

id	topic	weight	run_interval	valid_length	description
	spinal				
113	SPINALTAP	50	1	30	Case notation ge points for each t correlation seen each CNE projec

SPINALTAP

Show 25 entries | Refresh | First

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	2012-02-12
2CBAB00000M0286	cne_related/DRINKMINT158/user/nsa/yahooUser	2012-02-04
2CBAB00000M0286	cne_related/DRINKMINT195/user/nsa/yahooUser	2011-12-20
2CBAB00000M0286	cne_related/DRINKMINT322/user/nsa/yahooUser	2012-02-03
2CBAB00000M0286	cne_related/DRINKMINT350/user/nsa/yahooUser	2012-01-27
2CBAB00000M0286	cne_related/DRINKMINT384/user/nsa/yahooUser	2012-02-01
2CBAB00000M0286	cne_related/DRINKMINT410/user/nsa/yahooUser	2012-02-03
2CBAB00000M0286	cne_related/DRINKMINT420/user/nsa/yahooUser	2012-02-12

Application: Target Relationships

Histogram Grid

Page 1 of 1 | Clear Selection | Export | Interactive Mode

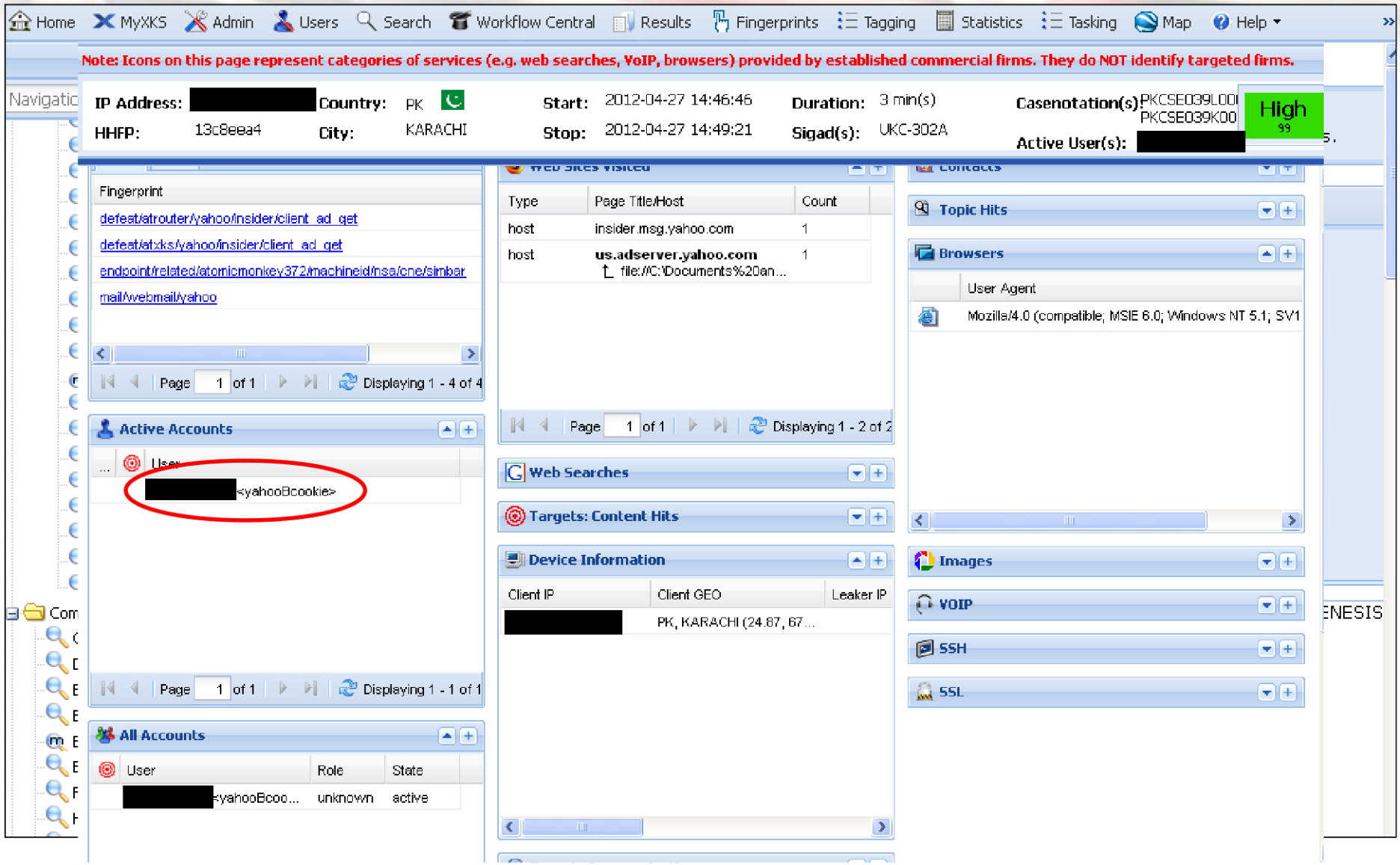
Filter	Input Source	Count
	WOLFACID_PRECIOUS5	82
	DOUBLETAP23	45
	DOUBLETAP14	33
	WOLFACID_URANIUM1	24
	WOLFACID_IODINE1	16
	WOLFACID_PRECIOUS4	13
	WOLFACID_ARGON8	12
	WOLFACID_IRON10	12
	ATOMICFOG40	8
	OFFICELINEBACKER105	8
	OFFICELINEBACKER90	8
	DOUBLETAP11	7
	WOLFACID_BARIUM49	7

ejkeyid

Help | Actions | Reports | View | Map View | FILTERS:

	State	ID	Datetime	Highlights	AppID (+Fingerprints)
1		255	2011-12-14 23:53:00		dnt_payload/file cne/technique/unitedrake cyber/cyberquest/cno_activity dnt_payload/header_parsed encryption/
2		214	2011-05-20 18:41:00		dnt_payload/file cne/technique/unitedrake cyber/cyberquest/cno_activity dnt_payload/header_parsed encryption/
3		215	2011-05-20 20:08:00		dnt_payload/file cne/technique/unitedrake cyber/cyberquest/cno_activity dnt_payload/header_parsed encryption/
4		438	2011-11-03 18:31:00		dnt_payload/file cne/technique/unitedrake cyber/cyberquest/cno_activity dnt_payload/header_parsed encryption/
5		85	2011-11-30 21:42:00		dnt_payload/file VPN/Site_to_Site_VPN/More_Setup_titles_subjects_or_filenames ccne/Discovery/MobileTerms c
6		243	2011-10-25 19:59:00		dnt_payload/file cne/technique/danderspritz cyber/cyberquest/cno_activity dnt_payload/header_parsed encryptio
7		244	2011-10-25 20:00:00		dnt_payload/file cne/technique/danderspritz cyber/cyberquest/cno_activity dnt_payload/header_parsed encryptio
8		257	2011-10-25 20:07:00		dnt_payload/file cne/technique/danderspritz cyber/cyberquest/cno_activity dnt_payload/header_parsed encryptio

Application: Selector Discovery



REENABLE

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

active_user_id	id_type	machine_name	q_technique	sigad	opportunity_type	unique_cour
[redacted]	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	SWITCHDOWN_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

Sigad
UKJ-2600
UKJ-2600
UKJ-2600
UKJ-2600
UKJ-2600
UKJ-2600
UKJ-2600
UKJ-2600
UKJ-2600
UKJ-2600
UKJ-2600
UKJ-2600
UKJ-2600
UKJ-2600
UKJ-2600
UKJ-2600
UKJ-2600
UKJ-2600
UKJ-2600
UKJ-2600
UKJ-2600
UKJ-2600
UKJ-2600
UKJ-2600
UKJ-2600
UKJ-2600

5 2012/01/11 08:00
L 2012/01/04 09:05
4 2011/12/02 13:47
3 2011/11/28 22:54
3 2011/11/28 20:27
5 2011/11/13 07:56
) 2011/11/12 10:12
7 2011/11/03 11:40
3 2011/10/11 12:18

REENABLE

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 25 entries — Refresh

active_user_id	from_port	to_port	id_type	machine_name	opportunity_type	q_technique	sigad	last_callback
[redacted]	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
JEEPFLEA_MARKET
JEEPFLEA
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
FREEPICKLEBRINE
FREEPAINTBALL
FREEOUTRUN
FREEOLDBIKE
FREEOILPAINT
FREEOILLEAK
FREEOBLIQUECASE
FREENIGHTTRAIN
FREENAVYBLUE

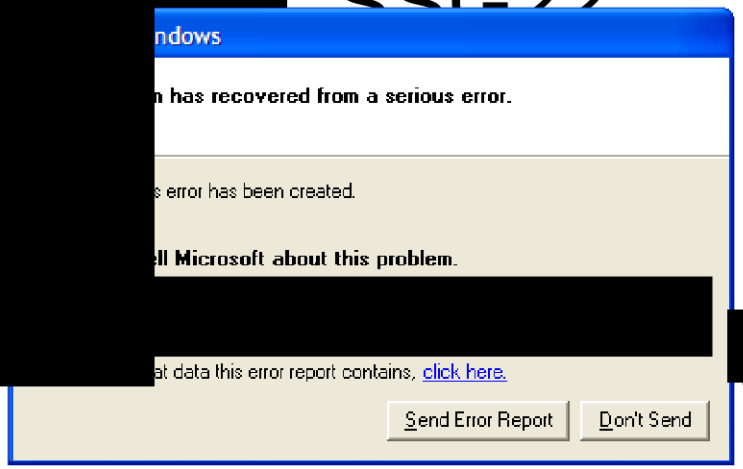
FREEMINTJELLY
FREEMINETUNNEL
FREEMETALSHARD
FREEMETALFILE
FREEMETALCRATE
FREEMARBLEBASIN
FREELOLLYPOP
FREELINEDOWN
FREELIKESAME
FREELIFERAFT
FREELEADSINGER
FREELEADSHOT
FREELANDLINE
FREEKNOCKOUT
FREEKINGSPAWN
FREEKIDPOOL
FREEJETFUEL
FREEHOOPDREAM
FREEHOOKHANDLE
FREEHOMEBASE
FREEHAVEFUN
FREEGLUESTRIP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

FREECHERRYCOLA
FREECEMENTBLOCK
FREECATBOX
FREECANESUGAR
FREECANALLOCK
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
DETASSELJANICE
DEPUTYSHIP
DARKTHUNDER
DARKSCREW
DARKRAZOR
DARKRAVEN
DARKINTENT
DARKHELMET
DARKFIRE
CYGNUSOLOR
CUDDLYBADGER
CRYPTICSENTINEL

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

Contributions

- [redacted] S32361
- [redacted] SSG22
- [redacted]
- [redacted]
- [redacted] 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.0065.2(	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

SLYNINJA151

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

Registry keys from CNE

Error report in passive

SLYNINJA151

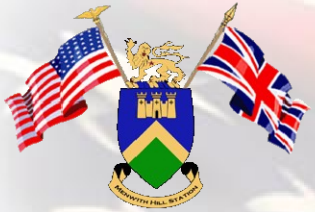
GET /StageOne/Generic/BEX/iexplore_exe/8_0_7601_17514/4ce79912/IEBHO_dll_unloaded/0_0_0_0/4e4178b9/603f1430/c0000005/00000008.htm?LCID=3081 &OS=6.1.7601.2.00010100.1.0.1.17514 &SM=Hewlett-Packard &SPN=HP Pavilion dm3 Notebook PC &BV=F.03 &MID=34F9B1DE-9D71-4009-AE54-65C45C1F876F HTTP/1.1

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

Passive access to CNE target

SLYNINJA151

Application Name	Sigad	Casenotation	Fm IP	Count
iexplore.exe	USJ-759A	E9DCJ00000M0000	[redacted]	32
AcroRd32.exe	USJ-759A	E9DCJ00000M0000	[redacted]	1
Flash Games.exe	USJ-759A	E9DCJ00000M0000	[redacted]	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…

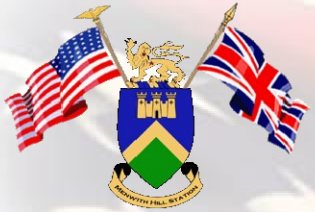
- Windows crash reports in passive:
  - Reveal crashes of TAO tools on targets
    - Troubleshoot problems with TAO tools
    - Identify OPSEC issues from repeated crashes

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