

(U) Fourth Party Opportunities



4th Party IPT

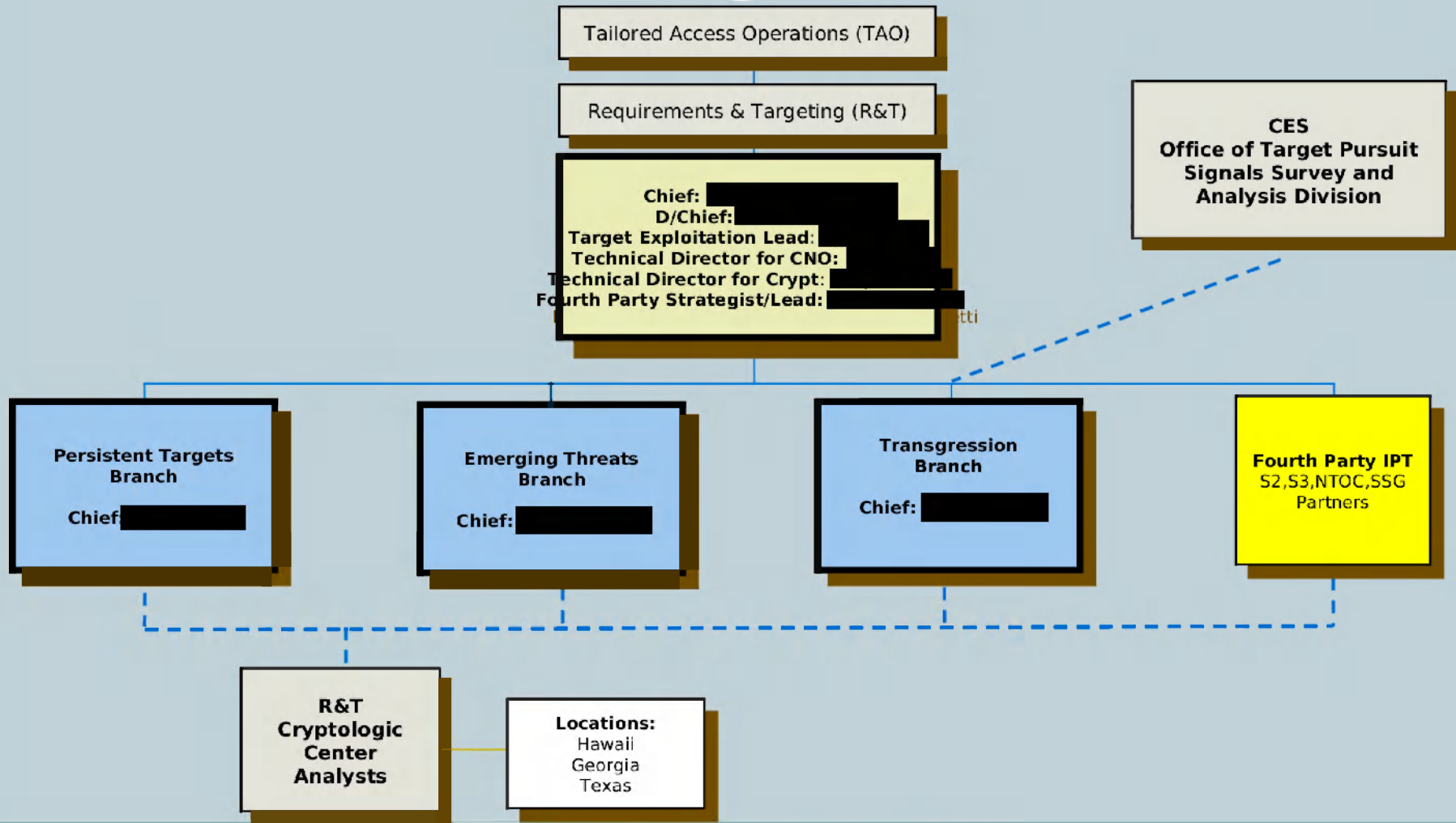
[REDACTED] (s3275
)

[REDACTED]

go 4thparty

I drink your milkshake

(U//FOUO) UNCLASSIFIED//FOR OFFICIAL USE ONLY
Cyber Counterintelligence
Division

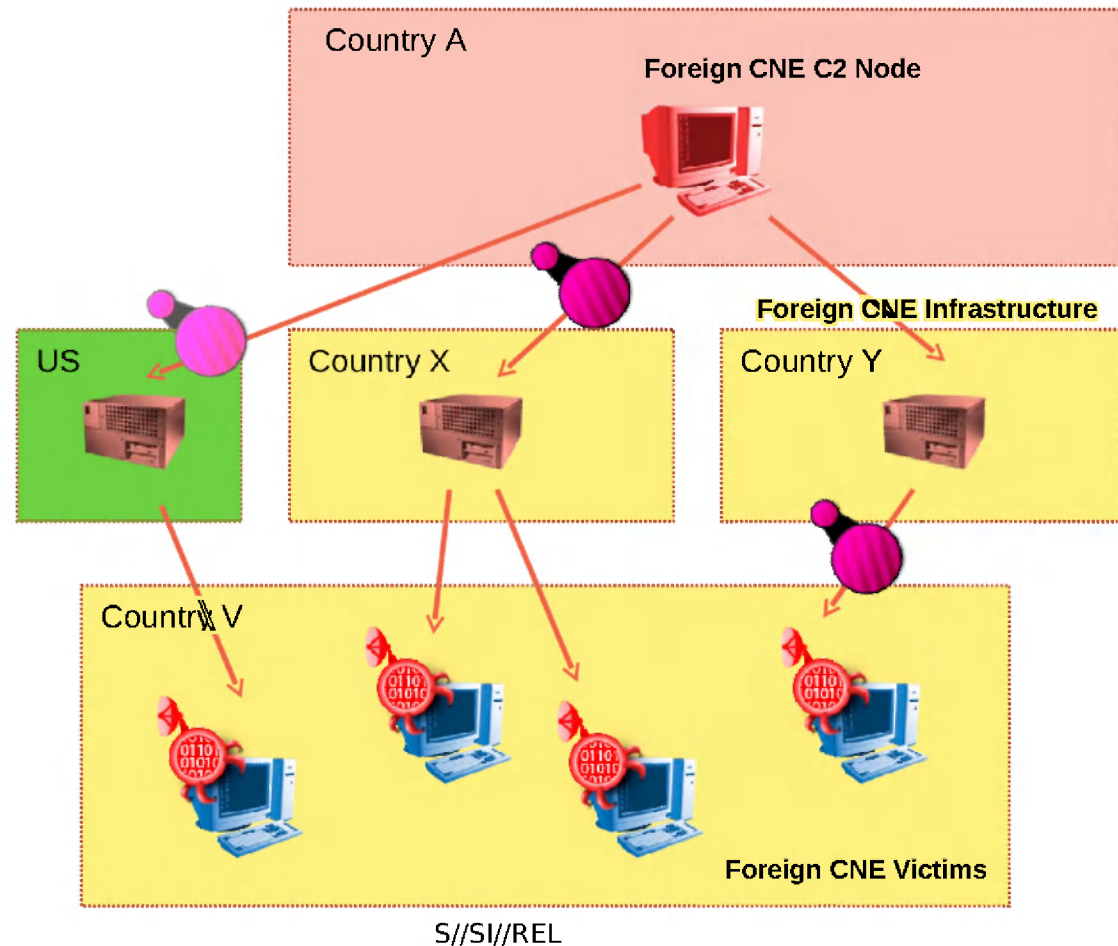


(U) What is 4th Party



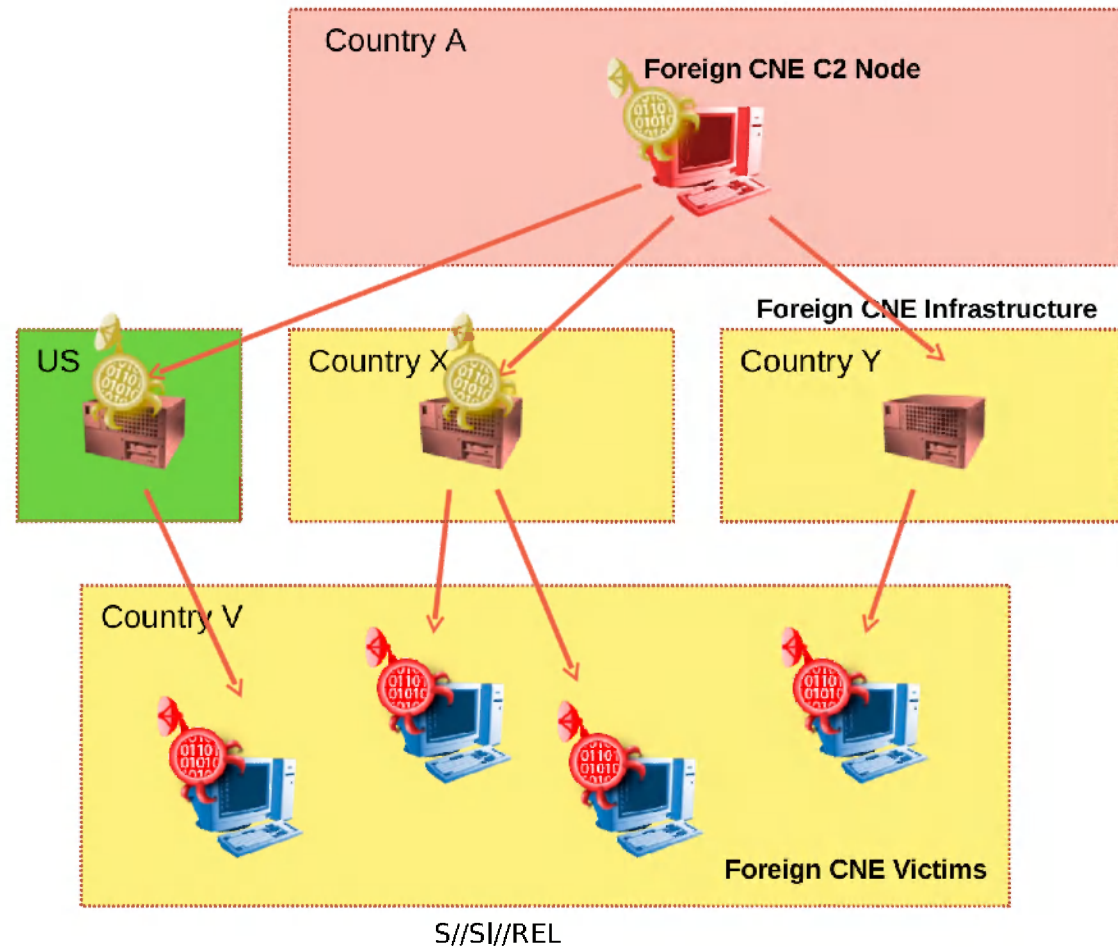
- (S//SI//REL) 4th party collection leverages CCNE accesses to provide Foreign Intelligence from foreign CNE victims
- (U) Types of 4th Party opportunities
 - (U) Passive Acquisition
 - (U) Active Acquisition
 - (U) Victim Stealing / Sharing
 - (U) Re-purposing

(S//SI//REL) *Passive acquisition* utilizes mid-point collection to target information being ex-filtrated from victims of foreign CNE activities. This often involves CES efforts to decrypt or de-obfuscate the collected data.



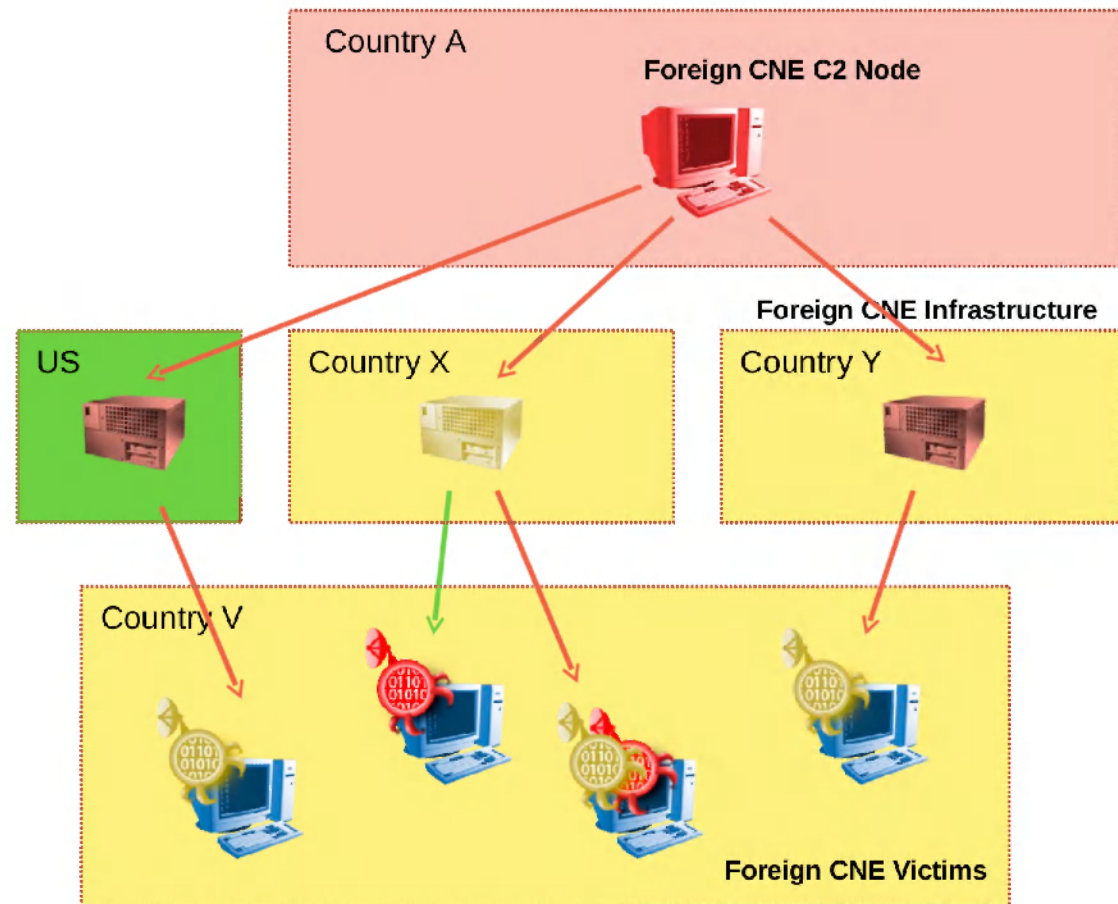
(U) Passive Acquisition

(S//SI//REL) Active acquisition utilizes end-point collection to target foreign CNE infrastructure in order to collect victim information.



(U) Active Acquisition

(S//SI//REL) *Victim stealing* exploits weaknesses in foreign CNE implants and C2 systems to gain access to victims and either take control of the foreign implant or replace it with our own. This is NOT a disruption or CNA activity. It is solely used to further CNE accesses.

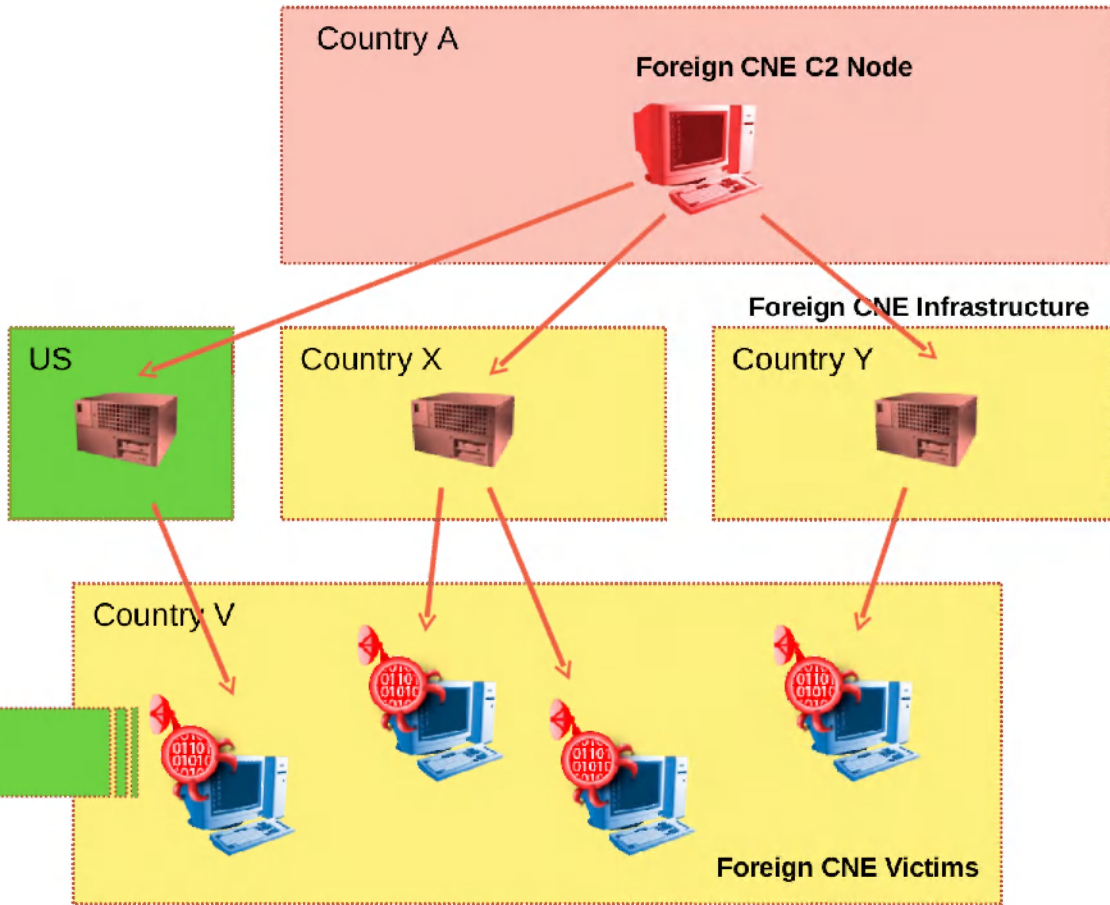


S//SI//REL

(U) Victim Stealing / Sharing



(S//SI//REL) *Re-purposing* utilizes captured foreign CNE components (implants, exploits, etc) to shorten the development cycle of our own CNE tools.



S//SI//REL

(U) Re-purposing



(U) 4th Party Decision Tree

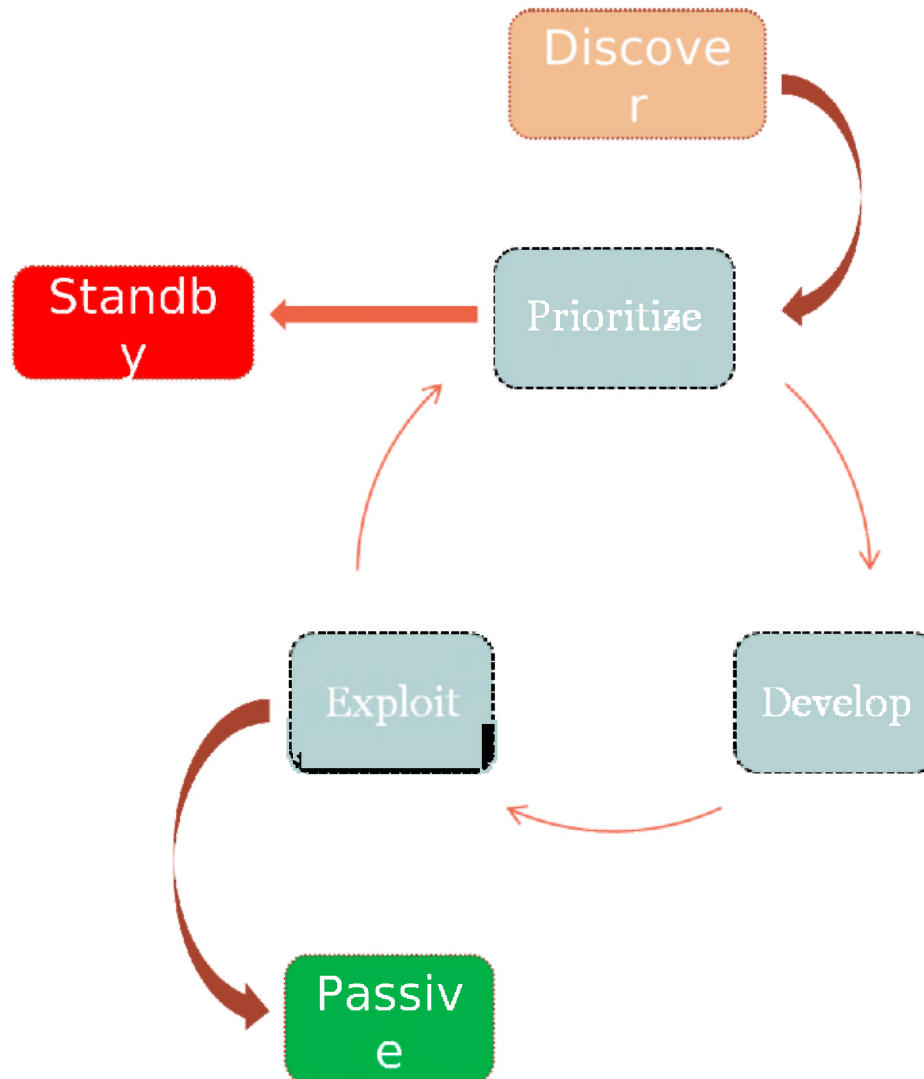
(S//REL) The best sustained outcome is *passive acquisition* of valuable 4th party collected information. Where the 4th party is not collecting information of interest, but the victim is still of interest *victim stealing* can be pursued. Where passive or cryptographic issues prevent (or delay) passive acquisition, *active acquisition* will be pursued.



S//SI//REL

(U) 4th Party Lifecycle

(S//REL) The prioritization, development and exploitation cycle is continuous until the priority is lowered to standby or the intelligence value is being realized through passive alone.



Fourth Party Example

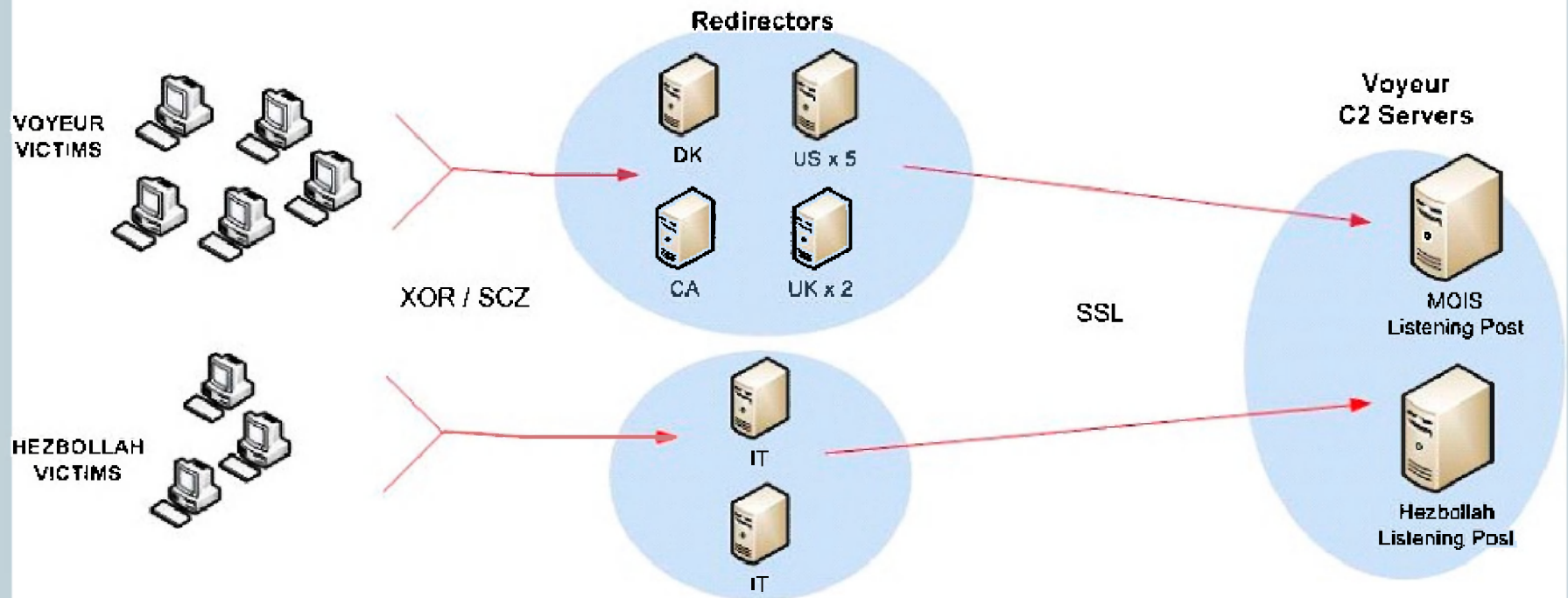


VOYEUR

(U) VOYEUR Network Map



Iranian MOIS Implant



(U) VOYEUR SQL Interface



Showing rows 0 - 29 (5,016 total. Query took 0.0154 sec)

Profiling [Edit] [Explain SQL] [Create PHP Code] [Refresh]

Show: 30 row(s) starting from record # 30

Sort by key: None

	Id	User	FromEmail	FromName	ToEmail	TcName	AttackSerial	AttackID	GroupName	Message	EffectivePlugins
<input type="checkbox"/>	1	admin					4d49777646757769536a	44277	mehrab-link-881217	Please use UTF-8 Character Encoding to view this e...	linkPlugin
<input type="checkbox"/>	2	admin					69775941306d78423944	44278	mehrab-link-881117	Please use UTF-8 Character Encoding to view this e...	linkPlugin
<input type="checkbox"/>	3	admin					45a58694b7063637032	44279	mehrab-link-881217	Please use UTF-8 Character Encoding to view this e...	linkPlugin
<input checked="" type="checkbox"/>	4	admin					7138706d4a4d4b4c764a	44280	mehrab-link-881217	Please use UTF-8 Character Encoding to view this e...	linkPlugin
<input type="checkbox"/>	5	admin					5231575f67315a713331	44281	mehrab-link-881217	Please use UTF-8 Character Encoding to view this e...	linkPlugin
<input type="checkbox"/>	6	admin					3356505a55726c615953	44282	mehrab-link-881217	Please use UTF-8 Character Encoding to view this e...	linkPlugin
<input type="checkbox"/>	7	admin					597575765f4931574132	44283	mehrab-link-881217	Please use UTF-8 Character Encoding to view this e...	linkPlugin
<input type="checkbox"/>	8	admin					6c685667305445552d71	44284	mehrab-link-881217	Please use UTF-8 Character Encoding to view this e...	linkPlugin
<input checked="" type="checkbox"/>	9	admin					65693578797445463345	44285	mehrab-link-881217	Please use UTF-8 Character Encoding to view this e...	linkPlugin
<input type="checkbox"/>	10	admin					75713441726364496b71	44286	mehrab-link-881217	Please use UTF-8 Character Encoding to view this e...	linkPlugin
<input type="checkbox"/>	11	admin					4a5a44737574525f34e2	44287		hi	
<input type="checkbox"/>	12	admin					3031456a384f52546259	44288	mehrab-link-881217	Please use UTF-8 Character Encoding to view this e...	linkPlugin
<input checked="" type="checkbox"/>	13	admin					776d5a49586848576333	44289	mehrab-link-881217	Please use UTF-8 Character Encoding to view this e...	linkPlugin
<input type="checkbox"/>	14	admin					3468624a48726e756b4f	44290		hi	
<input type="checkbox"/>	15	admin					7848536366f53345254	44291		hi -br /> 	linkPlugin socksPlugin

Find: la2ou Previous Next Highlight all Match case

(U) TUNINGFORK



https://onedata...ata/repository/ DIRTSHED - SEEKER CLOUD / AER - WikiInfo

TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL

Index of /Processed/DIRTSHED/[REDACTED]/2011-05-04/081700/opt/me2site/data/repository

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
Parent Directory	-	-	-
1684/	06-May-2011 02:02	-	-
1869/	06-May-2011 02:01	-	-
2421/	06-May-2011 02:11	-	-
2644/	06-May-2011 01:54	-	-
3027/	06-May-2011 01:25	-	-
3427/	06-May-2011 00:47	-	-
3505/	06-May-2011 00:44	-	-
3537/	06-May-2011 01:24	-	-
3551/	06-May-2011 02:00	-	-
3684/	06-May-2011 00:45	-	-
3803/	06-May-2011 02:14	-	-
3949/	06-May-2011 01:54	-	-
4493/	06-May-2011 01:57	-	-
4617/	06-May-2011 01:26	-	-
4683/	06-May-2011 02:11	-	-
4865/	06-May-2011 01:55	-	-
5254/	06-May-2011 01:29	-	-
5352/	06-May-2011 02:11	-	-
5364/	06-May-2011 02:13	-	-
5390/	06-May-2011 02:16	-	-
5426/	06-May-2011 01:26	-	-
5436/	06-May-2011 01:56	-	-

TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL

(U) SEEKER



DYNAMIC PAGE - HIGHEST POSSIBLE CLASSIFICATION IS TOP SECRET//SI//REL TO USA, AUS, CAN, GBR, NZL

home favorites targets preferences help SEE:ER turning exploration into knowledge 0.8.6 beta

DIRTSHED

UNIX | opt | me2site | data | packed | default | 2011.01.10-16.22.51-clients-archive.7z.001

Time	Attr	Size	Compressed	Name
03:57:06A	140	1276719708	FileMan/2011_01_08_08_56_36_2
03:57:02A	178		01_08_08_57_02_62.220.113.118
03:57:37A	140		FileMan/2011_01_08_08_57_07_2
03:57:08A	178		_01_08_08_57_08_85.183.189.11
03:57:33A	178		_01_08_08_57_33_217.218.133.6
03:58:08A	140		FileMan/2011_01_08_08_57_39_2
03:57:56A	178		Report/2011_01_08_08_57_56_21
03:58:40A	140		FileMan/2011_01_08_08_58_10_2
03:58:12A	178		_01_08_08_58_11_94.183.226.20
03:58:23A	7775		rt/2011_01_10_08_58_22_92.242.2
03:58:26A	18248		_01_08_08_58_25_92.242.222.2
03:58:28A	178		rt/2011_01_08_08_58_28_89.165
03:58:31A	664679		_01_08_08_58_31_95.92.105.23
03:58:11A	140		FileMan/2011_01_08_08_58_41_2
03:58:41A	76619		01_08_08_58_41_217.218.133.68
03:58:44A	23720		01_08_08_58_44_217.218.133.68
03:58:55A	178		rt/2011_01_08_08_58_55_119.2
03:59:42A	140		FileMan/2011_01_08_08_59_12_2
03:59:12A	178		03_59_12_91.99.185.141_98.bin
03:59:25A	2271		011_01_08_08_59_25_92.242.222
03:59:28A	178		2011_01_08_08_59_27_92.242.22
03:00:13A	140		FileMan/2011_01_08_08_59_43_2
03:59:45A	178		11_01_01_08_59_45_89.144.174
03:00:02A	178		01_08_09_00_02_62.220.113.118
03:00:12A	178		_01_08_09_00_12_85.183.189.11
03:00:44A	140		FileMan/2011_01_08_09_00_14_2
03:00:35A	178		_01_08_09_00_35_217.218.133.6
03:00:40A	178		2011_01_08_09_00_40_92.242.22
03:00:44A	11712		/2011_01_08_09_00_42_92.242.2
03:01:16A	140		FileMan/2011_01_08_09_00_45_2
03:00:57A	178		Report/2011_01_08_09_00_57_21
03:00:59A	178		_01_08_09_00_58_77.36.153.21
03:00:58A	180		_01_08_09_00_58_77.36.153.21
03:01:47A	140		FileMan/2011_01_08_09_01_17_2
03:01:29A	178		rt/2011_01_08_09_01_23_89.165
03:02:10A	140		FileMan/2011_01_08_09_01_48_2
03:01:57A	178		rt/2011_01_08_09_01_52_119.2

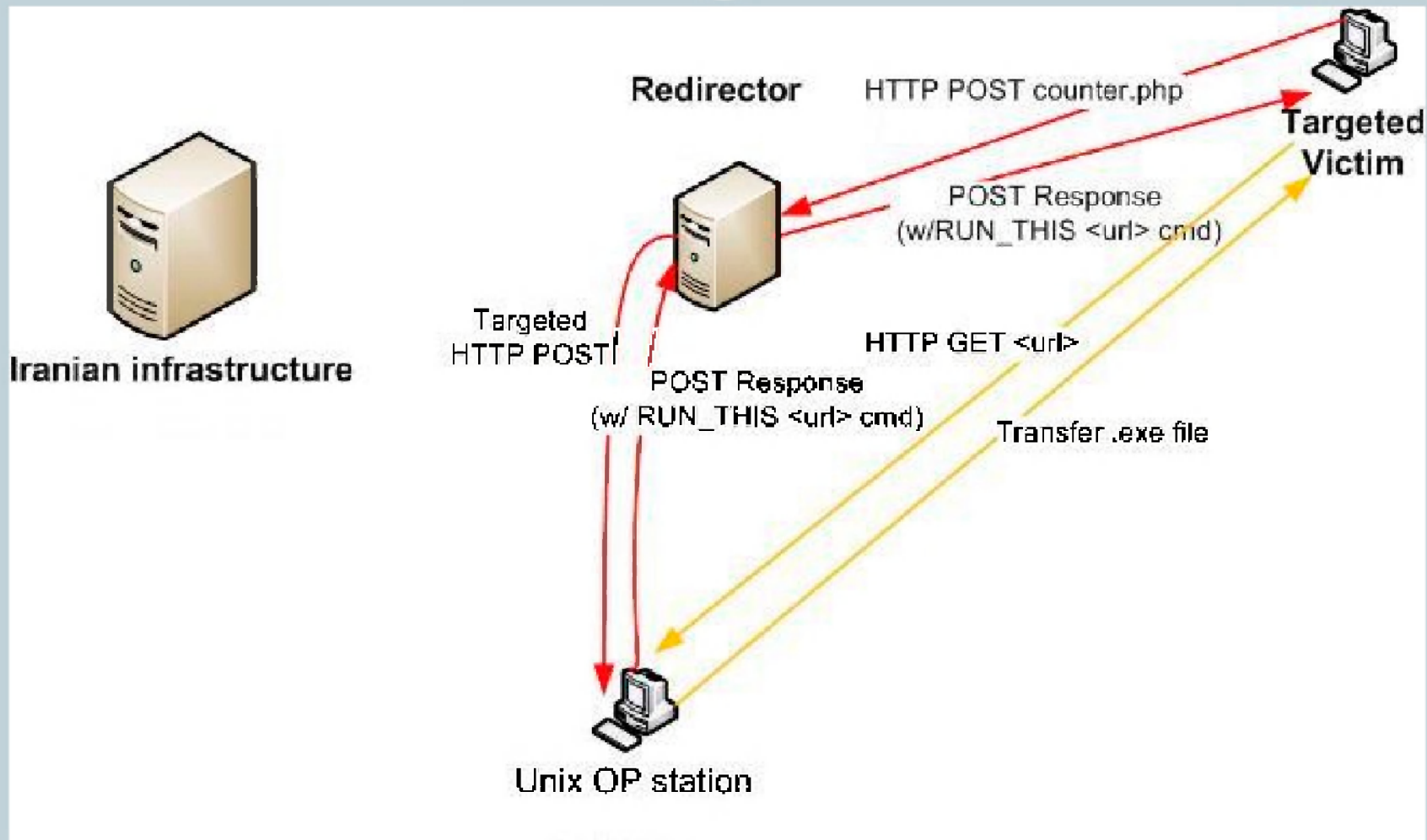
Information Owner: T1212.717-3500 Page Publisher: SEEKER Team: T1212.717-3500 DERIVED FROM: NSA/CSS I4-52 / DATED: 08 January 2007 / DECLASSIFY ON: 20320103
DYNAMIC PAGE - HIGHEST POSSIBLE CLASSIFICATION IS TOP SECRET//SI//REL TO USA, AUS, CAN, GBR, NZL

(U) Cloud/ABR

(TS//SI//REL TO USA, FVEY) Project DIRTSBED 

File Type	Hash	Language	Cone	Classified	Hitlist	Overlaps		
SHOCKWAVE	0	0	0	0	2	2	8	
SOURCECODE_C_CPP	0	0	0	28	40	40	74	
SOURCECODE_JAVA	0	0	0	0	2	2	80	
SOURCECODE_JAVASCRIPT	0	0	0	1	25	27	31	
SOURCECODE_PHP	0	0	0	127	521	537	1284	
SOURCECODE_PYTHON	0	0	0	138	546	546	546	
SOURCECODE_RUBY	0	0	0	19	70	70	71	
SQLITE_DATABASE	0	0	6	6	6	15	40	
TAR	0	0	0	13	13	13	17	
TAR-UNWRAPPED	0	0	0	209	209	209	364	
TEXT	0	0	1	278	833	859	4528	
THUMBS_DB	0	0	0	0	4	6	11	
TIFF	0	0	3	3	3	3	143	
TRUETYPE	0	0	0	0	0	0	98	
UNIX-BASH-SCRIPT	0	0	0	21	90	90	133	
UNIX-PERL-SCRIPT	0	0	0	1	4	4	43	
UNIX-SH-SCRIPT	0	0	0	177	490	490	513	
UNIX_PASSWORD_FILE	0	0	0	11	23	38	260	
UNKNOWN	0	0	0	0	0	0	1	
UNKNOWN-ENORMOUS	0	0	0	35	41	44	56	
UNKNOWN-HUGE	0	0	1	58	72	90	157	

(TS//SI//REL) Example: Victim Stealing



(U//FOUO) Repurposing



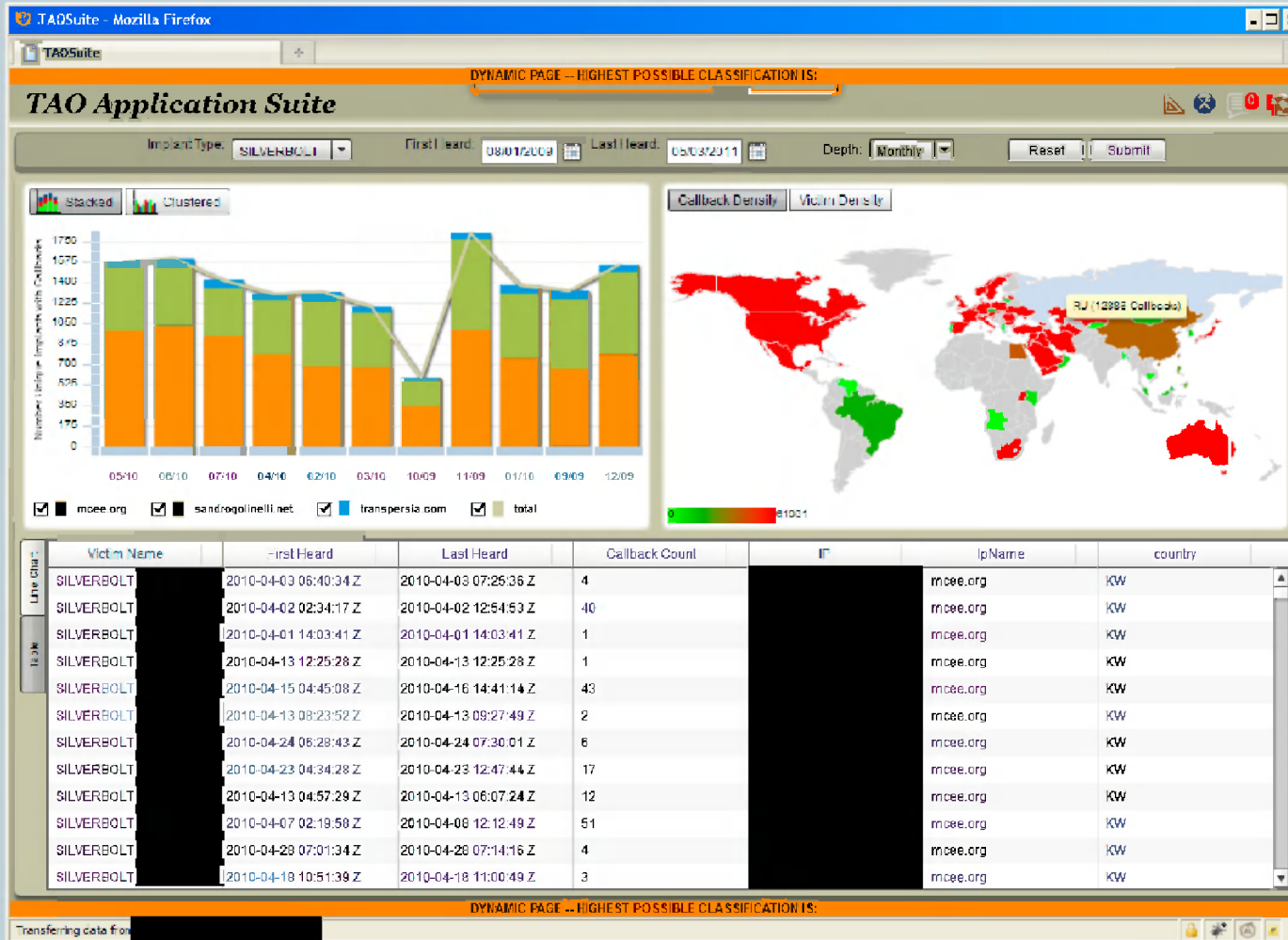
The screenshot displays the Immunity Debugger interface with the following components:

- Program Tree:** Shows the loaded module `SDSND32.DLL` and its sections: `.text`, `.pdata`, `.rsrc`, and `.reloc`.
- Symbol Tree:** Shows the loaded module `SDSND32.DLL` and its namespaces.
- Data Type Manager:** Shows the loaded module `SDSND32.DLL` and its data types.
- Listing:** Shows the assembly code for the function `FUN_100012c0`. The code starts with `__stdcall FUN_100012c0()` and includes instructions such as `SUB ESP, 0x400`, `PUSH EBX`, `PUSH EBP`, `PUSH ESI`, `MOV EBP, [USER32.DLL: GetKe...`, `PUSH EDI`, `MOV ECX, 0xffff`, `XOR EAX, EAX`, `LEA EDI, [ESP + local_3fc]`, `MOV dword ptr [ESP + local_...`, `STOSD, REP ES:EDI`, `MOV ECX, 0x96`, `MOV EDI, DAT_1000a818`, `STOSD, REP ES:EDI`, `LAD_100012f1`, `PUSH 0x8`, `CALL [KERNEL32.DLL: Sleep]`, `CALL FUN_100011d0`, and `MOV EBX, 7f7f`.
- Function Graph:** Shows the control flow graph for `FUN_100012c0`. The graph consists of several basic blocks connected by control flow edges. The blocks are:
 - `100012c0 - FUN_100012c0`: Contains the main function body.
 - `100012f1 - LAB_100012f1`: Contains instructions `CALL [KERNEL32.DLL: Sleep]` and `CALL FUN_100011d0`.
 - `100012f2 - LAB_100012f2`: Contains instructions `CALL [USER32.DLL: GetKe...` and `LAB_10001280`.
 - `10001280 - LAB_10001280`: Contains instructions `MOV EAX, [ESP + local_3fc]` and `MOV EAX, 7f7f`.

(U) Current Efforts



(U) VicDB



(S//SI) Survey Data



```
SYSTEM2\NETWORK SERVICE      SYSTEM2 NETWORK SERVICE      S-1-5-20
SYSTEM2\BUILTIN               SYSTEM2 BUILTIN               S-1-5-32
```

```
-----UserAccount-----
AccountType  Caption                Domain  FullName
512          SYSTEM2\Administrator SYSTEM2  SYSTEM2
512          SYSTEM2\ASPNET         SYSTEM2  ASP.NET Machine Account
512          SYSTEM2\Guest          SYSTEM2  SYSTEM2
512          SYSTEM2\HelpAssistant  SYSTEM2  Remote Desktop Help Assistant Account
512          SYSTEM2\SUPPORT_388945a0 SYSTEM2  CN=Microsoft Corporation,L=Redmond,S=Washington
```

```
-----TimeZone-----
Bias  Caption  SettingID
210   (GMT+03:30) [REDACTED]
```

```
-----dir "C:\Documents and Settings\Administrator\desktop"-----
Volume in drive C has no label.
Volume Serial Number is C437-1E2D
```

```
Directory of C:\Documents and Settings\Administrator\desktop

05/12/2011  05:31 PM  <DIR>          .
05/12/2011  05:31 PM  <DIR>          ..
05/08/2011  08:08 PM          134,915  1256694986[1].jpg
05/08/2011  08:15 PM          155,166  croppedbusiness_success_-_graph_mp_jpg_nls2[1].jpg
04/08/2011  09:48 PM           606  GetPLV.lnk
05/03/2011  07:40 PM  <DIR>          Hardware
05/03/2011  08:03 PM          2,473  Microsoft Office Excel 2007.lnk
05/09/2011  06:40 PM          2,497  Microsoft Office Word 2003.lnk
05/11/2011  11:24 AM          2,515  Microsoft Office Word 2007.lnk
04/22/2011  01:15 PM          1,515  Paint.lnk
          7 File(s)      259,687 bytes
          3 Dir(s)  51,504,803,840 bytes free
```

```
-----dir "C:\Documents and Settings\Administrator\My Documents"-----
Volume in drive C has no label.
Volume Serial Number is C437-1E2D
```

```
Connection-specific DNS Suffix . : MyDslDomain
Description . . . . . : Broadcom NetXtreme Gigabit Ethernet
Physical Address. . . . . : 00-0E-7F-62-5C-49
Dhcp Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
IP Address. . . . . : [REDACTED]
Subnet Mask . . . . . : [REDACTED]
Default Gateway . . . . . : [REDACTED]
DHCP Server . . . . . : [REDACTED]
DNS Servers . . . . . : [REDACTED]
Lease Obtained. . . . . : Thursday, May 19, 2011 11:39:16 AM
Lease Expires . . . . . : Saturday, May 21, 2011 11:39:16 AM
These Windows services are started:
```

- Automatic Updates
- Background Intelligent Transfer Service
- Client Service for NetWare
- COM+ Event System
- Computer Browser
- Cryptographic Services
- DCOM Server Process Launcher
- DHCP Client
- Distributed Link Tracking Client
- DNS Client
- Event Reporting Service

(U) DEADSEA



his system is audited for USSIF, F1 and Luman Rights Act compliance
TOP SECRET//COMINT//REL TO USA, AUS, GAN, SBR, and NZL//20820108

XKEYSCORE Welcome [redacted] [Warning: your password has expired!](#) [Log Out](#)

Home Search Workflow Central Results Fingerprints Statistics Map My Account XK Forum Help

Navigation Filter [x] [1] [2]

- Cone Byzantine Raptor Rolex
- Cone Byzantine Raptor Trojan3
- Cone Plaidiana Command Packet
- Cone Traffic
- Cone Victim Id
- Cone Zebedee Parse
- Cdma A11 Metadata
- Computer Serial Numbers
- DNS High Entropy
- DataFlurryPhoneInfoExtractor
- Diameter AVP Metadata
- Diameter Header Metadata
- Dynamic DNS Updates
- E Ticket
- ESP SPI
- Eclectiprot
- Electronic Attack Heuristics
- Email
- Encryption Sleg Camo
- Encryption Sleg JSTEG
- Exif Metadata
- Expression Engine
- FACEBOOK
- Facebook Chat Jabber
- Fourth Party CNE_DEADSEA_**
- Generic IDirect
- Google Analytics
- Google Street View
- Google Street View Thumb
- Google Street View Tile
- Gtp Pdp Context
- HAWALA
- Happyfoot
- IE Cookies
- ...

Help

Show/Hide Fields* Advanced Features Show Hidden Search Fields Clear Search Values Reload Last Search Values **There are hidden Fields.**

Search: Fourth Party CNE_DEADSEA_

Query Name:

Justification: [Recent Justifications](#)

Additional Justification:

Miranda Number:

Current Time: 2011-05-13 13:33:16 GMT

Datetime: Start: Stop:

equity	<input type="text"/>
attribute_name	<input type="text"/>
attribute_value	<input type="text"/>
function_id	<input type="text"/>
computer_id	<input type="text"/>
direction	<input type="text"/>
implant_corwand	<input type="text"/>
install_id	<input type="text"/>

(S//SI) Discovery for 4th Party



DYNAMIC PAGE - HIGHEST POSSIBLE CLASSIFICATION IS TOP SECRET//COMINT//REL TO USA, FVEY

CROSSBONES2
LOGGED IN AS ██████████ PROFILE
SEARCH

Home
Entries
Reports
Activity Groups
User Groups
Tasking
Tags
Profile

NAVIGATION

- Home
- Entries
- New Journal Entry
- List Snippets
- New Snippet
- List Persons
- New Individual
- New Organization
- List Events
- Reports
- Activity Groups
- User Groups
- Tasking
- Tags
- Profile

CROSSBONES JOURNAL ENTRIES

(U//FOUO) This entry may contain information not fully assessed and is intended for analytic collaboration only. The recipient may not use, report or further disseminate this information unless or until it is published in a report.

DATA ELEMENTS

to add/cobos

██████████

email addresses

(TS//SI//REL) Perfect Keylogger Activity 🔔 👤 ⭐

XBJE/1/16896/05/2011 TOP SECRET//COMINT//REL TO USA, FVEY May 06, 2011

Warning: There are no diamond model events defined on this journal entry.

Content
Enrichments
Events
History

<p>author ██████████</p> <p>project / user group (CYBEROUPERT - MHR)</p> <p>intrusion sets UNKNOWN</p> <p>access PUBLIC</p> <p>details</p> <p>(TS//SI//REL) Perfect Keylogger is installed on hostname DOM (Russian for "home"), private IP address ██████████ for user "Home". Websites surfing information and screenshots have been stored at an account at Russian IP ██████████ inbox.ru mail server, and are being delivered to a U.S. IP. A courtesy copy of the logs is delivered to user ██████████. ██████████ is a Moscow-based software services company, member of a leading Russian technology group. ██████████ is probably ██████████.</p> <p>Apparently, the victim(s) of the keylogging are members of the ██████████ including ██████████. ██████████ possibly wife to the ██████████ referenced above, as well as ██████████.</p> <p>Keylogger is probably installed to monitor children's and wife's activity</p> <p>██████████ is well-connected. Her email is ██████████. She has a presence on LinkedIn. And her Facebook password was sniffed as ██████████. Several other passwords for both ██████████ and ██████████ have been captured. Possibly ██████████ is ██████████ Head of PR and Advertising at ██████████ Moscow.</p> <p>Her contacts include:</p> <p>██████████ Director for Corporate Development at ██████████</p> <p>██████████ probably husband.</p>	<p>source SIGINT:FORNSAT</p> <p>source site / source signal USJ-759 /</p> <p>source classification TOP SECRET//COMINT//REL TO USA, FVEY</p> <p>source date 2011-05-06 00:00:00 UTC</p> <p>source description</p>
--	--

Actions

- New Journal Entry
- Attach File
- New Association
- New Signature
- Like This
- Follow This Entry
- Rescan for Data Facets
- Export Events
- Add a Link

ASSIGNED TAGS

- direction
- intent
- result
- methodology
- phase
- actor
- victim
- capability
- infrastructure
- geopolitical environment
- technology
- other: positive correlations
- other: negative correlations

KEYWORDS

keywored

UPLOAD / ATTACH FILE

Contact us



EMAIL: DL 4THPARTY

NSANET: GO 4THPARTY

JABBER: S2 CYBER ANALYSIS