

TOP SECRET//COMINT//REL TO USA, FVEY



XKEYSCORE for Counter-CNE

"Using the XKS CNE dataset and a DISGRUNTLEDDUCK fingerprint, we now see at least 21 TAO boxes with evidence of this intrusion set, most of which are associated with projects aimed at Iran WMD targets." -- MHS, July 2010

March, 2011

xks-cne@r1.r.nsa

TOP SECRET//COMINT//REL TO USA, FVEY

UNCLASSIFIED//FOUO

Overall Classification



The overall classification of this presentation is:

TOP SECRET//COMINT//REL TO USA, FVEY

UNCLASSIFIED//FOUO

What is XKEYSCORE?



- A suite of software running on a Linux host
- *Classically*, used for DNI processing, selection and survey
- A distributed hierarchy of servers at field sites and headquarters
 - Extract and tag metadata & content from traffic
 - Servicing analyst queries and workflows
- Web and programmatic front-ends

What is XKEYSCORE?



- A suite of software running on a Linux host
- *Classically*, used for DNI processing, selection and survey
- A distributed hierarchy of servers at field sites and headquarters
 - Extract and tag metadata & content from traffic
 - Servicing analyst queries and workflows
- Web and programmatic front-ends

TOP SECRET//COMINT//REL TO USA, FVEY

XKEYSCORE GUI



The screenshot shows the XKEYSCORE web interface in a Mozilla Firefox browser window. The browser's address bar displays the URL: <https://xks-central.corp.usa.ic.gov:8443/XKEYSCORE/search/standardsearchformsearch/Home.ec>. The page title is "XKEYSCORE - For Analysis...".

The main content area displays a search result for IP address 2304, with a count of 144. Below this, a table lists search results with the following columns: **IP**, **Country**, **City**, **Lat**, **Lon**, **Country (II)**, **City (IP)**, and **To Loc**. The table contains 14 rows of data, all showing IP address 2304 and Country FR (France).

IP	Country	City	Lat	Lon	Country (II)	City (IP)	To Loc
2304	FR	NEUILLYSUF	48.88	2.27	FR	NEUILLYSUF	00
2304	FR	NEUILLYSUF	48.88	2.27	FR	NEUILLYSUF	00
2304	FR	NEUILLYSUF	48.88	2.27	FR	NEUILLYSUF	00
2304	FR	NEUILLYSUF	48.88	2.27	FR	NEUILLYSUF	00
2304	FR	NEUILLYSUF	48.88	2.27	FR	NEUILLYSUF	00
2304	FR	NEUILLYSUF	48.88	2.27	FR	NEUILLYSUF	00
2304	FR	NEUILLYSUF	48.88	2.27	FR	NEUILLYSUF	00
2304	FR	NEUILLYSUF	48.88	2.27	FR	NEUILLYSUF	00
2304	FR	NEUILLYSUF	48.88	2.27	FR	NEUILLYSUF	00
2304	FR	NEUILLYSUF	48.88	2.27	FR	NEUILLYSUF	00
2304	FR	NEUILLYSUF	48.88	2.27	FR	NEUILLYSUF	00
2304	FR	NEUILLYSUF	48.88	2.27	FR	NEUILLYSUF	00
2304	FR	NEUILLYSUF	48.88	2.27	FR	NEUILLYSUF	00
2304	FR	NEUILLYSUF	48.88	2.27	FR	NEUILLYSUF	00
2304	FR	NEUILLYSUF	48.88	2.27	FR	NEUILLYSUF	00

The page footer includes the text "TOP SECRET//COMINT//REL TO USA, FVEY" and "saved: 802397578693333".

TOP SECRET//COMINT//REL TO USA, FVEY

Example Search



- Let's try a search for suspicious stuff...
http_activity search, 5-eyes defeat, look for fingerprints:
`ndist/discovery/heuristic/BHAM/get_with_content OR http/get/with_content`
- While the search runs, some gotchas:
 - You choose where your query is run
 - Content and metadata age-off
 - Burden is on user/auditor to comply with USSID-18 or other rules
 - Geolocation based on IP

Search Results



2011-12-11 18:47:44 3-41146/00000 192 Private Address 10 Private Address 43070 12468 TCP 774

Date/Time	Case Notation	From IP	To IP	From Port	To Port	Process	Length
2011-12-11 18:47:44	3-41146/00000	192 Private Address	10 Private Address	43070	12468	TCP	774

GET /CAVIT HTTP/1.0
User-Agent: 62531C333F62DA7333FD2C02709E7DD2
Accept: */*
Host: 10 Private Address:12468
Content-Type: application/x-www-form-urlencoded
Connection: Keep-Alive
Reset from local:(1231) seq = 2661134980

Notes:

- Strange User-Agent
- Probably NOT CNE but definitely something non-standard
- Content: maybe a HTTP tunnel for some weird protocol?
Reset from local...
- Should we write a Fingerprint?

Fingerprints and Appids



- Useful for identifying classes of traffic or particular targets (for SIGDEV or collection):
 - `mail/webmail/yahoo`
 - `browser/cellphone/blackberry`
 - `topic/s2B/chinese_missile`
- appid – a contest, highest scoring appid wins
- fingerprint – many fingerprints per session
- microplugin – a fingerprint or appid that is relatively complex (e.g. extracts and databases metadata)

Fingerprints and Appids (more)



- Written in language called "GENESIS" (go genesis-language):

```
appid('encyclopedia/wikipedia', 2.0) =  
  http_host('wikipedia' or 'wikimedia');  
fingerprint('dns/malware/MalwareDomains') =  
  dns_host('erofreex.info' or 'datayakoz.info'  
  or 'erogirlx.info' or 'pornero.info' or ...)
```

- If a fingerprint contains a schema definition, a search form automatically appears in the XKEYSCORE GUI
- Power users can drop in to C++ to express themselves

More about searches



- Many different searches
 - Base search is Full Log DNI
 - Depending on traffic type, will generate searchable results for (example):

HTTP Activity	Network Information	GEO Info
Extracted Files	Email Addresses	Registry
Logins and Passwords	Document Metadata	Machine Info

- workflow – a user query that is run automatically usually every 24 hours

XKEYSCORE Gotchas



- Not all sites run latest XKEYSCORE software or fingerprints
- fingerprint submission:
 - XKEYSCORE team weighs mission-worthiness of user fingerprints vs computational cost
- Content and metadata ageoff

XKEYSCORE CNE



- Lots of endpoint data flows into XKS
TAO (no ECIs), GCHQ (almost all)
- Other limited flows include SIGINT
Forensics Center, TAO STAT
- XKEYSCORE works well for endpoint data
- Sometimes the paradigm breaks (e.g.
collected browser history file)

XKEYSCORE CNE (more)



- **Payload types:**
dirwalk, extracted file, system survey, network config, captured credentials, registry query, key logger, etc.
- **Labeled `dnt_payload` in appid/fingerprint ontology**
- **Let's look at some DANDERSPRITZ data...**

TOP SECRET//COMINT//REL TO USA, FVEY

XKEYSCORE CNE (more)



XK Session Viewer - Mozilla Firefox

File Edit View History Bookmarks Tools Help

https://xks.central.com.usia.gov:8423/XKEYSCORE/lay_outs/popOut.Layout.jsp?pageTitle=Session%20Viewer&showURL=%2FXKEYSCORE%2F%2FmainViewer

This system is audited for US SID 18 and Human Rights Act compliance
CLASSIFICATION: TOP SECRET//COMINT//REL TO USA, AUS, CAN, GDR, NZL

XKEYSCORE C2C Session Viewer

Session [56] of 783

Date/Time	Case Number	From IP	To IP	From Port	To Port	Protocol	Length
2011-04-12 02:06:12	CC.WHU.JCGA/CCTD						10074

Session Header (3) | Meta (4)

Format: JINI_PAY_LOAD | Send to: | Download Search | Mode: | Scripts | Origins | Search Content: enter text to search | Clear

Quick Clicks

- Session
- One-Click Searches
 - Find incoming traffic
 - external:experimental/process
 - Find traffic on
 - external:pay load/processlist
 - Find application
 - external:experts/etd/case on

Done

PAYLOAD XML

```
<Process creationTime='2011-04-05T00:37:09.031Z50003' description='initia...' pid='463' ppid='352'>svchost.exe</Process>
<Process creationTime='2011-04-05T00:37:11.734Z50003' description='initia...' pid='655' ppid='110'>svchost.exe</Process>
<Process creationTime='2011-04-05T00:37:34.781Z50003' description='initia...' pid='728' ppid='440'>svchost.exe</Process>
<Process creationTime='2011-04-05T00:37:35.999Z50003' description='initia...' pid='797' ppid='440'>svchost.exe</Process>
<Process creationTime='2011-04-05T00:37:36.484Z50003' description='initia...' pid='844' ppid='440'>svchost.exe</Process>
<Process creationTime='2011-04-05T00:37:40.703Z50003' description='initia...' pid='863' ppid='440'>svchost.exe</Process>
<Process creationTime='2011-04-05T00:37:41.590Z50003' description='initia...' pid='895' ppid='440'>svchost.exe</Process>
<Process creationTime='2011-04-05T00:37:42.718Z50003' description='initia...' pid='964' ppid='110'>csrss.exe</Process>
<Process creationTime='2011-04-05T00:37:54.281Z50003' description='initia...' pid='1348' ppid='110'>svchost.exe</Process>
<Process creationTime='2011-04-05T00:37:54.640Z50003' description='initia...' pid='1348' ppid='440'>svchost.exe</Process>
<Process creationTime='2011-04-05T00:37:57.171Z50003' description='initia...' pid='1492' ppid='440'>svchost.exe</Process>
<Process creationTime='2011-04-05T00:37:57.710Z50003' description='initia...' pid='1530' ppid='440'>svchost.exe</Process>
<Process creationTime='2011-04-05T00:37:50.046Z50003' description='initia...' pid='1532' ppid='440'>svchost.exe</Process>
<Process creationTime='2011-04-05T00:38:00.750Z50003' description='initia...' pid='1530' ppid='440'>svchost.exe</Process>
<Process creationTime='2011-04-05T00:38:00.750Z50003' description='initia...' pid='1630' ppid='110'>svchost.exe</Process>
<Process creationTime='2011-04-05T00:38:01.734Z50003' description='initia...' pid='1620' ppid='440'>svchost.exe</Process>
<Process creationTime='2011-04-05T00:38:01.421Z50003' description='initia...' pid='1644' ppid='440'>svchost.exe</Process>
<Process creationTime='2011-04-05T00:38:02.125Z50003' description='initia...' pid='1672' ppid='440'>svchost.exe</Process>
<Process creationTime='2011-04-05T00:38:02.500Z50003' description='initia...' pid='1650' ppid='440'>svchost.exe</Process>
<Process creationTime='2011-04-05T00:38:02.025Z50003' description='initia...' pid='1720' ppid='440'>svchost.exe</Process>
<Process creationTime='2011-04-05T00:38:08.046Z50003' description='initia...' pid='1832' ppid='440'>svchost.exe</Process>
<Process creationTime='2011-04-05T00:38:10.817Z50003' description='initia...' pid='1942' ppid='110'>svchost.exe</Process>
<Process creationTime='2011-04-05T00:38:14.562Z50003' description='initia...' pid='2216' ppid='440'>svchost.exe</Process>
<Process creationTime='2011-04-05T00:38:14.671Z50003' description='initia...' pid='2240' ppid='1644'>svchost.exe</Process>
<Process creationTime='2011-04-05T00:38:17.025Z50003' description='initia...' pid='2390' ppid='2240'>svchost.exe</Process>
<Process creationTime='2011-04-05T00:38:23.031Z50003' description='initia...' pid='2620' ppid='655'>svchost.exe</Process>
<Process creationTime='2011-04-05T00:45:47.108Z40503' description='initia...' pid='1698' ppid='704'>explorer.exe</Process>
<Process creationTime='2011-04-05T00:45:48.072Z40503' description='initia...' pid='1736' ppid='244'>svchost.exe</Process>
<Process creationTime='2011-04-05T00:45:54.601Z385003' description='initia...' pid='2042' ppid='1688'>svchost.exe</Process>
<Process creationTime='2011-04-05T00:45:57.899Z38603' description='initia...' pid='2888' ppid='1688'>svchost.exe</Process>
<Process creationTime='2011-04-05T00:46:00.750Z86603' description='initia...' pid='2956' ppid='1688'>svchost.exe</Process>
<Process creationTime='2011-04-05T00:40:02.203Z31203' description='initia...' pid='755' ppid='1000'>svchost.exe</Process>
<Process creationTime='2011-04-05T00:40:06.075Z59703' description='initia...' pid='452' ppid='1000'>svchost.exe</Process>
<Process creationTime='2011-04-05T00:46:15.408Z22603' description='initia...' pid='3530' ppid='3395'>svchost.exe</Process>
<Process creationTime='2011-04-05T00:46:23.636Z89403' description='initia...' pid='428' ppid='1822'>svchost.exe</Process>
<Process creationTime='2011-04-05T00:56:53.99713903' description='initia...' pid='4050' ppid='392'>svchost.exe</Process>
<Process creationTime='2011-04-11T22:28:03.26030503' description='initia...' pid='2424' ppid='320'>svchost.exe</Process>
<Process creationTime='2011-04-11T22:28:03.416Z85503' description='initia...' pid='5198' ppid='320'>svchost.exe</Process>
<Process creationTime='2011-04-11T22:25:30.503350003' description='initia...' pid='5440' ppid='320'>svchost.exe</Process>
<Process creationTime='2011-04-11T22:25:39.660250003' description='initia...' pid='5430' ppid='320'>svchost.exe</Process>
<Process creationTime='2011-04-11T22:25:00.456215003' description='initia...' pid='363' ppid='320'>svchost.exe</Process>
<Process creationTime='2011-04-11T22:25:00.699170003' description='initia...' pid='1334' ppid='320'>svchost.exe</Process>
<Process creationTime='2011-04-11T22:24:36.068331503' description='initia...' pid='4656' ppid='320'>svchost.exe</Process>
<Process creationTime='2011-04-11T22:24:36.068331503' description='initia...' pid='2572' ppid='320'>svchost.exe</Process>
```

This system is audited for US SID 18 and Human Rights Act compliance
CLASSIFICATION: TOP SECRET//COMINT//REL TO USA, AUS, CAN, GDR, NZL

TOP SECRET//COMINT//REL TO USA, FVEY

XKEYSCORE CNE (more)



- Recent Developments
 - Upgrade of XKEYSCORE CNE
 - Keyloggers: keylogger/perfect/extension
 - PCAP Reingestion
- Router Redirection

Counter CNE Methodology



(refer to Counter CNE Resources slide...)

- Hypothesis/research-driven
 - “Could South Korean CNE be using similar selectors to FVEY CNE?”
 - “What keywords could be used to find keyloggers (“example: keylog OR keystroke”)
- Bogus or Unusual Traffic
 - HTTP GET with content (example in this presentation)
 - HTTP POST at odd hours (from Russia 0200-0359Z)
 - Funky user agents
- Known-Host or User driven (e.g. drop sites)
- **XKEYSCORE is GOOD at these kinds of things**

CNE-Specific



- Registry searches (e.g. SIMBAR)
- Fused Active/Passive search
 - common selectors
 - document hashes
- Known Processes (malicious executables or code)
 - ... Let's enhance the process list appid
- map-reduce within CNE cluster using GENESIS calls

XKEYSCORE Doesn't Do...



- ... at all (well, automatically, anyways)
 - Paired traffic heuristic-based approach
 - HTTP[S] imbalance (e.g. GET without response)
 - IP/DNS mismatch*
- ... on an automatic basis
 - Network or host characterization
 - Changes in IP/DNS mapping over time
 - Changes over time in malware comms

Counter CNE Resources



- *How to Discover Intrusions [using XKEYSCORE]* by [REDACTED] and [REDACTED] (paper)
 - MHS INDEX – Foreign CNE Discovery Page
https://wiki.itd.nsa/wiki/Foreign_CNE_Discovery
 - CSEC and GCHQ – DONUT (unknown protocols):
<https://tiso.sigint.cse/snipehunt/index.php/DONUT>
 - GCHQ Discovery Posted some Research of Detecting Man-on-the-Side Attacks:
<https://tiso.sigint.cse/snipehunt/index.php/MOTS>
- GCQH Disco Team posts POC's for different Intrusions and some Details:
<https://wiki.gchq/index.php/Discovery>
- The GCHQ DISCO team also posts Discovery Theories they run once a week:
https://wiki.gchq/index.php/Discovery_Afternoons
 - XKEYSCORE Fingerprints



Points of Contact

- MHS Index Team
[REDACTED]: [REDACTED]@nsa.ic.gov
- CES/TRANGRESSION
[REDACTED]: [REDACTED]@nsa.ic.gov
[REDACTED]: [REDACTED]@nsa.ic.gov
- NSA/Countering Foreign Intelligence
[REDACTED]: [REDACTED]@nsa.ic.gov
- NTOC ??
- XKEYSCORE
[REDACTED], [REDACTED]: xks-cne@r1.r.nsa