

Wikimedia Foundation v. NSA
No. 15-cv-0062-TSE (D. Md.)

Plaintiff's Exhibit 30



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

[REDACTED]
xks-cne@r1.r.nsa

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

XKEYSCORE GUI



XK Metaviewer: shared by f610065:Category Hits at 67D - Mozilla Firefox

https://xks-central.corp.nsa.ic.gov:8143/XKEYSCORE/search/standardsearchformysearch:Home.do

ESS1377: SIDToday for 1/24... | Ethernet - Wikipedia, the free... | My Signatures | XK Metaviewer: shared by r... | XKEYSCORE - For Analysts...

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

XKEYSCORE Welcome [redacted] Log Out

Home Admin Users Search Workflow Controls Results Fingerprints Statistics Map My Account XKI drum Help

Navigation Filter

- Search Wizard
- CNF
 - Email Addresses
 - Extracted Files
 - Full Log DNI
 - Keylogger
 - Machine Information
 - Network Information
 - Registry
- Classic
 - MultiSearch
 - Classic AM
 - Alert
 - BlackBerry
 - Call Logs
 - Category DNI
 - Cellular DNI
 - Cisco Passwords
 - Clamant
 - DNS
 - Document Metadata
 - Document Tagging
 - Email Addresses
 - Extracted Files
 - Full Log DNI
 - Gen Inf
 - HTTP Activity
 - KE Parser
 - Keylogger
 - Logins and Passwords

Histogram Grid

Page 1 of 1

Filter: Fri Port Count

<input type="checkbox"/>	2304	174
--------------------------	------	-----

shared by f610065:Category Hits

Hold Actions Reports View Map View FILTERS

From	Siged	Active User	Case Notation	From IP	To IP	From Port	To Port	From Country (IP)	From City (IP)	From Latitude (IP)	From Longitude (IP)	To Country (IP)	To City (IP)	To Latitude (IP)	To Longitude (IP)
IFTNCOI	US-967D		UA2AA00CB	57	57	2304	2521	FR	NEUILLYSUF	48.88	2.27	FR	NEUILLYSUF	48.88	2.27
IETTGOI	US-967D		UA2AA00CB	57	57	2304	1679	FR	NEUILLYSUF	48.88	2.27	FR	NEUILLYSUF	48.88	2.27
ILINCOI	US-067D		UA2AA00CB	57	57	2304	3190	FR	NEUILLYSUF	48.88	2.27	FR	NEUILLYSUF	48.88	2.27
IETTGOI	US-967D		UA2AA00CB	57	57	2304	1655	FR	NEUILLYSUF	48.88	2.27	FR	NEUILLYSUF	48.88	2.27
IETTGOI	US-067D		UA2AA00CB	57	57	2304	1120	FR	NEUILLYSUF	48.88	2.27	FR	NEUILLYSUF	48.88	2.27
IFTNCOI	US-967D		UA2AA00CB	57	57	2304	1130	FR	NEUILLYSUF	48.88	2.27	FR	NEUILLYSUF	48.88	2.27
IETTGOI	US-967D		UA2AA00CB	57	57	2304	1679	FR	NEUILLYSUF	48.88	2.27	FR	NEUILLYSUF	48.88	2.27
ILINCOI	US-067D		UA2AA00CB	57	57	2304	2580	FR	NEUILLYSUF	48.88	2.27	FR	NEUILLYSUF	48.88	2.27
IETTGOI	US-967D		UA2AA00CB	57	57	2304	3190	FR	NEUILLYSUF	48.88	2.27	FR	NEUILLYSUF	48.88	2.27
ILINCOI	US-067D		UA2AA00CB	57	57	2304	1120	FR	NEUILLYSUF	48.88	2.27	FR	NEUILLYSUF	48.88	2.27
IFTNCOI	US-967D		UA2AA00CB	57	57	2304	1600	FR	NEUILLYSUF	48.88	2.27	FR	NEUILLYSUF	48.88	2.27
IETTGOI	US-967D		UA2AA00CB	57	57	2304	1608	FR	NEUILLYSUF	48.88	2.27	FR	NEUILLYSUF	48.88	2.27
ILINCOI	US-067D		UA2AA00CB	57	57	2304	3050	FR	NEUILLYSUF	48.88	2.27	FR	NEUILLYSUF	48.88	2.27
IETTGOI	US-967D		UA2AA00CB	57	57	2304	1063	FR	NEUILLYSUF	48.88	2.27	FR	NEUILLYSUF	48.88	2.27

Page 1 of 6 Page Size: 30 (Max: 100 rows per page)

Displaying 1 - 30 of 174

saved 80219757069313

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

Done



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

XK Session Viewer - Mozilla Firefox

ic.gov https://xks-central.corp.nsa.ic.gov:8443/XKEYSCORE/layouts/popOutLayout.jsp?pageTitle=Session+Viewer&rowUrl=%2F

This system is audited for USSID 18 and Human Rights Act compliance
 CLASSIFICATION: SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL

X-KEYSCORE C2C Session Viewer

Session 15 of 17

Date/Time	Case Notation	From IP	To IP	From Port	To Port	Protocol	Length
2011-04-11 13:47:44	3-411846/000000	192.██████████ (Private Address)	10.██████████ (Private Address)	43070	12468	ICP	774

Session Headers (3) Meta (7) Attachments (1)

Formatter: ASCII Send to: Download Session Mode: Snippet Options Search Content

Quick Clicks

- Session
- Attachments
 - unknown
 - lex
 - unknown_516.x-ww
- One-Click Searches
 - Find fingerprint
 - nds/discovery/feurs
 - http/getwith_content
 - nds/discovery/feurs
 - Find traffic on
 - 192.██████████
 - 10.██████████
 - Find application
 - http/getx-www-form-url
 - Find proxy hash
 - 0d0c20f7
 - Find opposite side of sess
 - 192.██████████-43070
 - 10.██████████

```

GET /CAVIT HTTP/1.0
User-Agent: 62521C333F63DA79333FB2C02702E7BD2
Accept: */*
Host: 10.██████████:12468
Content-type: application/x-www-form-urlencoded
Connection: Keep-Alive

Reset from local:(1231) seq = 2661134980
    
```

This system is audited for USSID 18 and Human Rights Act compliance
 CLASSIFICATION: SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL

Done

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...**

XKEYSCORE CNE (more)



XK Session Viewer - Mozilla Firefox

https://xks-central.compsa.af.mil:8443/XKEYSCORE/layouts/popOutLayout.jsp?pageTitle=Session Viewer ShowUrl=%2FXKEYSCORE%2F%2FmetaViewer!

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

X-KEYSCORE C2C Session Viewer

Session: 50 of 703

Date/Time	Case Fixation	From IP	To IP	From Port	To Port	Protocol	Length
2011-04-12 02:06:12	CC.WYUJCCAACDTD						10074

Session: Header (3) Meta (4)

Format: XML_PAYLOAD Send to: Download Session Mode: Snippet Use one Search context: enter text to search

Quick Clicks

- Security
- One-Click Searches
 - Find Intranet
 - ... exfil/experimental/process
 - Find traffic on
 - ... dnt_payload/processlist
 - ... dnt_payload/processlist
 - ... dnt_payload/processlist
 - Find opposite side of case on
 - ... C ->

PAYLOAD XML

```

<Process creationTime="2011-04-05T00:37:09.631250000" description="initia." pid="463" ppid="302">lsass.exe</Process>
<Process creationTime="2011-04-05T00:37:11.72343750000" description="initia." pid="655" ppid="140">svchost.exe</Process>
<Process creationTime="2011-04-05T00:37:34.781250000" description="initia." pid="728" ppid="440">svchost.exe</Process>
<Process creationTime="2011-04-05T00:37:35.359375000" description="initia." pid="792" ppid="440">svchost.exe</Process>
<Process creationTime="2011-04-05T00:37:36.484375000" description="initia." pid="844" ppid="440">svchost.exe</Process>
<Process creationTime="2011-04-05T00:37:40.703125000" description="initia." pid="863" ppid="440">svchost.exe</Process>
<Process creationTime="2011-04-05T00:37:41.390525000" description="initia." pid="895" ppid="440">svchost.exe</Process>
<Process creationTime="2011-04-05T00:37:42.718750000" description="initia." pid="968" ppid="140">ccsvchost.exe</Process>
<Process creationTime="2011-04-05T00:37:54.640525000" description="initia." pid="1348" ppid="440">msdtc.exe</Process>
<Process creationTime="2011-04-05T00:37:57.171875000" description="initia." pid="1454" ppid="440">fwrts.exe</Process>
<Process creationTime="2011-04-05T00:37:57.710750000" description="initia." pid="1530" ppid="440">svchost.exe</Process>
<Process creationTime="2011-04-05T00:37:58.046375000" description="initia." pid="1532" ppid="440">HLPlaserJetService.exe</Process>
<Process creationTime="2011-04-05T00:38:00.625000000" description="initia." pid="1530" ppid="440">HP5Svc.exe</Process>
<Process creationTime="2011-04-05T00:38:00.750000000" description="initia." pid="1630" ppid="140">KPMONJ-1.exe</Process>
<Process creationTime="2011-04-05T00:38:01.234375000" description="initia." pid="1620" ppid="440">svchost.exe</Process>
<Process creationTime="2011-04-05T00:38:01.421875000" description="initia." pid="1644" ppid="440">HOSTSVI.exe</Process>
<Process creationTime="2011-04-05T00:38:07.125000000" description="initia." pid="1672" ppid="440">svchost.exe</Process>
<Process creationTime="2011-04-05T00:38:02.500000000" description="initia." pid="1696" ppid="440">svchost.exe</Process>
<Process creationTime="2011-04-05T00:38:02.625000000" description="initia." pid="1720" ppid="440">ftvscan.exe</Process>
<Process creationTime="2011-04-05T00:38:08.046375000" description="initia." pid="1802" ppid="440">svchost.exe</Process>
<Process creationTime="2011-04-05T00:38:108.437500000" description="initia." pid="1928" ppid="140">VMwareSvc.exe</Process>
<Process creationTime="2011-04-05T00:38:14.562500000" description="initia." pid="2216" ppid="440">svchost.exe</Process>
<Process creationTime="2011-04-05T00:38:14.671875000" description="initia." pid="2240" ppid="1644">HOSTSVI.exe</Process>
<Process creationTime="2011-04-05T00:38:17.625000000" description="initia." pid="2350" ppid="1740">fwrts.exe</Process>
<Process creationTime="2011-04-05T00:38:23.031250000" description="initia." pid="2620" ppid="656">winbrvse.exe</Process>
<Process creationTime="2011-04-05T00:45:47.108340500" description="initia." pid="1638" ppid="704">explorer.exe</Process>
<Process creationTime="2011-04-05T00:45:48.67234375000" description="initia." pid="1736" ppid="844">svchost.exe</Process>
<Process creationTime="2011-04-05T00:45:54.681250000" description="initia." pid="2042" ppid="1688">VMwareRay.exe</Process>
<Process creationTime="2011-04-05T00:45:57.839375000" description="initia." pid="2838" ppid="1688">VMwareUser.exe</Process>
<Process creationTime="2011-04-05T00:46:00.750766600" description="initia." pid="2956" ppid="1688">svchost.exe</Process>
<Process creationTime="2011-04-05T00:46:02.203303200" description="initia." pid="750" ppid="1000">cfm.exe</Process>
<Process creationTime="2011-04-05T00:46:06.675359700" description="initia." pid="452" ppid="1000">hpstservice.exe</Process>
<Process creationTime="2011-04-05T00:46:15.408522600" description="initia." pid="3530" ppid="3395">cmd.exe</Process>
<Process creationTime="2011-04-05T00:46:25.556893000" description="initia." pid="328" ppid="1823">dwm.exe</Process>
<Process creationTime="2011-04-05T00:56:53.997113900" description="initia." pid="4050" ppid="392">logon.scr</Process>
<Process creationTime="2011-04-11T22:28:03.260310500" description="Started" pid="242" ppid="320">csrss.exe</Process>
<Process creationTime="2011-04-11T22:28:03.416595500" description="Started" pid="5130" ppid="320">svchost.exe</Process>
<Process creationTime="2011-04-11T22:25:30.503396000" description="Started" pid="5440" ppid="320">csrss.exe</Process>
<Process creationTime="2011-04-11T22:25:39.660251000" description="Started" pid="5430" ppid="320">winlogon.exe</Process>
<Process creationTime="2011-04-11T22:25:39.953250000" description="Started" pid="363" ppid="320">csrss.exe</Process>
<Process creationTime="2011-04-11T22:25:39.609140000" description="Started" pid="138" ppid="320">winlogon.exe</Process>
<Process creationTime="2011-04-11T22:48:36.768533500" description="Started" pid="4656" ppid="320">csrss.exe</Process>
<Process creationTime="2011-04-11T22:48:36.956257500" description="Started" 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

Done



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