The First 24: Responding to an Attack Within the Critical First Day

David Amsler, CEO/CIO

Foreground Security

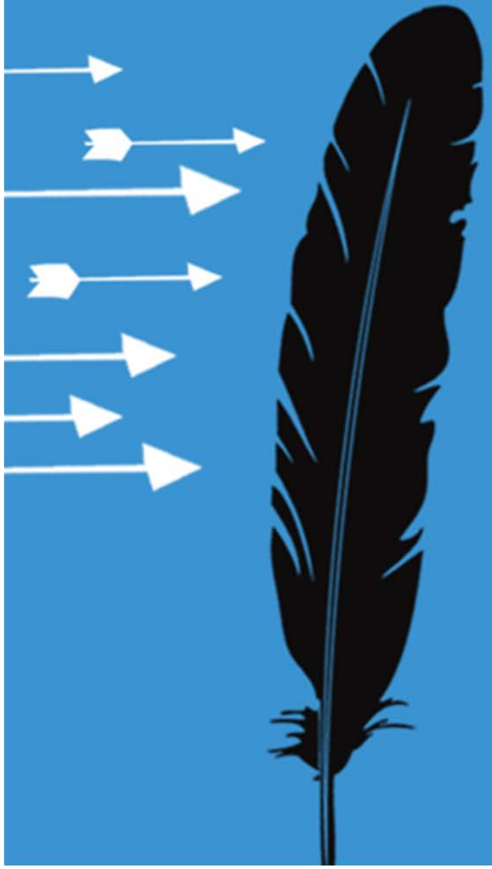
Session ID: DAS-107

Session Classification: Intermediate

RSACONFERENCE2012

THE FIRST 24

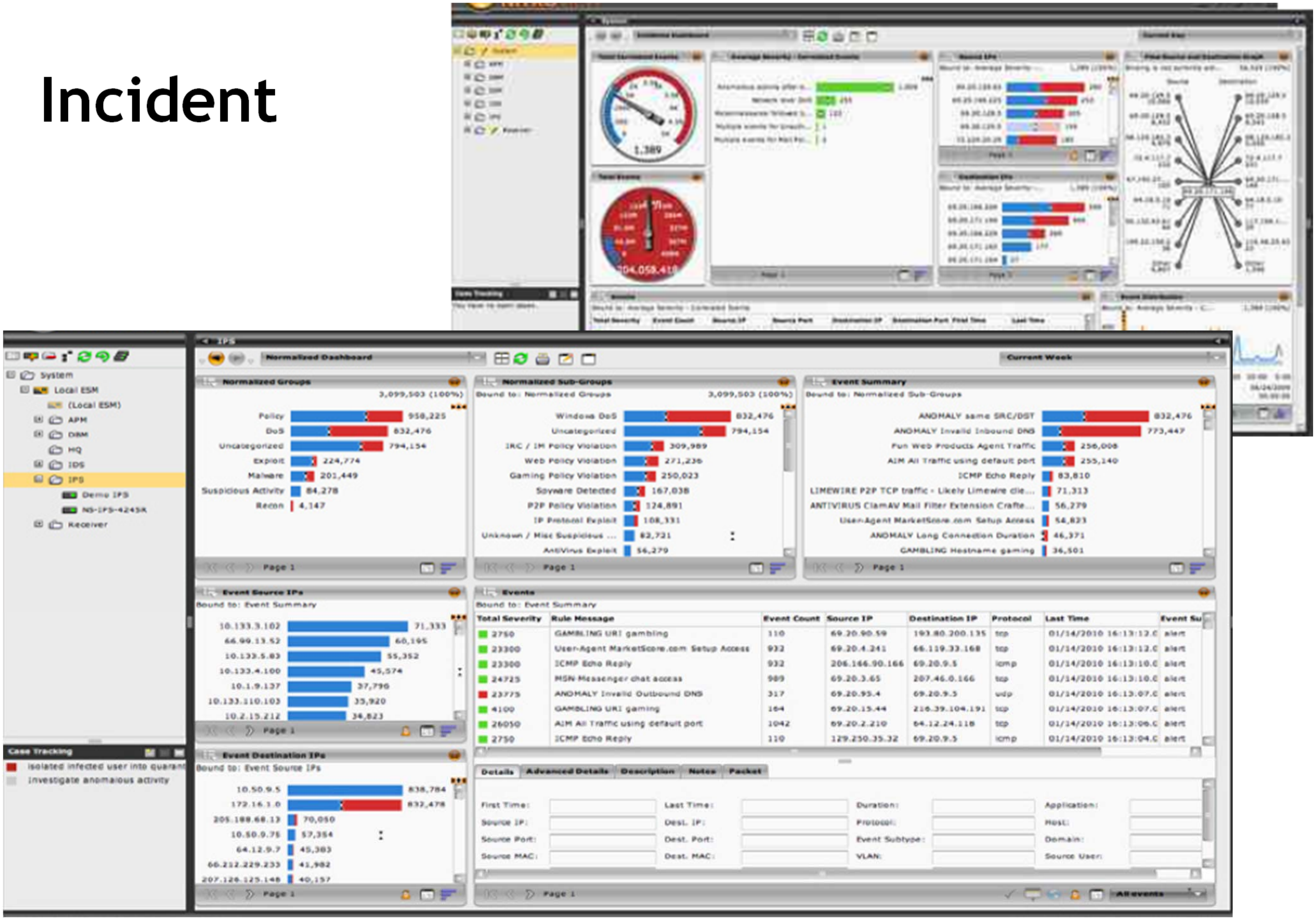
- True Story: The Incident = OWNED!
  - Names & details have been redacted to protect the innocent
- Our Response
  - It was a bloody battle
- Failures
  - No one is perfect
- Successes
  - What did we do in advance to make us successful



Incident = OWNED

WEDNESDAY, NOVEMBER 23, 2011. 10:00pm

Incident



Normalized Groups — 3,099,503 (100%)

Policy 958,225
DoS 832,476
Uncategorized 794,154
Exploit 224,774
Malware 201,449
Suspicious Activity 84,278
Recon 4,147

Normalized Sub-Groups — Bound to: Normalized Groups — 3,099,503 (100%)

Windows DoS 832,476
Uncategorized 794,154
IRC / IM Policy Violation 309,989
Web Policy Violation 271,236
Gaming Policy Violation 250,023
Spyware Detected 167,038
P2P Policy Violation 124,891
IP Protocol Exploit 108,331
Unknown / Misc Suspicious ... 82,721
AntiVirus Exploit 56,279

Event Summary — Bound to: Normalized Sub-Groups

ANOMALY same SRC/DST 832,476
ANOMALY Invalid Inbound DNS 773,447
Fun Web Products Agent Traffic 256,008
AIM All Traffic using default port 255,140
ICMP Echo Reply 83,810
LIMEWIRE P2P TCP traffic - Likely Limewire clie... 71,313
ANTIVIRUS ClamAV Mail Filter Extension Crafte... 56,279
User-Agent MarketScore.com Setup Access 54,823
ANOMALY Long Connection Duration 46,371
GAMBLING Hostname gaming 36,501

Event Source IPs — Bound to: Event Summary

10.133.3.102 71,333
66.99.13.52 60,195
10.133.5.83 55,352
10.133.4.100 45,574
10.1.9.137 37,796
10.133.110.103 35,920
10.2.15.212 34,823

Event Destination IPs — Bound to: Event Source IPs

10.50.9.5 838,784
172.16.1.0 832,478
205.188.68.13 70,050
10.50.9.75 57,354
64.12.9.7 45,383
66.212.229.233 41,982
207.126.125.148 40,157

Events — Bound to: Event Summary

Total Severity	Rule Message	Event Count	Source IP	Destination IP	Protocol	Last Time	Event Su
🟩 2750	GAMBLING URI gambling	110	69.20.90.59	193.80.200.135	tcp	01/14/2010 16:13:12.0	alert
🟩 23300	User-Agent MarketScore.com Setup Access	932	69.20.4.241	66.119.33.168	tcp	01/14/2010 16:13:12.0	alert
🟩 23300	ICMP Echo Reply	932	206.166.90.166	69.20.9.5	icmp	01/14/2010 16:13:10.0	alert
🟩 24725	MSN Messenger chat access	989	69.20.3.65	207.46.0.166	tcp	01/14/2010 16:13:10.0	alert
🟥 23775	ANOMALY Invalid Outbound DNS	317	69.20.95.4	69.20.9.5	udp	01/14/2010 16:13:07.0	alert
🟩 4100	GAMBLING URI gaming	164	69.20.15.44	216.39.104.191	tcp	01/14/2010 16:13:07.0	alert
🟩 26050	AIM All Traffic using default port	1042	69.20.2.210	64.12.24.118	tcp	01/14/2010 16:13:06.0	alert
🟩 2750	ICMP Echo Reply	110	129.250.35.32	69.20.9.5	icmp	01/14/2010 16:13:04.0	alert

Details | Advanced Details | Description | Notes | Packet

First Time:
Last Time:
Duration:
Application:
Source IP:
Dest. IP:
Protocol:
Host:
Source Port:
Dest. Port:
Event Subtype:
Domain:
Source MAC:
Dest. MAC:
VLAN:
Source User:

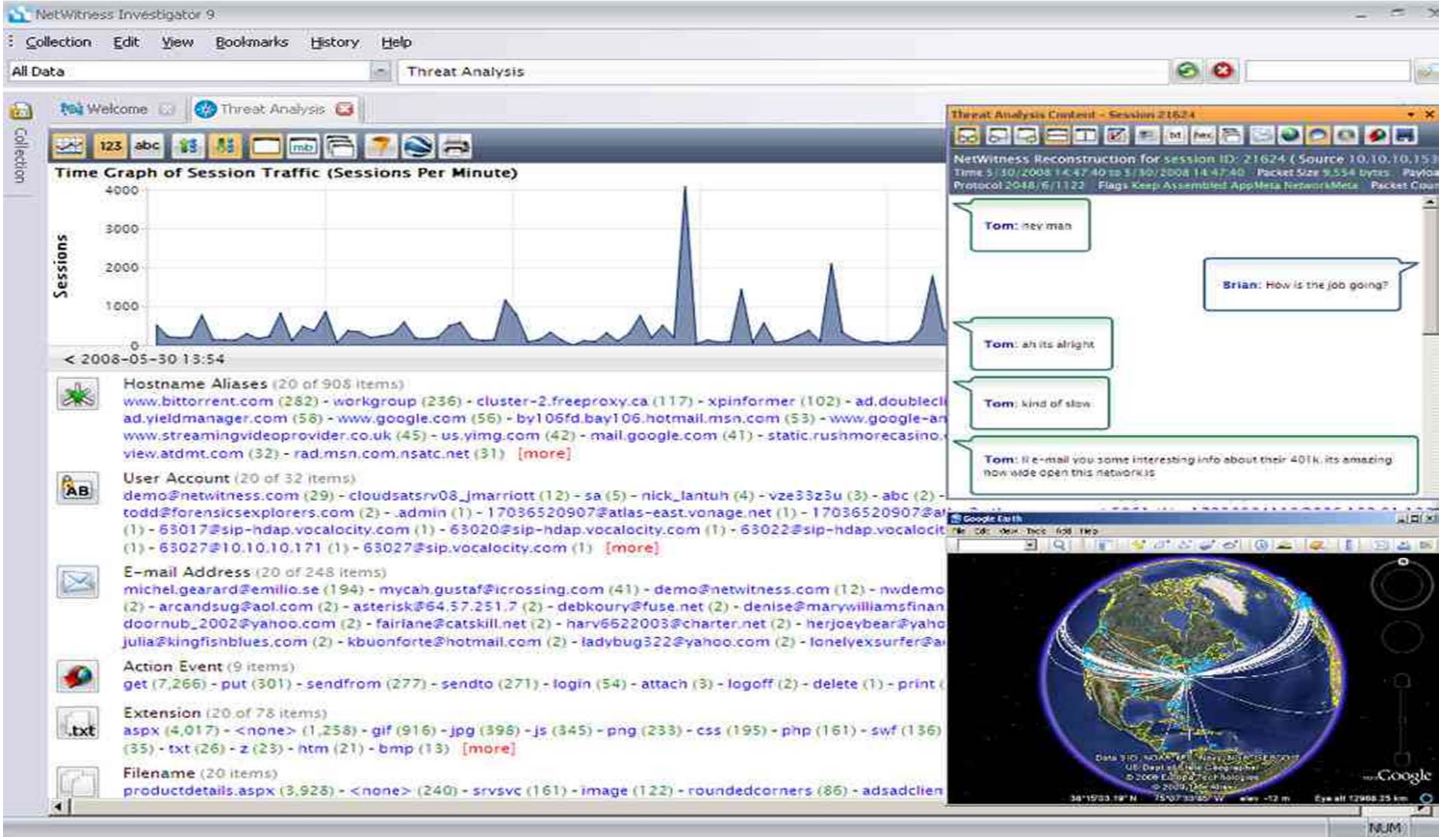
Case Tracking

🟥 isolated infected user into quarant
Investigate anomalous activity

FOREGROUND SECURITY™

RSACONFERENCE2012

Incident



Hostname Aliases (20 of 908 items)
www.bittorrent.com (282) - workgroup (236) - cluster-2.freeproxy.ca (117) - xpinformer (102) - ad.doublecli
ad.yieldmanager.com (56) - www.google.com (56) - by106fd.bay106.hotmail.msn.com (53) - www.google-an
www.streamingvideoprovider.co.uk (45) - us.yimg.com (42) - mail.google.com (41) - static.rushmorecasino.
view.atdmt.com (32) - rad.msn.com.nsatc.net (31) [more]

User Account (20 of 32 items)
demo@netwitness.com (29) - cloudsatsrv08_jmarriott (12) - sa (5) - nick_lantuh (4) - vze33z3u (3) - abc (2) -
todd@forensicsexplorers.com (2) - .admin (1) - 17036520907@atlas-east.vonage.net (1) - 17036520907@at
(1) - 63017@sip-hdap.vocalocity.com (1) - 63020@sip-hdap.vocalocity.com (1) - 63022@sip-hdap.vocalocit
(1) - 63027@10.10.10.171 (1) - 63027@sip.vocalocity.com (1) [more]

E-mail Address (20 of 248 items)
michel.gearard@emilio.se (194) - mycah.gustaf@icrossing.com (41) - demo@netwitness.com (12) - nwdemo
(2) - arcandsug@aol.com (2) - asterisk@64.57.251.7 (2) - debkoury@fuse.net (2) - denise@marywilliamsfinan
doornub_2002@yahoo.com (2) - fairlane@catskill.net (2) - harv6622003@charter.net (2) - herjoeybear@yaho
julia@kingfishblues.com (2) - kbuonforte@hotmail.com (2) - ladybug322@yahoo.com (2) - lonelyexsurfer@a

Action Event (9 items)
get (7,266) - put (301) - sendfrom (277) - sendto (271) - login (54) - attach (3) - logoff (2) - delete (1) - print (

Extension (20 of 78 items)
aspx (4,017) - <none> (1,258) - gif (916) - jpg (398) - js (345) - png (233) - css (195) - php (161) - swf (136)
(35) - txt (26) - z (23) - htm (21) - bmp (13) [more]

Filename (20 items)
productdetails.aspx (3,928) - <none> (240) - srvsvc (161) - image (122) - roundedcorners (86) - adsadclien

NetWitness Reconstruction for session ID: 21624 (Source 10.10.10.153
Time 5/30/2008 14:47:40 to 5/30/2008 14:47:40 Packet Size 9,554 bytes Payloa
Protocol 2048/6/1122 Flags Keep Assembled AppMeta NetworkMeta Packet Coun

Tom: hey man

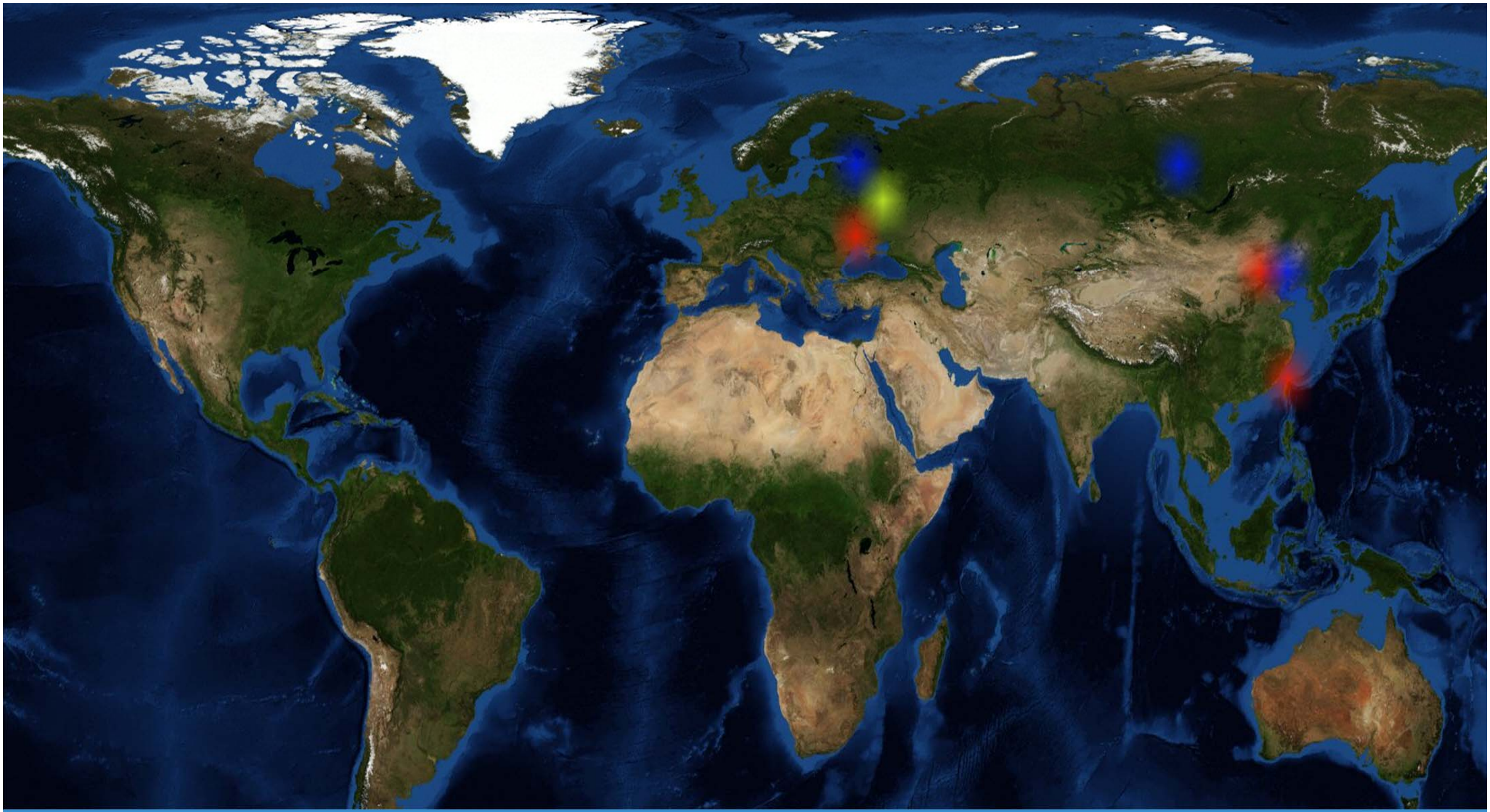
Brian: How is the job going?

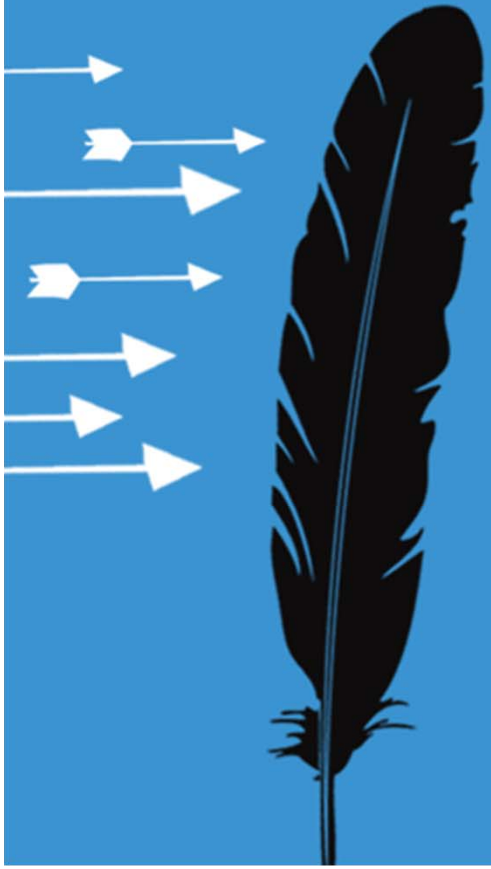
Tom: ah its alright

Tom: kind of slow

Tom: Ill e-mail you some interesting info about their 401k, its amazing how wide open this network is

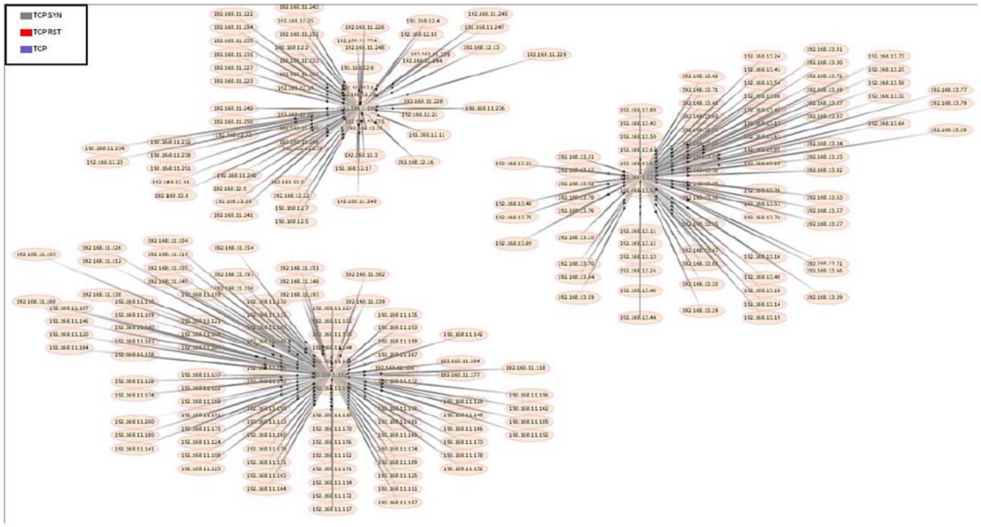
Incident

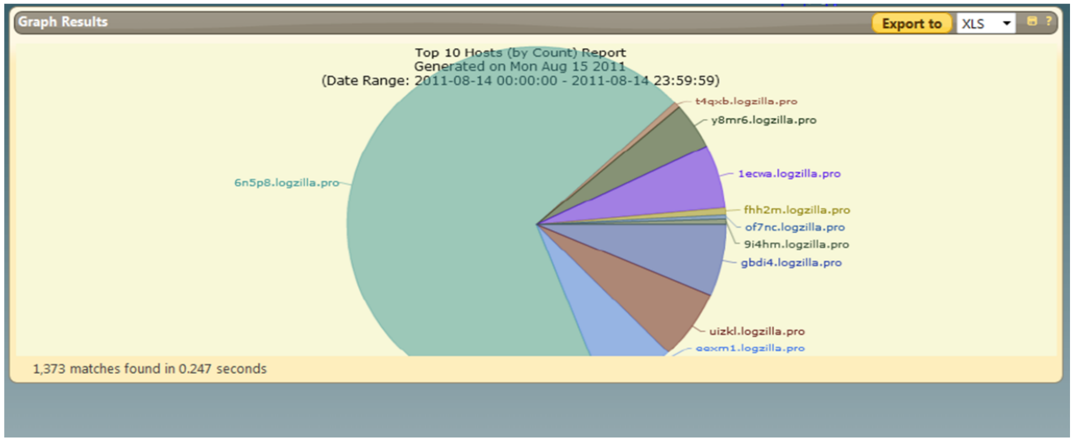




Our Team Responds

Step 1: SOC Analysis





Top 10 Hosts (by Count) Report
Generated on Mon Aug 15 2011
(Date Range: 2011-08-14 00:00:00 - 2011-08-14 23:59:59)

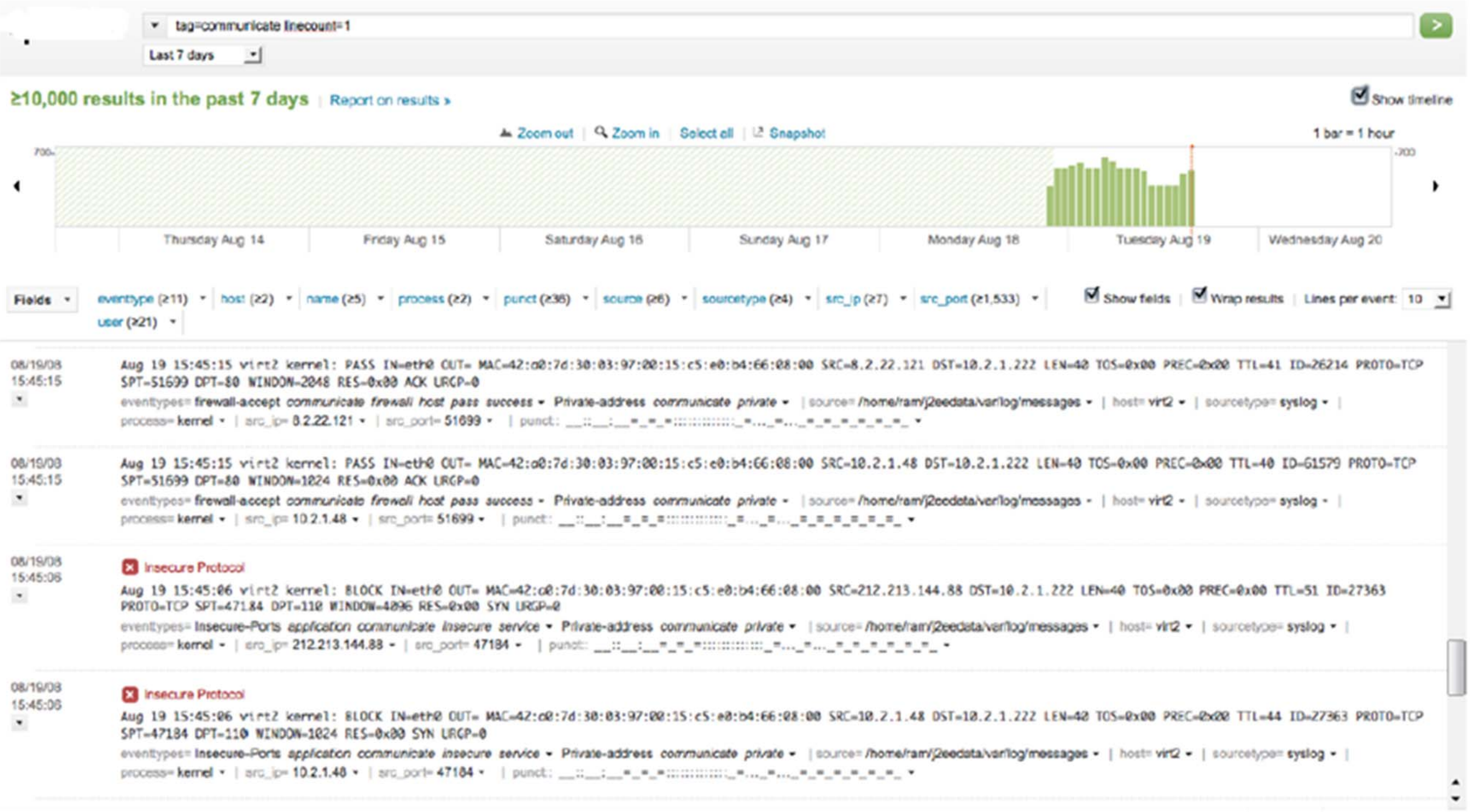
1,373 matches found in 0.247 seconds

- Tier 1 Analysts Investigate
  - Gather Data
  - Investigate the IP’s: Internal & External
  - This is LARGE and traffic looks very suspicious (encrypted and tunneled)

FOREGROUND SECURITY™

RSACONFERENCE2012

Investigate



```
08/19/08
15:45:15
Aug 19 15:45:15 virt2 kernel: PASS IN=eth0 OUT= MAC=42:a0:7d:30:03:97:00:15:c5:e0:b4:66:08:00 SRC=8.2.22.121 DST=10.2.1.222 LEN=40 TOS=0x00 PREC=0x00 TTL=41 ID=26214 PROTO=TCP
SPT=51699 DPT=80 WINDOW=2048 RES=0x00 ACK URGP=0
eventtypes= firewall-accept communicate firewall host pass success ▾ Private-address communicate private ▾ | source= /home/ram/j2eedata/var/log/messages ▾ | host= virt2 ▾ | sourcetype= syslog ▾ |
process= kernel ▾ | src_ip= 8.2.22.121 ▾ | src_port= 51699 ▾ | punct: __::__:__=_=_=:::::::::::::_=..._=..._=_=_=_=_=_=_ ▾

08/19/08
15:45:15
Aug 19 15:45:15 virt2 kernel: PASS IN=eth0 OUT= MAC=42:a0:7d:30:03:97:00:15:c5:e0:b4:66:08:00 SRC=10.2.1.48 DST=10.2.1.222 LEN=40 TOS=0x00 PREC=0x00 TTL=40 ID=61579 PROTO=TCP
SPT=51699 DPT=80 WINDOW=1024 RES=0x00 ACK URGP=0
eventtypes= firewall-accept communicate firewall host pass success ▾ Private-address communicate private ▾ | source= /home/ram/j2eedata/var/log/messages ▾ | host= virt2 ▾ | sourcetype= syslog ▾ |
process= kernel ▾ | src_ip= 10.2.1.48 ▾ | src_port= 51699 ▾ | punct: __::__:__=_=_=:::::::::::::_=..._=..._=_=_=_=_=_=_ ▾

08/19/08
15:45:06
☒ Insecure Protocol
Aug 19 15:45:06 virt2 kernel: BLOCK IN=eth0 OUT= MAC=42:a0:7d:30:03:97:00:15:c5:e0:b4:66:08:00 SRC=212.213.144.88 DST=10.2.1.222 LEN=40 TOS=0x00 PREC=0x00 TTL=51 ID=27363
PROTO=TCP SPT=47184 DPT=110 WINDOW=4096 RES=0x00 SYN URGP=0
eventtypes= Insecure-Ports application communicate insecure service ▾ Private-address communicate private ▾ | source= /home/ram/j2eedata/var/log/messages ▾ | host= virt2 ▾ | sourcetype= syslog ▾ |
process= kernel ▾ | src_ip= 212.213.144.88 ▾ | src_port= 47184 ▾ | punct: __::__:__=_=_=:::::::::::::_=..._=..._=_=_=_=_=_=_ ▾

08/19/08
15:45:06
☒ Insecure Protocol
Aug 19 15:45:06 virt2 kernel: BLOCK IN=eth0 OUT= MAC=42:a0:7d:30:03:97:00:15:c5:e0:b4:66:08:00 SRC=10.2.1.48 DST=10.2.1.222 LEN=40 TOS=0x00 PREC=0x00 TTL=44 ID=27363 PROTO=TCP
SPT=47184 DPT=110 WINDOW=1024 RES=0x00 SYN URGP=0
eventtypes= Insecure-Ports application communicate insecure service ▾ Private-address communicate private ▾ | source= /home/ram/j2eedata/var/log/messages ▾ | host= virt2 ▾ | sourcetype= syslog ▾ |
process= kernel ▾ | src_ip= 10.2.1.48 ▾ | src_port= 47184 ▾ | punct: __::__:__=_=_=:::::::::::::_=..._=..._=_=_=_=_=_=_ ▾
```

Step 1: SOC Analysis

- Tier 1 Analysts Investigate
- Create Incident Report
- Call in the Calvary!!!

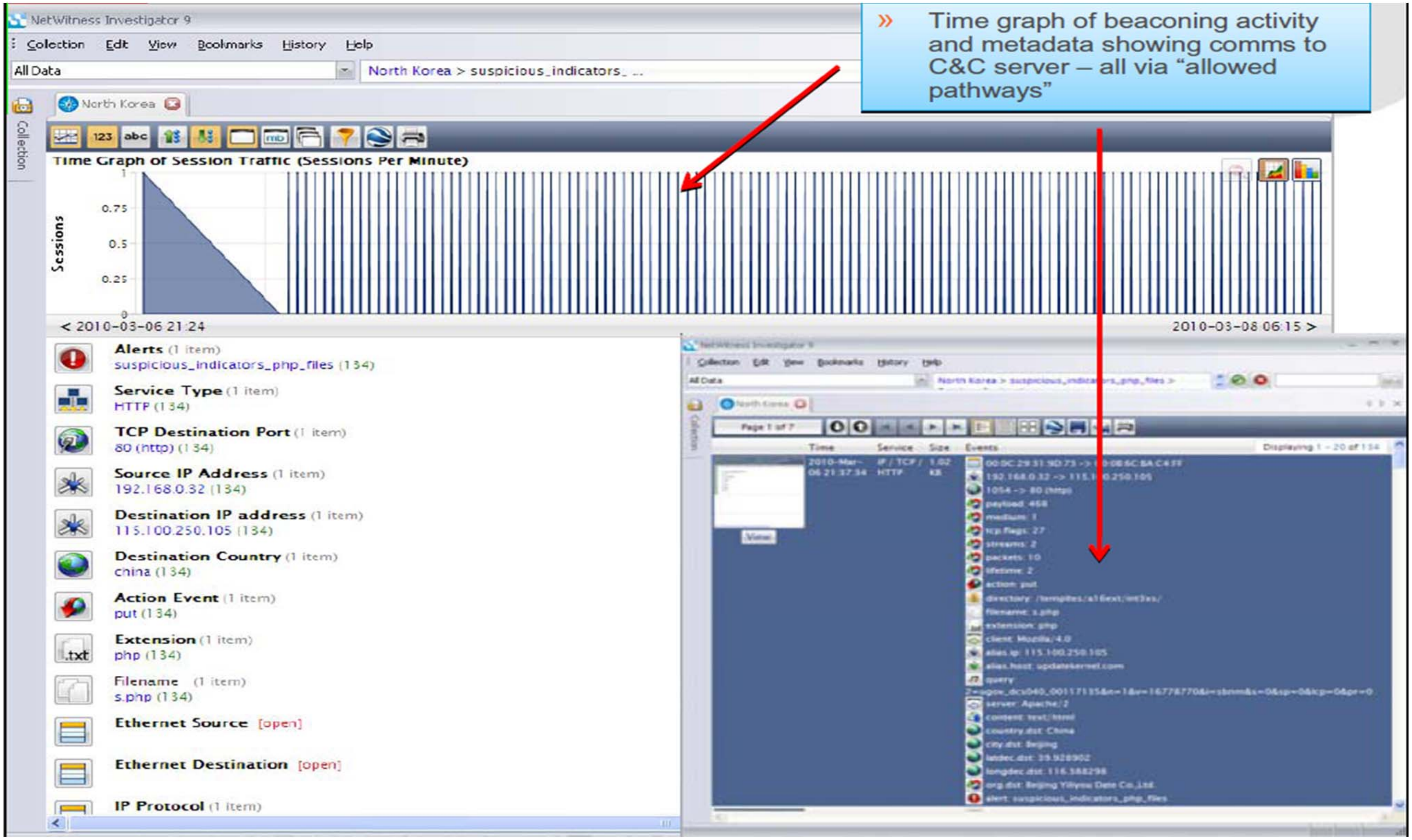
Step 2: Here comes the Calvary!

- Tier 2 & 3 Analysts Investigate

Step 2: IR Response

- Do not alert the adversary = Change Nothing YET
- Indicators of Compromise
- Make Forensic Images of Infected Systems
- Communication Plan

Investigation


NetWitness Investigator 9
Collection Edit View Bookmarks History Help
All Data
North Korea > suspicious_indicators_ ...
North Korea
Collection
123 abc
Time Graph of Session Traffic (Sessions Per Minute)
Sessions
1
0.75
0.5
0.25
0
< 2010-03-06 21:24
2010-03-08 06:15 >

» Time graph of beaconing activity and metadata showing comms to C&C server – all via "allowed pathways"

Alerts (1 item)
suspicious_indicators_php_files (134)

Service Type (1 item)
HTTP (134)

TCP Destination Port (1 item)
80 (http) (134)

Source IP Address (1 item)
192.168.0.32 (134)

Destination IP address (1 item)
115.100.250.105 (134)

Destination Country (1 item)
china (134)

Action Event (1 item)
put (134)

Extension (1 item)
php (134)

Filename (1 item)
s.php (134)

Ethernet Source [open]

Ethernet Destination [open]

IP Protocol (1 item)

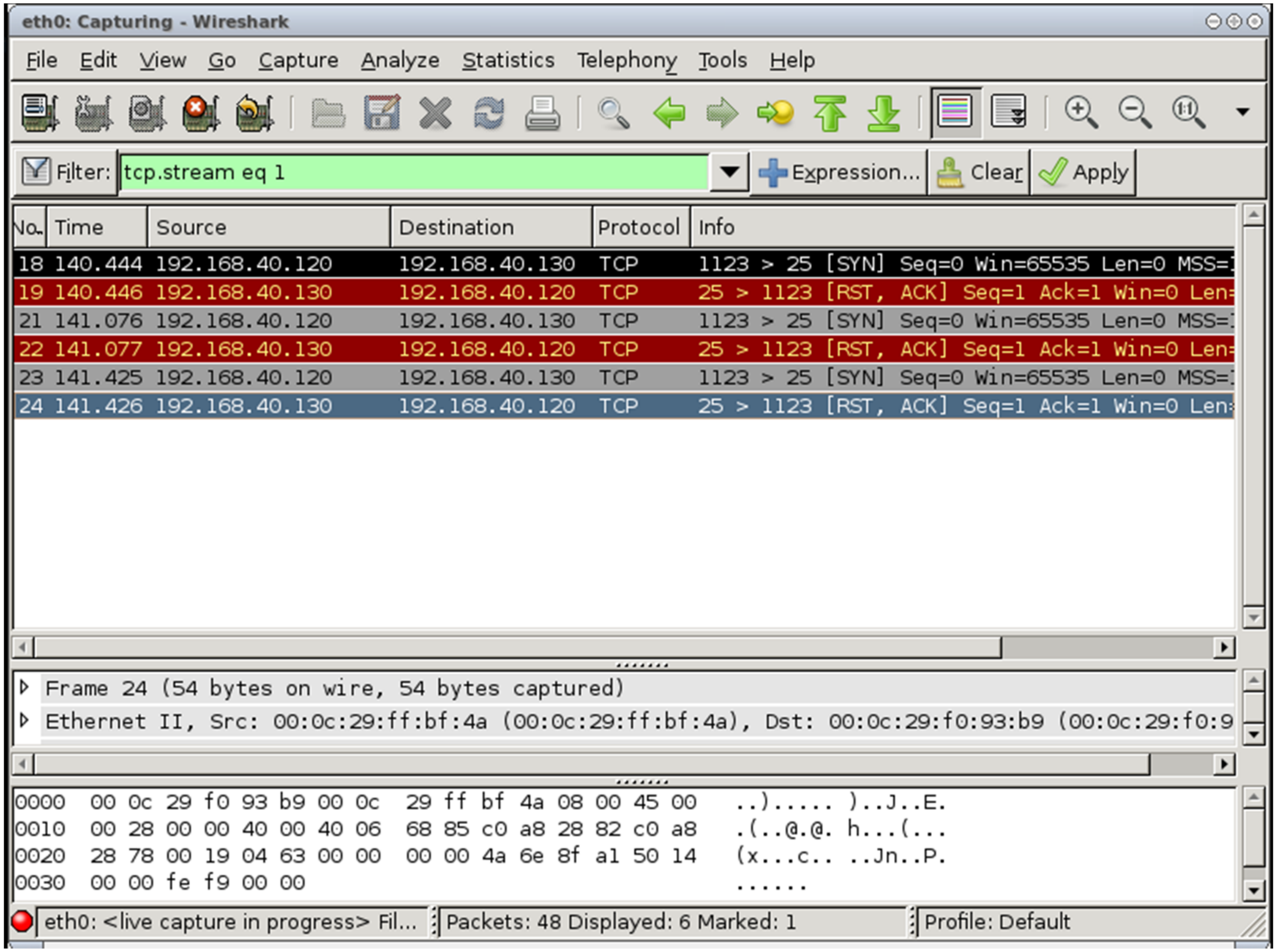
NetWitness Investigator 9
Collection Edit View Bookmarks History Help
All Data
North Korea > suspicious_indicators_php_files >
North Korea
Collection
Page 1 of 7
View

Displaying 1 – 20 of 134

Time	Service	Size	Events
2010-Mar-06 21:37:34	IP / TCP / HTTP	1.02 KB	00:0C:29:31:9D:73 -> 00:0B:6C:BA:C4:FF 192.168.0.32 -> 115.100.250.105 1054 -> 80 (http) payload: 468 medium: 1 tcp.flags: 27 streams: 2 packets: 10 lifetime: 2 action: put directory: /templtes/a16ext/int3xs/ filename: s.php extension: php client: Mozilla/4.0 alias.ip: 115.100.250.105 alias.host: updatekernel.com query: ?=ugov_dcs040_00117135&n=1&v=16778770&i=sbnm&s=0&sp=0&lcp=0&pr=0 server: Apache/2 content: text/html country.dst: China city.dst: Beijing latdec.dst: 39.928902 longdec.dst: 116.388298 org.dst: Beijing Yiiyou Date Co.,Ltd alert: suspicious_indicators_php_files

Step 3: Indicators of Compromise

Analysis


eth0: Capturing - Wireshark
File Edit View Go Capture Analyze Statistics Telephony Tools Help
Expression...
Clear
Apply

Filter: tcp.stream eq 1

```
No. Time    Source          Destination     Protocol Info
18 140.444 192.168.40.120  192.168.40.130  TCP      1123 > 25 [SYN] Seq=0 Win=65535 Len=0 MSS=1
19 140.446 192.168.40.130  192.168.40.120  TCP      25 > 1123 [RST, ACK] Seq=1 Ack=1 Win=0 Len=
21 141.076 192.168.40.120  192.168.40.130  TCP      1123 > 25 [SYN] Seq=0 Win=65535 Len=0 MSS=1
22 141.077 192.168.40.130  192.168.40.120  TCP      25 > 1123 [RST, ACK] Seq=1 Ack=1 Win=0 Len=
23 141.425 192.168.40.120  192.168.40.130  TCP      1123 > 25 [SYN] Seq=0 Win=65535 Len=0 MSS=1
24 141.426 192.168.40.130  192.168.40.120  TCP      25 > 1123 [RST, ACK] Seq=1 Ack=1 Win=0 Len=
```

```
▷ Frame 24 (54 bytes on wire, 54 bytes captured)
▷ Ethernet II, Src: 00:0c:29:ff:bf:4a (00:0c:29:ff:bf:4a), Dst: 00:0c:29:f0:93:b9 (00:0c:29:f0:9
```

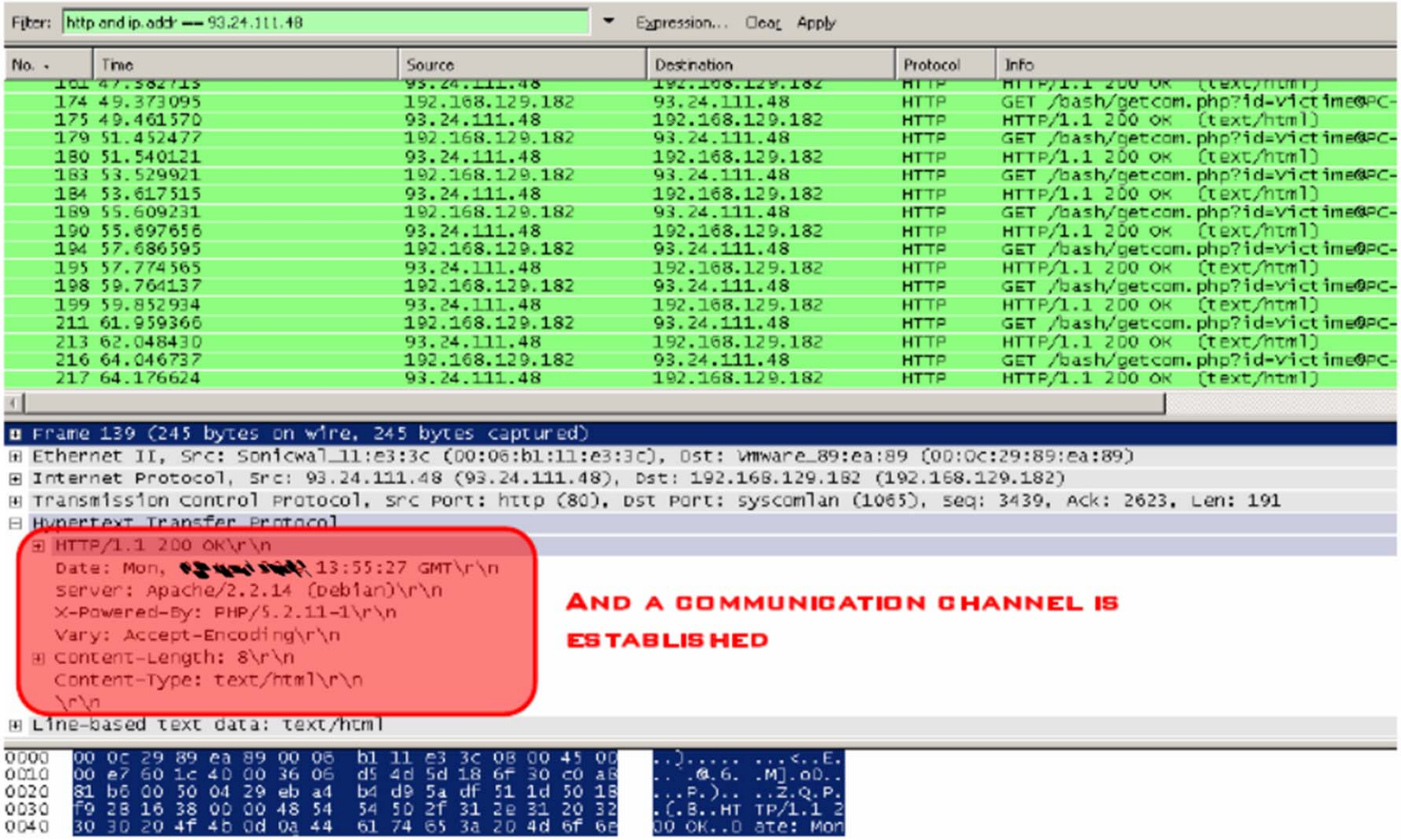
```
0000  00 0c 29 f0 93 b9 00 0c  29 ff bf 4a 08 00 45 00   ..)..... )..J..E.
0010  00 28 00 00 40 00 40 06  68 85 c0 a8 28 82 c0 a8   .(..@.@. h...(...
0020  28 78 00 19 04 63 00 00  00 00 4a 6e 8f a1 50 14   (x...c.. ..Jn..P.
0030  00 00 fe f9 00 00                                  ......
```

eth0: <live capture in progress> Fil...

Packets: 48 Displayed: 6 Marked: 1

Profile: Default

Analysis



Filter: http and ip.addr == 93.24.111.48
Expression... Clear Apply

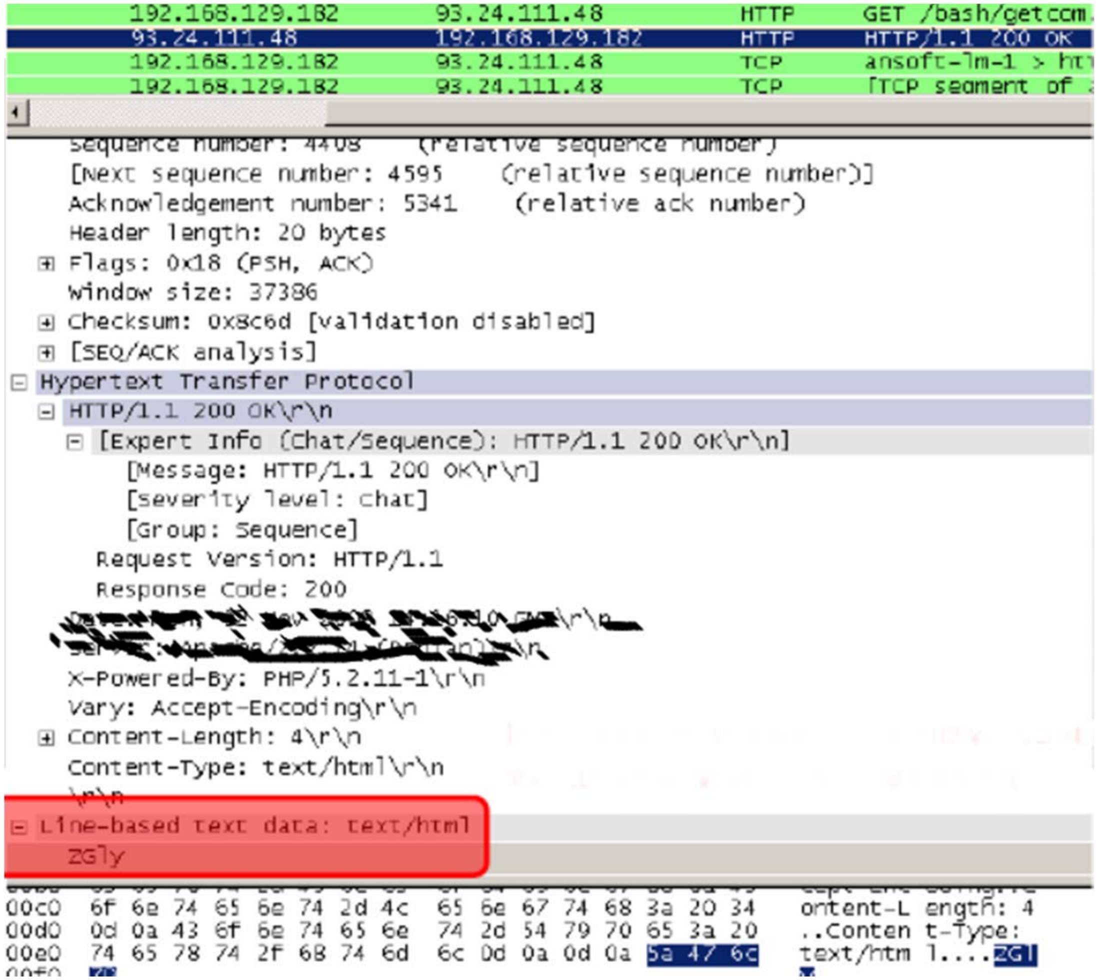
```
No. .  Time        Source           Destination      Protocol  Info
181 47.382713  93.24.111.48     192.168.129.182  HTTP   HTTP/1.1 200 OK  (text/html)
174 49.373095  192.168.129.182  93.24.111.48     HTTP   GET /bash/getcom.php?id=victime@PC-
175 49.461570  93.24.111.48     192.168.129.182  HTTP   HTTP/1.1 200 OK  (text/html)
179 51.452477  192.168.129.182  93.24.111.48     HTTP   GET /bash/getcom.php?id=victime@PC-
180 51.540121  93.24.111.48     192.168.129.182  HTTP   HTTP/1.1 200 OK  (text/html)
183 53.529921  192.168.129.182  93.24.111.48     HTTP   GET /bash/getcom.php?id=victime@PC-
184 53.617515  93.24.111.48     192.168.129.182  HTTP   HTTP/1.1 200 OK  (text/html)
189 55.609231  192.168.129.182  93.24.111.48     HTTP   GET /bash/getcom.php?id=victime@PC-
190 55.697656  93.24.111.48     192.168.129.182  HTTP   HTTP/1.1 200 OK  (text/html)
194 57.686595  192.168.129.182  93.24.111.48     HTTP   GET /bash/getcom.php?id=victime@PC-
195 57.774565  93.24.111.48     192.168.129.182  HTTP   HTTP/1.1 200 OK  (text/html)
198 59.764137  192.168.129.182  93.24.111.48     HTTP   GET /bash/getcom.php?id=victime@PC-
199 59.852934  93.24.111.48     192.168.129.182  HTTP   HTTP/1.1 200 OK  (text/html)
211 61.959366  192.168.129.182  93.24.111.48     HTTP   GET /bash/getcom.php?id=victime@PC-
213 62.048430  93.24.111.48     192.168.129.182  HTTP   HTTP/1.1 200 OK  (text/html)
216 64.046737  192.168.129.182  93.24.111.48     HTTP   GET /bash/getcom.php?id=victime@PC-
217 64.176624  93.24.111.48     192.168.129.182  HTTP   HTTP/1.1 200 OK  (text/html)
```

```
⊞ Frame 139 (245 bytes on wire, 245 bytes captured)
⊞ Ethernet II, Src: Sonicwal_11:e3:3c (00:06:b1:11:e3:3c), Dst: Vmware_89:ea:89 (00:0c:29:89:ea:89)
⊞ Internet Protocol, Src: 93.24.111.48 (93.24.111.48), Dst: 192.168.129.182 (192.168.129.182)
⊞ Transmission Control Protocol, Src Port: http (80), Dst Port: syscomlan (1065), Seq: 3439, Ack: 2623, Len: 191
⊟ Hypertext Transfer Protocol
  ⊞ HTTP/1.1 200 OK\r\n
    Date: Mon, [redacted] 13:55:27 GMT\r\n
    Server: Apache/2.2.14 (Debian)\r\n
    X-Powered-By: PHP/5.2.11-1\r\n
    Vary: Accept-Encoding\r\n
  ⊞ Content-Length: 8\r\n
    Content-Type: text/html\r\n
    \r\n
⊞ Line-based text data: text/html
```

```
0000  00 0c 29 89 ea 89 00 06  b1 11 e3 3c 08 00 45 00   ..)..... ...<..E.
0010  00 e7 60 1c 40 00 36 06  d5 4d 5d 18 6f 30 c0 a8   ..`.@.6. .M].o0..
0020  81 b6 00 50 04 29 eb a4  b4 d9 5a df 51 1d 50 18   ...P.).. ..Z.Q.P.
0030  f9 28 16 38 00 00 48 54  54 50 2f 31 2e 31 20 32   .(.8..HT TP/1.1 2
0040  30 30 20 4f 4b 0d 0a 44  61 74 65 3a 20 4d 6f 6e   00 OK..D ate: Mon
```

AND A COMMUNICATION CHANNEL IS ESTABLISHED

Analysis



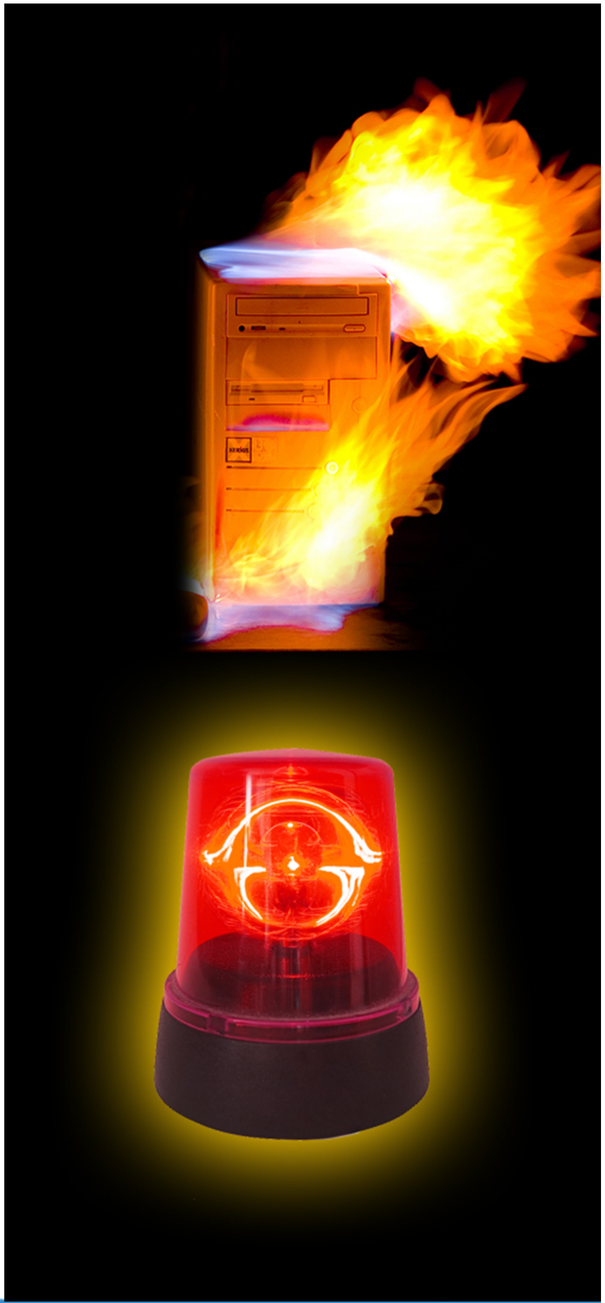
```
192.168.129.182      93.24.111.48       HTTP     GET /bash/getcom.
93.24.111.48         192.168.129.182    HTTP     HTTP/1.1 200 OK
192.168.129.182      93.24.111.48       TCP      ansoft-lm-1 > htt
192.168.129.182      93.24.111.48       TCP      [TCP segment of a

    Sequence number: 4408    (relative sequence number)
    [Next sequence number: 4595    (relative sequence number)]
    Acknowledgement number: 5341    (relative ack number)
    Header length: 20 bytes
  ⊞ Flags: 0x18 (PSH, ACK)
    Window size: 37386
  ⊞ Checksum: 0x8c6d [validation disabled]
  ⊞ [SEQ/ACK analysis]
⊟ Hypertext Transfer Protocol
  ⊟ HTTP/1.1 200 OK\r\n
    ⊟ [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
        [Message: HTTP/1.1 200 OK\r\n]
        [Severity level: Chat]
        [Group: Sequence]
      Request Version: HTTP/1.1
      Response Code: 200
    [redacted]
    X-Powered-By: PHP/5.2.11-1\r\n
    Vary: Accept-Encoding\r\n
  ⊞ Content-Length: 4\r\n
    Content-Type: text/html\r\n
    \r\n
⊟ Line-based text data: text/html
    ZGly

00c0  6f 6e 74 65 6e 74 2d 4c  65 6e 67 74 68 3a 20 34   ontent-L ength: 4
00d0  0d 0a 43 6f 6e 74 65 6e  74 2d 54 79 70 65 3a 20   ..Conten t-Type: 
00e0  74 65 78 74 2f 68 74 6d  6c 0d 0a 0d 0a 5a 47 6c   text/htm l....ZGl
```

Step 4: Full Incident Profile

- Complete Profile on Incident
  - Malware Profile
    - As best as we could at this point – still needed more time to reverse and Analyze
  - Traffic Profile
  - Infection Profile

Step 4:
Full Incident Profile

- Further Attack Profile
  - Hitting Domain Controllers and got a System Admin Account
- Now we are in trouble and we have to do something immediately!!!



Step 5: Respond/Remediate

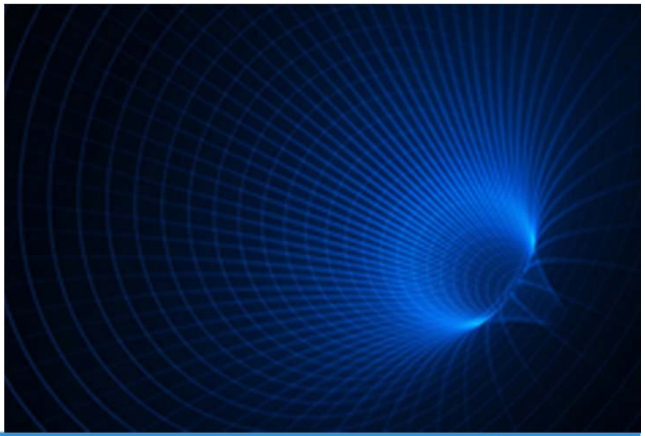
- Coordinated Response Effort

Step 5: Respond/Remediate

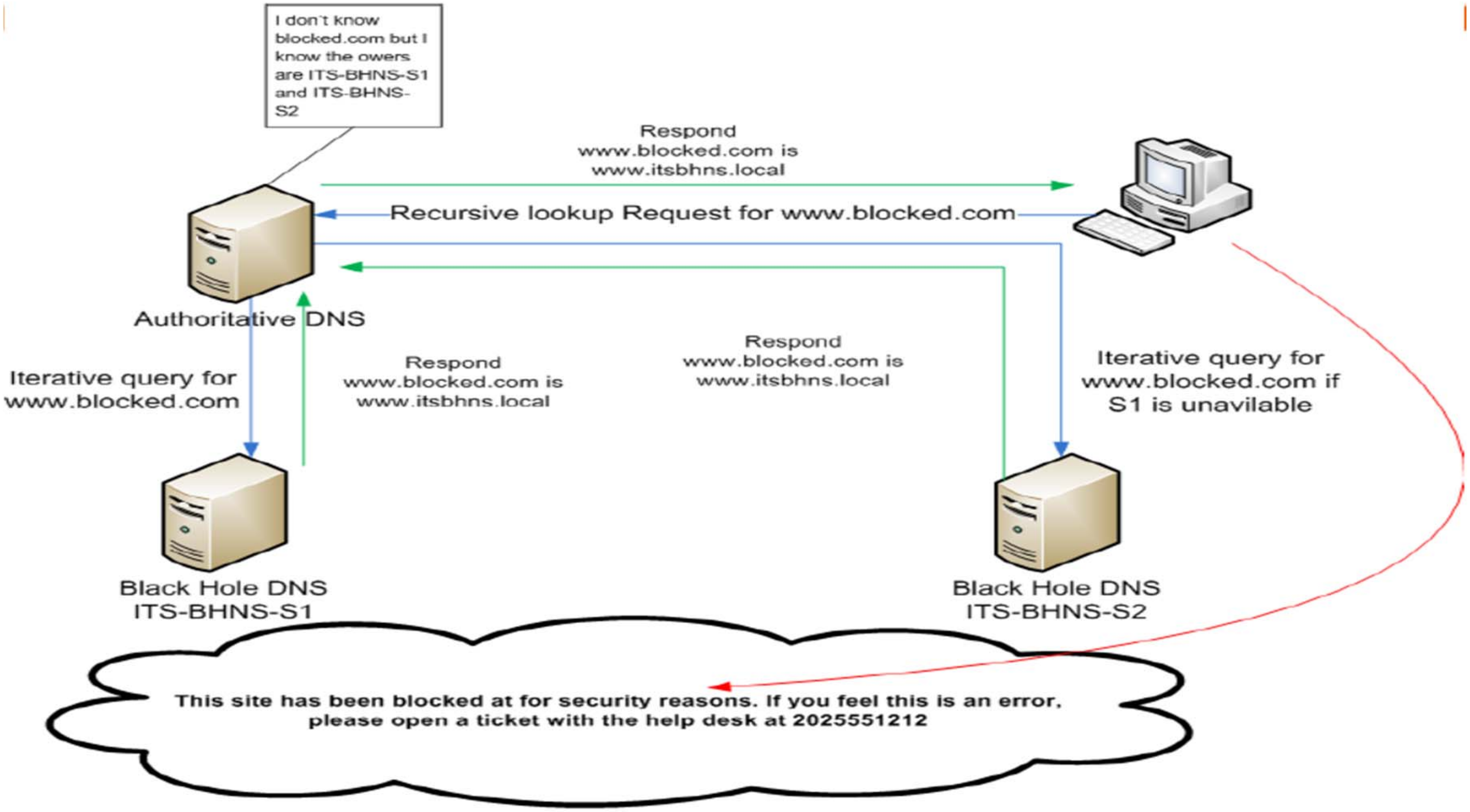
- However, attacker disappears in the middle of this!!!

Step 6:
Re-verse Malware

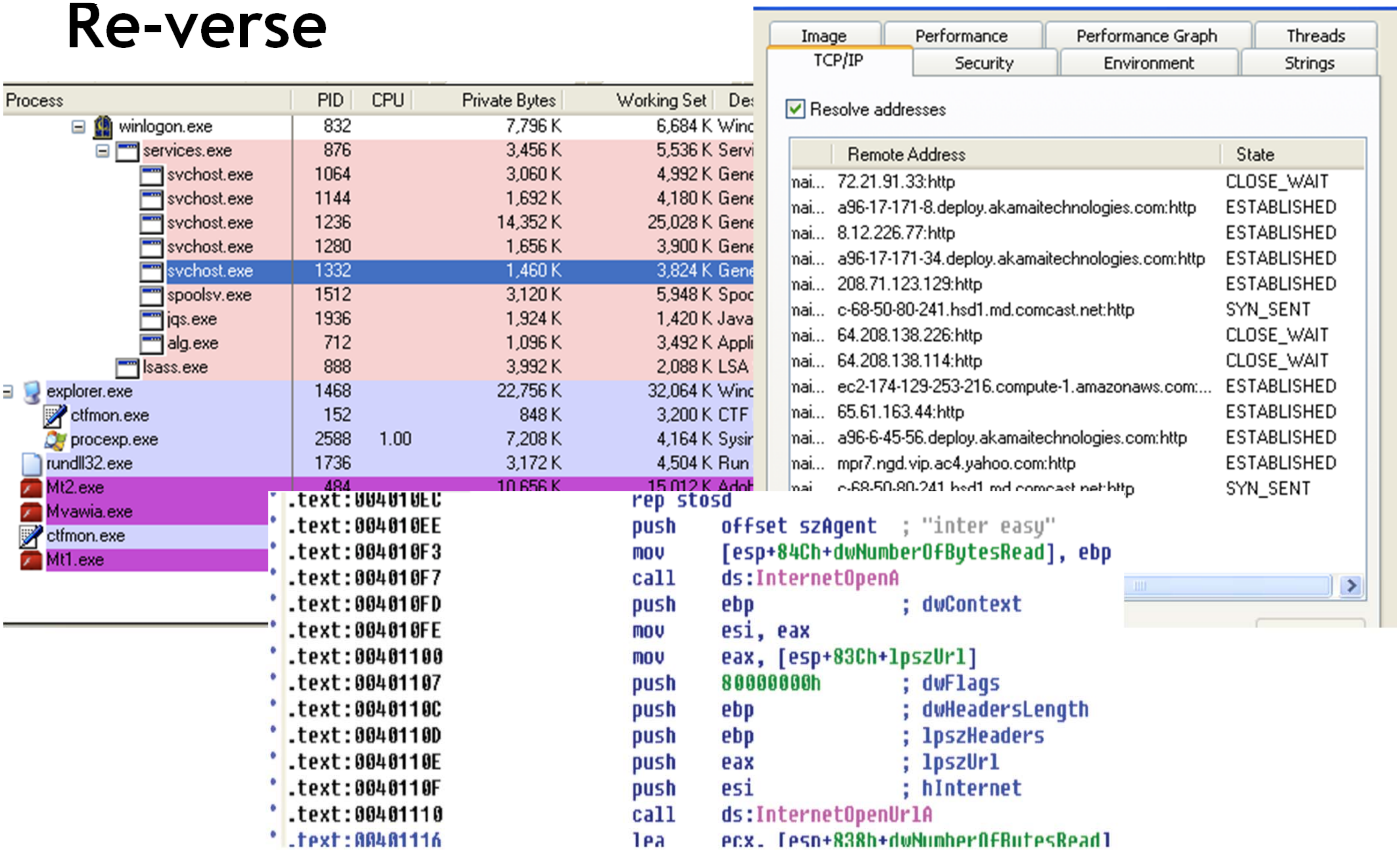
- Analyze Malware
- Reverse
- “Black Hole Network”



Black Hole Network (DNS)


I don`t know blocked.com but I know the owers are ITS-BHNS-S1 and ITS-BHNS-S2
Respond www.blocked.com is www.itsbhns.local
Recursive lookup Request for www.blocked.com
Authoritative DNS
Iterative query for www.blocked.com
Respond www.blocked.com is www.itsbhns.local
Respond www.blocked.com is www.itsbhns.local
Iterative query for www.blocked.com if S1 is unavilable
Black Hole DNS ITS-BHNS-S1
Black Hole DNS ITS-BHNS-S2
This site has been blocked at for security reasons. If you feel this is an error, please open a ticket with the help desk at 2025551212

Re-verse



Process	PID	CPU	Private Bytes	Working Set	Des
winlogon.exe	832		7,796 K	6,684 K	Winc
services.exe	876		3,456 K	5,536 K	Servi
svchost.exe	1064		3,060 K	4,992 K	Gene
svchost.exe	1144		1,692 K	4,180 K	Gene
svchost.exe	1236		14,352 K	25,028 K	Gene
svchost.exe	1280		1,656 K	3,900 K	Gene
svchost.exe	1332		1,460 K	3,824 K	Gene
spoolsv.exe	1512		3,120 K	5,948 K	Spoo
jqs.exe	1936		1,924 K	1,420 K	Java
alg.exe	712		1,096 K	3,492 K	Appli
lsass.exe	888		3,992 K	2,088 K	LSA
explorer.exe	1468		22,756 K	32,064 K	Winc
ctfmon.exe	152		848 K	3,200 K	CTF
procexp.exe	2588	1.00	7,208 K	4,164 K	Sysir
rundll32.exe	1736		3,172 K	4,504 K	Run
Mt2.exe	484		10,656 K	15,012 K	Adob
Mvawia.exe					
ctfmon.exe					
Mt1.exe					

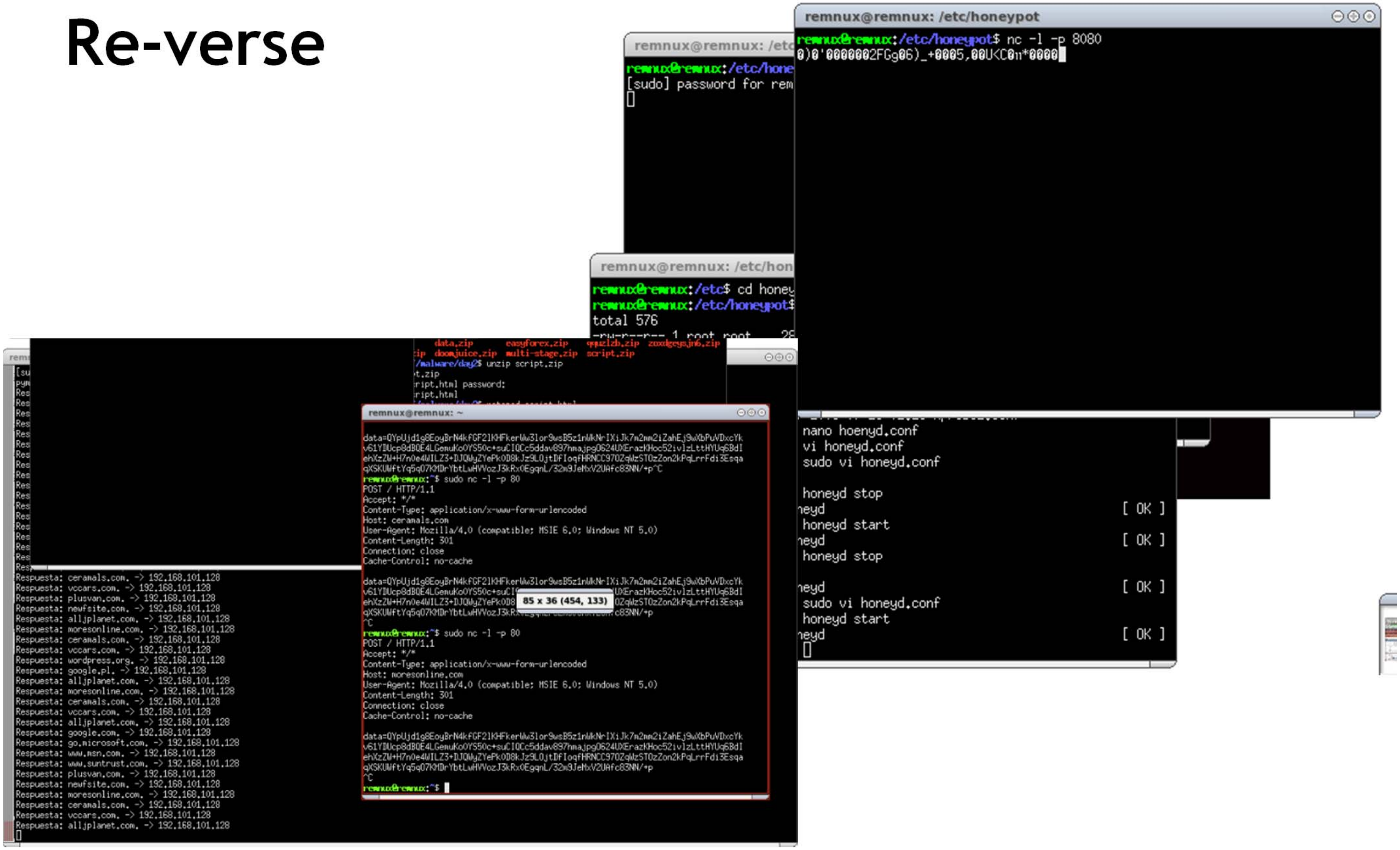
Image | Performance | Performance Graph | Threads
TCP/IP | Security | Environment | Strings

☑ Resolve addresses

	Remote Address	State
nai...	72.21.91.33:http	CLOSE_WAIT
nai...	a96-17-171-8.deploy.akamaitechnologies.com:http	ESTABLISHED
nai...	8.12.226.77:http	ESTABLISHED
nai...	a96-17-171-34.deploy.akamaitechnologies.com:http	ESTABLISHED
nai...	208.71.123.129:http	ESTABLISHED
nai...	c-68-50-80-241.hsd1.md.comcast.net:http	SYN_SENT
nai...	64.208.138.226:http	CLOSE_WAIT
nai...	64.208.138.114:http	CLOSE_WAIT
nai...	ec2-174-129-253-216.compute-1.amazonaws.com:...	ESTABLISHED
nai...	65.61.163.44:http	ESTABLISHED
nai...	a96-6-45-56.deploy.akamaitechnologies.com:http	ESTABLISHED
nai...	mpr7.ngd.vip.ac4.yahoo.com:http	ESTABLISHED
nai...	c-68-50-80-241.hsd1.md.comcast.net:http	SYN_SENT

```
.text:004010EC                 rep stosd
.text:004010EE                 push    offset szAgent  ; "inter easy"
.text:004010F3                 mov     [esp+84Ch+dwNumberOfBytesRead], ebp
.text:004010F7                 call    ds:InternetOpenA
.text:004010FD                 push    ebp             ; dwContext
.text:004010FE                 mov     esi, eax
.text:00401100                 mov     eax, [esp+83Ch+lpszUrl]
.text:00401107                 push    80000000h       ; dwFlags
.text:0040110C                 push    ebp             ; dwHeadersLength
.text:0040110D                 push    ebp             ; lpszHeaders
.text:0040110E                 push    eax             ; lpszUrl
.text:0040110F                 push    esi             ; hInternet
.text:00401110                 call    ds:InternetOpenUrlA
.text:00401116                 lea     ecx, [esp+838h+dwNumberOfBytesRead]
```

Re-verse



```
remnux@remnux: /etc/honeypot
remnux@remnux:/etc/honeypot$ nc -l -p 8080
0)0'0000002FGg06)_+0005,00U<C0п*0000
```

```
remnux@remnux: /etc
remnux@remnux:/etc/hone
[sudo] password for rem
```

```
remnux@remnux: /etc/hon
remnux@remnux:/etc$ cd honey
remnux@remnux:/etc/honeypot$
total 576
-rw-r--r-- 1 root root     28
```

```
    data.zip       easyforex.zip    qquzlzb.zip  zoxdgeysjn6.zip
zip  doomjuice.zip  multi-stage.zip  script.zip
/malware/day2$ unzip script.zip
t.zip
ript.html password:
ript.html
```

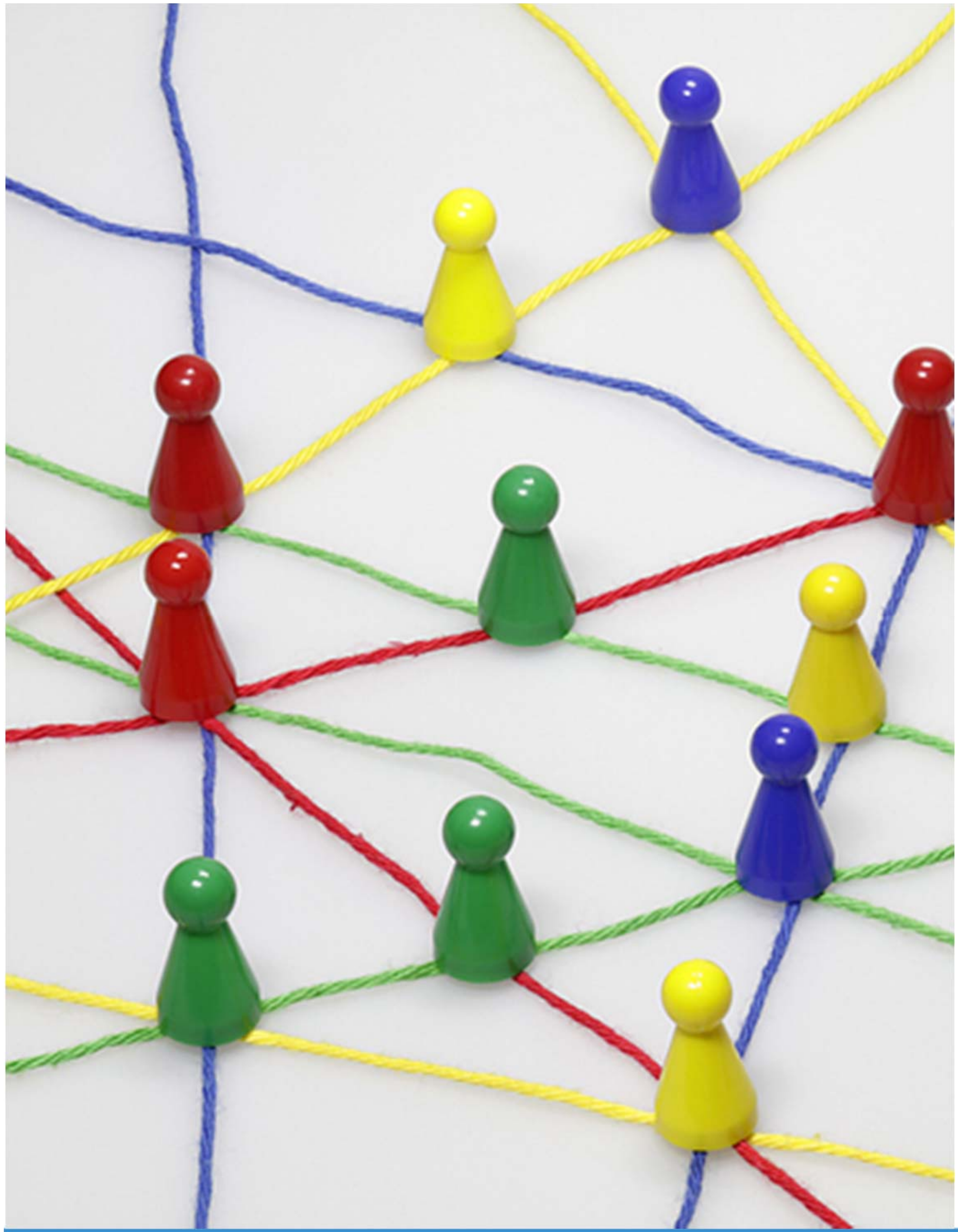
```
remnux@remnux: ~

data=QYpUjd1g8EoyBrN4kfGF2lKHFkerWw3lor9wsB5z1nWkNrIXiJk7m2mm2iZahEj9wXbPuVDxcYk
v61YDUcp8dBQE4LGemuKoOYS50c+suCIQCc5ddav897hmajpg0624UXErazKHoc52ivlzLttHYUq6BdI
ehXzZW+H7n0e4WILZ3+DJQWyZYePkOD8kJz9L0jtDfIoqfHRNCC970ZqWzSTOzZon2kPqLrrFdi3Esqa
qXSKUWftYq5q07KMDrYbtLwHVVozJ3kRx0EgqnL/32m9JeMxV2UAfc83NN/+p^C
remnux@remnux:~$ sudo nc -l -p 80
POST / HTTP/1.1
Accept: */*
Content-Type: application/x-www-form-urlencoded
Host: ceramals.com
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0)
Content-Length: 301
Connection: close
Cache-Control: no-cache

data=QYpUjd1g8EoyBrN4kfGF2lKHFkerWw3lor9wsB5z1nWkNrIXiJk7m2mm2iZahEj9wXbPuVDxcYk
v61YDUcp8dBQE4LGemuKoOYS50c+suCI                  UXErazKHoc52ivlzLttHYUq6BdI
ehXzZW+H7n0e4WILZ3+DJQWyZYePkOD8  85 x 36 (454, 133)  0ZqWzSTOzZon2kPqLrrFdi3Esqa
qXSKUWftYq5q07KMDrYbtLwHVVozJ3kR                   c83NN/+p
^C
remnux@remnux:~$ sudo nc -l -p 80
POST / HTTP/1.1
Accept: */*
Content-Type: application/x-www-form-urlencoded
Host: moresonline.com
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0)
Content-Length: 301
Connection: close
Cache-Control: no-cache

data=QYpUjd1g8EoyBrN4kfGF2lKHFkerWw3lor9wsB5z1nWkNrIXiJk7m2mm2iZahEj9wXbPuVDxcYk
v61YDUcp8dBQE4LGemuKoOYS50c+suCIQCc5ddav897hmajpg0624UXErazKHoc52ivlzLttHYUq6BdI
ehXzZW+H7n0e4WILZ3+DJQWyZYePkOD8kJz9L0jtDfIoqfHRNCC970ZqWzSTOzZon2kPqLrrFdi3Esqa
qXSKUWftYq5q07KMDrYbtLwHVVozJ3kRx0EgqnL/32m9JeMxV2UAfc83NN/+p
^C
remnux@remnux:~$ 
```

```
rem
[su
pym
Res
Res
Res
Res
Res
Res
Res
Res
Res
Res
Res
Res
Res
Res
Res
Res
Res
Respuesta: ceramals.com. -> 192.168.101.128
Respuesta: vccars.com. -> 192.168.101.128
Respuesta: plusvan.com. -> 192.168.101.128
Respuesta: newfsite.com. -> 192.168.101.128
Respuesta: alljplanet.com. -> 192.168.101.128
Respuesta: moresonline.com. -> 192.168.101.128
Respuesta: ceramals.com. -> 192.168.101.128
Respuesta: vccars.com. -> 192.168.101.128
Respuesta: wordpress.org. -> 192.168.101.128
Respuesta: google.pl. -> 192.168.101.128
Respuesta: alljplanet.com. -> 192.168.101.128
Respuesta: moresonline.com. -> 192.168.101.128
Respuesta: ceramals.com. -> 192.168.101.128
Respuesta: vccars.com. -> 192.168.101.128
Respuesta: alljplanet.com. -> 192.168.101.128
Respuesta: google.com. -> 192.168.101.128
Respuesta: go.microsoft.com. -> 192.168.101.128
Respuesta: www.msn.com. -> 192.168.101.128
Respuesta: www.suntrust.com. -> 192.168.101.128
Respuesta: plusvan.com. -> 192.168.101.128
Respuesta: newfsite.com. -> 192.168.101.128
Respuesta: moresonline.com. -> 192.168.101.128
Respuesta: ceramals.com. -> 192.168.101.128
Respuesta: vccars.com. -> 192.168.101.128
Respuesta: alljplanet.com. -> 192.168.101.128
```

```
 nano hoenyd.conf
 vi honeyd.conf
 sudo vi honeyd.conf

 honeyd stop
neyd                                        [ OK ]
 honeyd start
neyd                                        [ OK ]
 honeyd stop

neyd                                        [ OK ]
 sudo vi honeyd.conf
 honeyd start
neyd                                        [ OK ]
```

Step 6: Re-verse Malware cont.

- What did we learn from this?



Step 7: Investigate

- How deep is the Hole?

Step 7: Investigate

- Full Attacker Profile

Step 8: Communicate

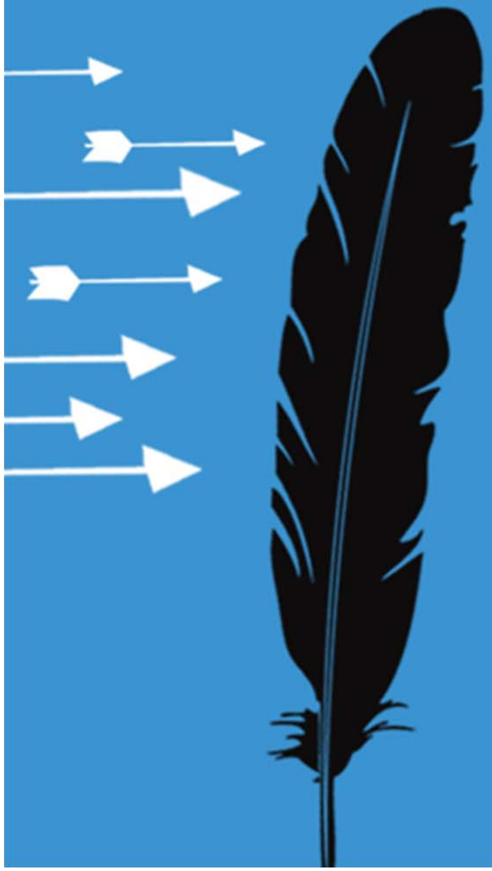
- Who
- What
- When
- Where
- How

Step 9: Remediate

- Active Plan of Defense:
  - New Systems
  - Domain Controllers
  - Blocking
  - Active Monitoring
  - Encryption
  - New Capabilities/Tools

Step 10: Post-Mortem

- Success vs Failure
- What do we need to do differently
- Develop Intelligence
- Information Sharing



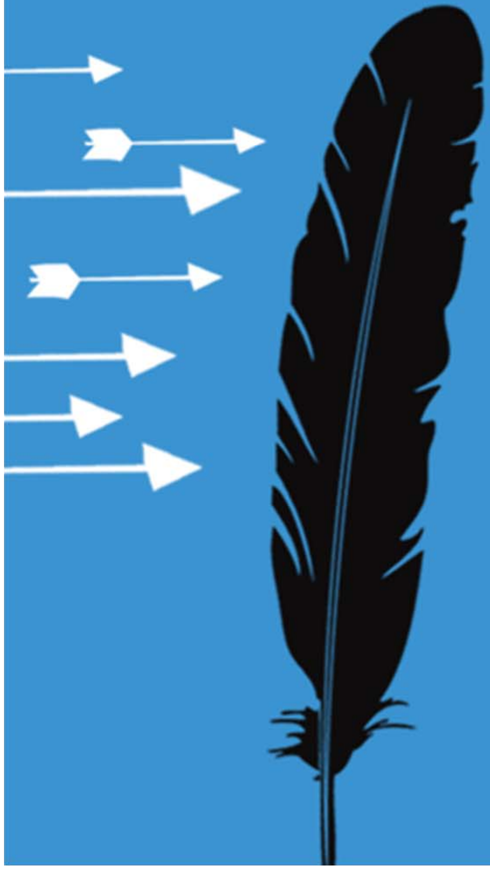
Failures

Some of our Failures

- Did not have full capabilities needed or implemented fully
- Communication Plan Lacking

Some of our Failures

- Too many assumptions or rapid reactions
  - POINT = Never turn off systems (you alert the attacker and you lose valuable forensic data)



Successes

What did we do right?

- Boy Scout Motto =
  “Always be prepared”

What did we do right?

- Logs/SEIM
- Having the Forensic tool sets
- Incident Response Plan & Process
- Full Cooperation of all teams

Success for You

- You Must be Prepared in advance:
- Success =
  - People
  - Processes
  - Technology

Success for You

- People
  - Skills (Malware Analysis, Full Packet Inspection, SOC Analysts, Incident Response Capabilities)
  - This is the hardest part: find these people, train these people, retain these people
  - What do we do that is unique here

People

Success for You

- Processes
  - Incident Response Plan
    - Detailed and thorough for all types of incidents
  - Processes
    - Communication Plan and capabilities (Wiki, chat, etc)
    - Roles & responsibilities (you don't want people doing the same thing)

Process

Success for You

- Technology
  - Full Packet Capture
    - Retention
    - Analysis (Manual & Automated)
  - SEIM/Log Analysis
  - IR&F Tools
    - Host Based & network
    - Scanning Tools (not vuln scanning)
  - Malware Lab/”Black Hole”

Technology

Follow Up

- Questions??

- Take Away – www.foregroundsecurity.com/RSA