
Security
SUCKS!

F

U

D

Is Your Security Team Smarter Than the Bad Guys?… probably not…

The New York Times

Technology

WORLD | U.S. | N.Y. / REGION | BUSINESS | TECHNOLOGY | SCIENCE | HEALTH | SPORTS | OPINION

Search Technology | Go

Inside Technology: Internet | Start-Ups | Business Computing | Companies

Bits Blog »

Malicious Software Infects Corporate Computers

By JOHN MARKOFF
Published: February 18, 2010

A malicious software program has infected the computers of
than 2,500 corporations around the world, according to Net
a computer network security firm.

Tuesday, February 16, 2010

THE WALL STREET JOURNAL. | TECH

Welcome, E
My Account

Asia Edition | Today's Paper • Video • Columns • Blogs • Topics • Journal Community

Home | World | Asia | Business | Markets | Market Data | Tech | Life & Style | Opinion | More

Digits | Personal Technology | All Things Digital

TOP STORIES IN Technology

4 of 10 — Broad New Hacking Attack Detected

5 of 10 — Google Gives $2 Million to Wikipedia

Applie

TECHNOLOGY | FEBRUARY 16, 2010

Broad New Hacking Attack Detected

Global Offensive Snagged Corporate, Personal Data at nearly 2,500 Companies; Operation Is Still Running

Article | Comments (3)

Email | Print | Save This | + More | Text

By SIOBHAN GORMAN

Hackers in Europe and China successfully broke into computers at nearly 2,500 companies and government agencies over the last 18 months in a coordinated global attack that exposed vast amounts of personal and corporate secrets to theft, according to a computer-security company that discovered the breach.

The damage from the latest cyberattack is still being assessed, and affected companies are still being notified. But data compiled by NetWitness, the closely held firm that discovered the breaches, showed that hackers gained access to a wide array of data at 2,411 companies, from credit-card transactions to intellectual property.

Comments | View All »

The Washington Post

TODAY
Subscr

Advertisement

MEDIA PLANET

CLICK HERE to view Mediaplanet's Asthma & Allergy report!

NEWS | POLITICS | OPINIONS | BUSINESS | LOCAL | SPORTS | ART

SEARCH: | go | Search Archi

washingtonpost.com > Technology > Special Reports > Cyber-Securit

More than 75,000 computer systems ha cyber attacks, security firm says

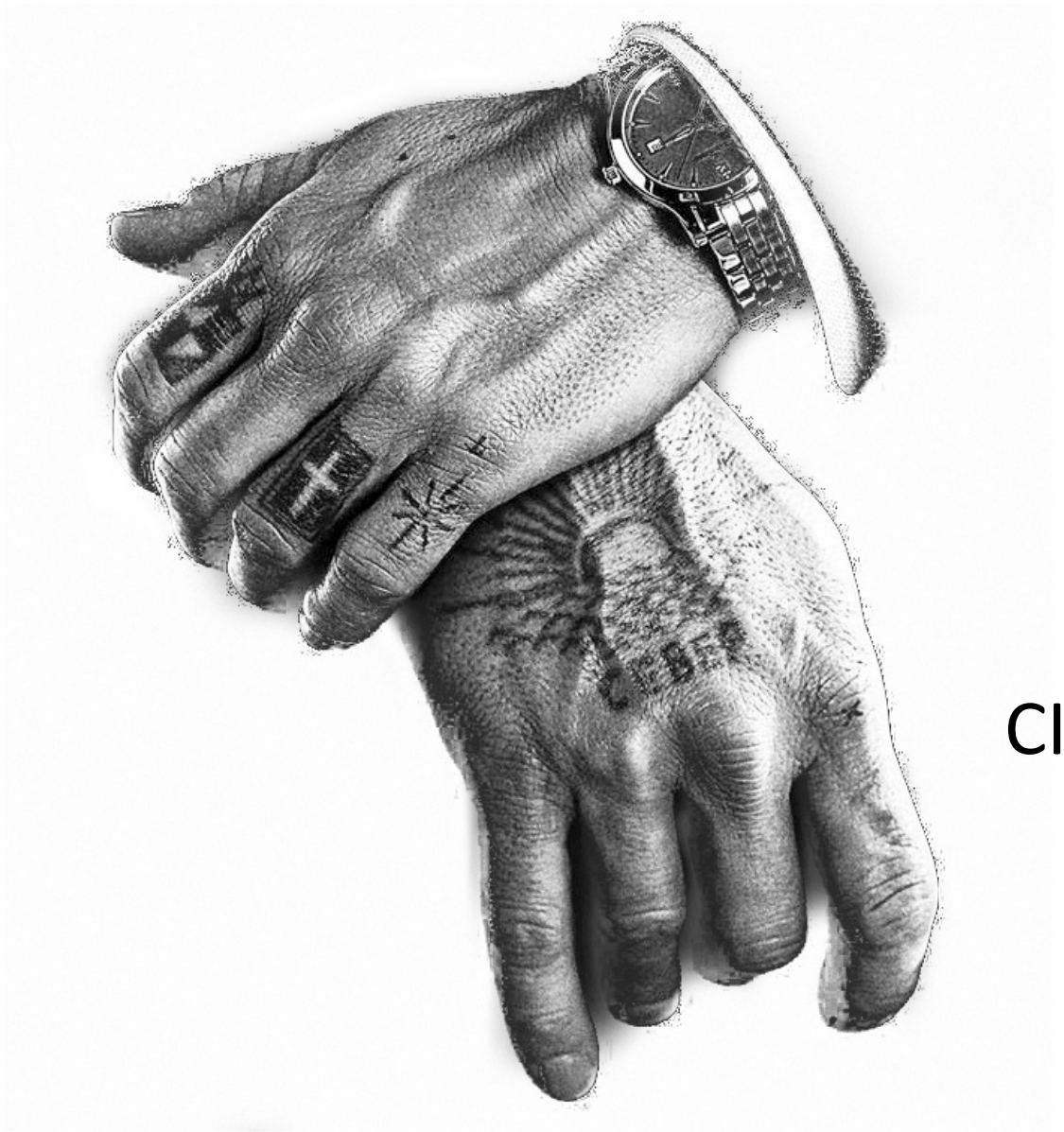
By Ellen Nakashima
Washington Post Staff Writer
Thursday, February 18, 2010

More than 75,000 computer systems at nearly 2,500 companies in the United States and around the world have been hacked in what appears to be one of the largest and most sophisticated attacks by cyber criminals discovered to date, according to a northern Virginia security firm.

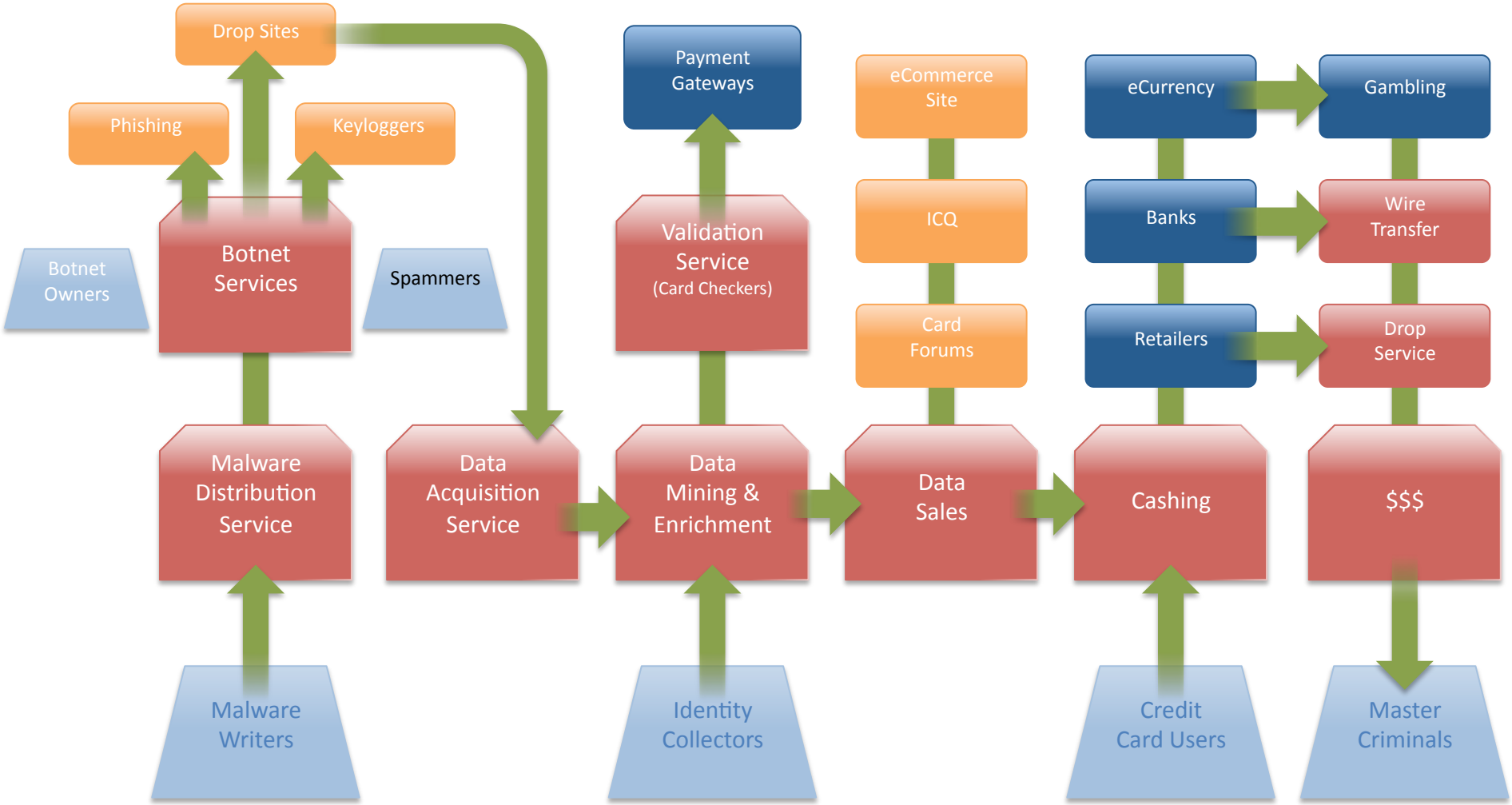

Risk Management
Sucks


R
I
S
K


Who Really Pwns You?



CIO**ski** for a day….


Drop Sites
Phishing
Keyloggers
Botnet Owners
Botnet Services
Spammers
Malware Distribution Service
Malware Writers
Data Acquisition Service
Payment Gateways
Validation Service (Card Checkers)
Data Mining & Enrichment
Identity Collectors
eCommerce Site
ICQ
Card Forums
Data Sales
eCurrency
Banks
Retailers
Cashing
Credit Card Users
Gambling
Wire Transfer
Drop Service
$$$
Master Criminals


There ARE specific targets…

FAIL?

Google hackers duped system ad...

The Washington Post

NEWS | POLITICS | OPINIONS | BUSINESS | LOCAL | SPORTS | ARTS & LIVING | GOING OUT GUIDE | JOBS | CARS | REAL ESTATE |SHOPPING

Google hackers duped system administrators to penetrate networks, experts say

By Ellen Nakashima
Washington Post Staff Writer
Wednesday, April 21, 2010; A15

The hackers who penetrated the computer networks of Google and more than 30 other large companies used an increasingly common means of attack: duping system administrators and other executives who have access to passwords, intellectual property and other information, according to cybersecurity experts familiar with the cases.

"Once you gain access to the directory of user names and passwords, in minutes you can take over a network," said George Kurtz, worldwide chief technology officer for McAfee, a Silicon Valley computer security firm that has been working with more than half a dozen of the targeted companies.

DEFINITELY

Figuring out whom to target and how is the result of research, said Shawn Carpenter, a principal forensics analyst at the security firm NetWitness whose former job involved trying to hack into government agencies' Web sites to help them find their weak spots. "One of the first things we do is build up a dossier," he said. "What conferences has this person spoken at? What people do they know? Are they likely to open up this type of e-mail attachment if I spoof it as coming from a person who has sat on a panel with them?"

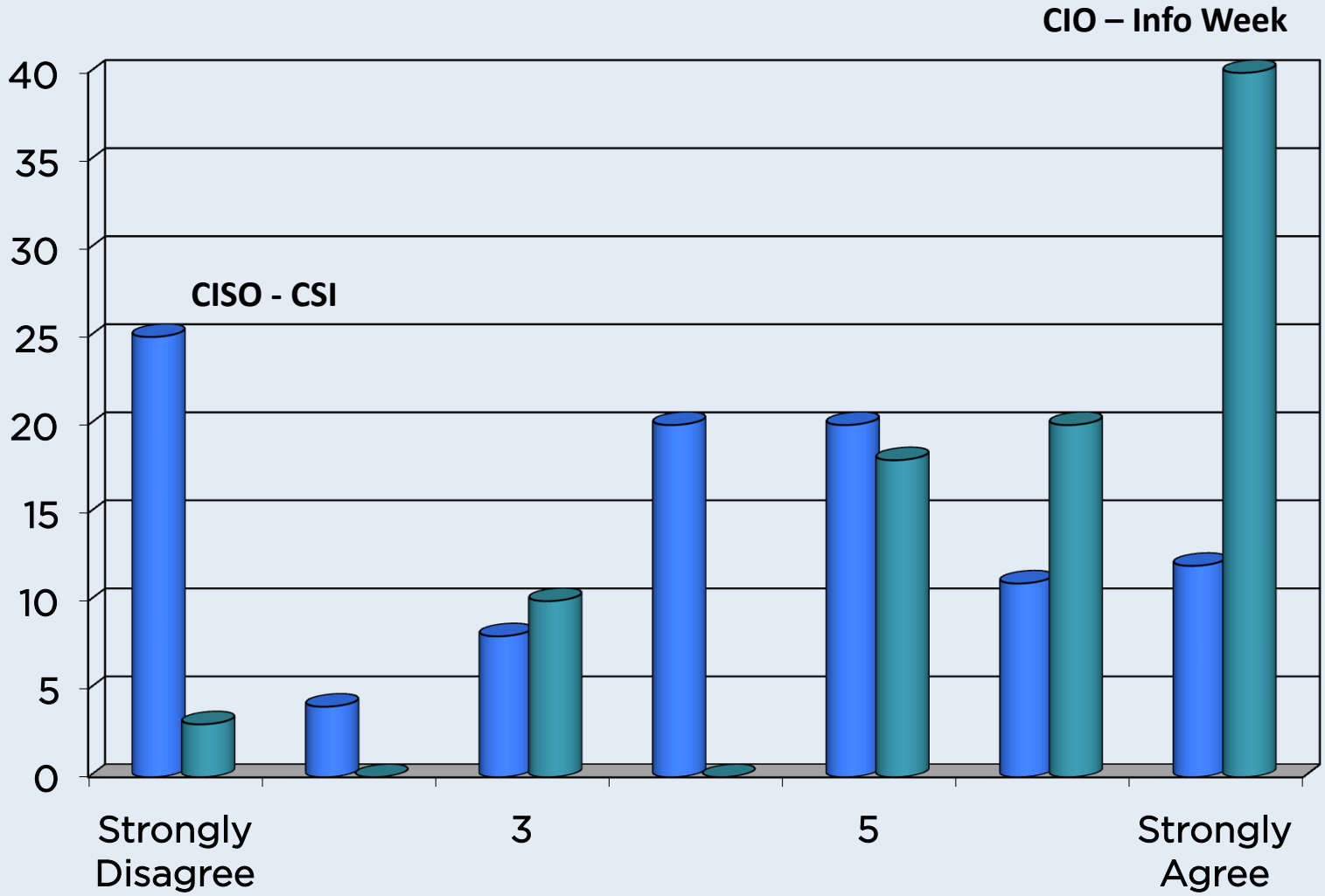
The essence of the attack is "exploiting those human tendencies of curiosity and trust," Carpenter said.

The targeting of personnel is only one aspect of a larger, more sophisticated operation that involves planning the mode of attack, reconnaissance inside a company's network, deciding what type of data to go after, and harvesting and analyzing the data, experts said.

"There's a life cycle of activities that occurs, involving many steps, both with human intelligence and electronic intelligence, to ultimately penetrate these organizations," said Eddie Schwartz, NetWitness's chief security officer. "When you're combining all of these techniques, this is the work of a highly organized group or groups that has specific targets in mind."

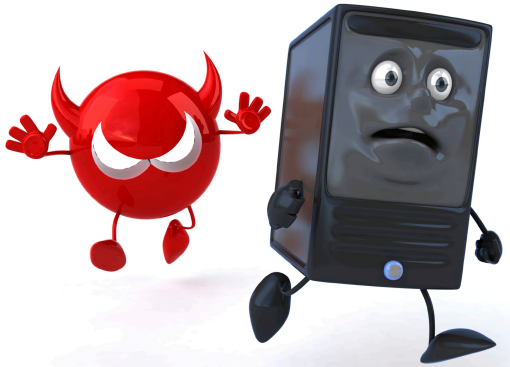
Staff researcher Julie Tate contributed to this report.

The Security Suck-i-ness Factor



RISK=
Threats x
Assets x
Vulnerabilities

SUCKER!!!



Just a question on signatures...

Does the signature team not do Zeus/ZBot configuration files? We have submitted a number (20+) of ".bin" files over the last 6-8 weeks but have yet to see these files detected using "Official" signatures. Should we not submit these files?

Tom

Good Question, Tom!! Maybe You are NOT a SUCKER…


THE
END
OF THE
BEGINNING
Quaint gatehouse on market
Area mortgage rates
Rental M
Home Im
To Advertise
M.I. CONTRA
BATHTUB &
RESURFA
SALE
ONLY $5,995
KraftMaid Cabinetry
Authorized Dealer
DIRECT TO YOUR HOME
Centurion Construction Inc.
Specializing in Siding & All Exterior Work
Ugly Tub & Tile Embarrassing You?
TUBS AND TILES REGLAZED
10 Year Guarantee
GOOD JOB! You're Using The Classifieds.
#1 MOVIE IN AMERICA!
IMAX
BEST PICTURE OF THE YEAR
TOP TEN LISTS
THE DARK KNIGHT

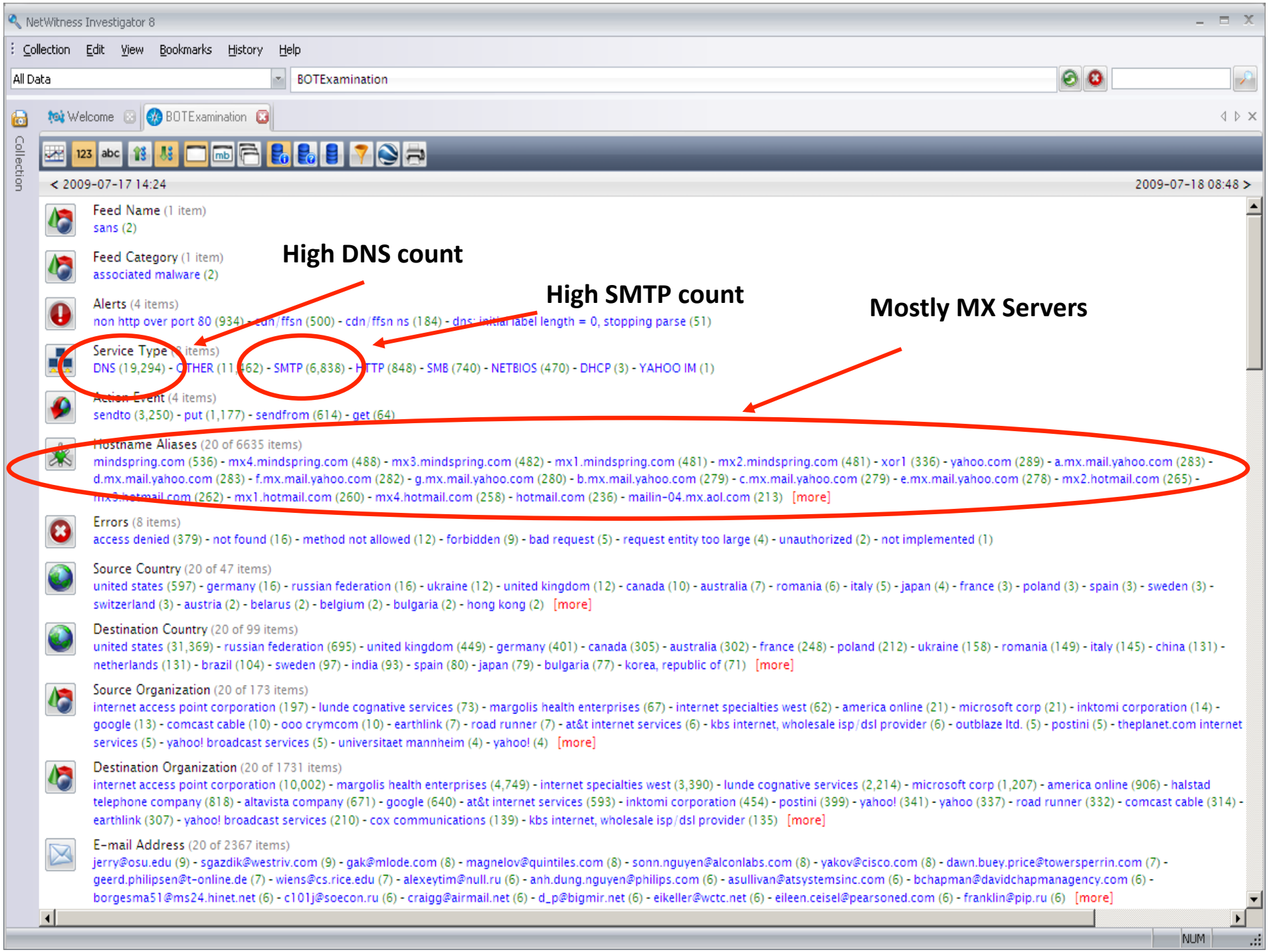
The Money Keeps Rolling…

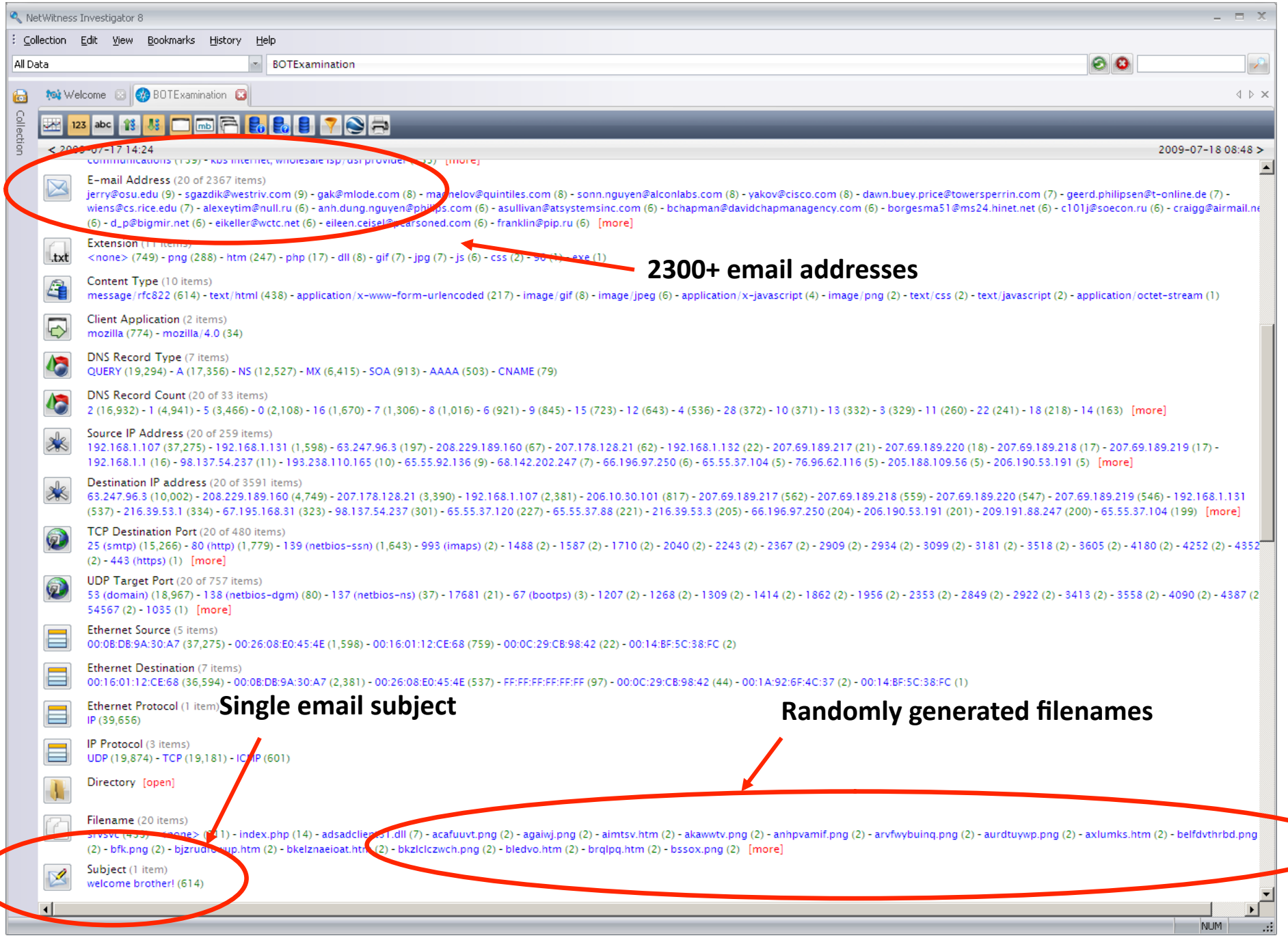
Your Network, viewed by criminals and others…

vs.

You having your act together regarding advanced threats…

Which of These Sucks Less?


NetWitness Investigator 8
Collection Edit View Bookmarks History Help
All Data
BOTExamination
Welcome
BOTExamination
Collection
< 2009-07-17 14:24
2009-07-18 08:48 >
Feed Name (1 item)
sans (2)
Feed Category (1 item)
associated malware (2)
Alerts (4 items)
non http over port 80 (934) - cdn/ffsn (500) - cdn/ffsn ns (184) - dns: initial label length = 0, stopping parse (51)
Service Type (8 items)
DNS (19,294) - OTHER (11,462) - SMTP (6,838) - HTTP (848) - SMB (740) - NETBIOS (470) - DHCP (3) - YAHOO IM (1)
Action Event (4 items)
sendto (3,250) - put (1,177) - sendfrom (614) - get (64)
Hostname Aliases (20 of 6635 items)
mindspring.com (536) - mx4.mindspring.com (488) - mx3.mindspring.com (482) - mx1.mindspring.com (481) - mx2.mindspring.com (481) - xor1 (336) - yahoo.com (289) - a.mx.mail.yahoo.com (283) - d.mx.mail.yahoo.com (283) - f.mx.mail.yahoo.com (282) - g.mx.mail.yahoo.com (280) - b.mx.mail.yahoo.com (279) - c.mx.mail.yahoo.com (279) - e.mx.mail.yahoo.com (278) - mx2.hotmail.com (265) - mx3.hotmail.com (262) - mx1.hotmail.com (260) - mx4.hotmail.com (258) - hotmail.com (236) - mailin-04.mx.aol.com (213) [more]
Errors (8 items)
access denied (379) - not found (16) - method not allowed (12) - forbidden (9) - bad request (5) - request entity too large (4) - unauthorized (2) - not implemented (1)
Source Country (20 of 47 items)
united states (597) - germany (16) - russian federation (16) - ukraine (12) - united kingdom (12) - canada (10) - australia (7) - romania (6) - italy (5) - japan (4) - france (3) - poland (3) - spain (3) - sweden (3) - switzerland (3) - austria (2) - belarus (2) - belgium (2) - bulgaria (2) - hong kong (2) [more]
Destination Country (20 of 99 items)
united states (31,369) - russian federation (695) - united kingdom (449) - germany (401) - canada (305) - australia (302) - france (248) - poland (212) - ukraine (158) - romania (149) - italy (145) - china (131) - netherlands (131) - brazil (104) - sweden (97) - india (93) - spain (80) - japan (79) - bulgaria (77) - korea, republic of (71) [more]
Source Organization (20 of 173 items)
internet access point corporation (197) - lunde cognative services (73) - margolis health enterprises (67) - internet specialties west (62) - america online (21) - microsoft corp (21) - inktomi corporation (14) - google (13) - comcast cable (10) - ooo crymcom (10) - earthlink (7) - road runner (7) - at&t internet services (6) - kbs internet, wholesale isp/dsl provider (6) - outblaze ltd. (5) - postini (5) - theplanet.com internet services (5) - yahoo! broadcast services (5) - universitaet mannheim (4) - yahoo! (4) [more]
Destination Organization (20 of 1731 items)
internet access point corporation (10,002) - margolis health enterprises (4,749) - internet specialties west (3,390) - lunde cognative services (2,214) - microsoft corp (1,207) - america online (906) - halstad telephone company (818) - altavista company (671) - google (640) - at&t internet services (593) - inktomi corporation (454) - postini (399) - yahoo! (341) - yahoo (337) - road runner (332) - comcast cable (314) - earthlink (307) - yahoo! broadcast services (210) - cox communications (139) - kbs internet, wholesale isp/dsl provider (135) [more]
E-mail Address (20 of 2367 items)
jerry@osu.edu (9) - sgazdik@westriv.com (9) - gak@mlode.com (8) - magnelov@quintiles.com (8) - sonn.nguyen@alconlabs.com (8) - yakov@cisco.com (8) - dawn.buey.price@towersperrin.com (7) - geerd.philipsen@t-online.de (7) - wiens@cs.rice.edu (7) - alexeytim@null.ru (6) - anh.dung.nguyen@philips.com (6) - asullivan@atsystemsinc.com (6) - bchapman@davidchapmanagency.com (6) - borgesma51@ms24.hinet.net (6) - c101j@soecon.ru (6) - craigg@airmail.net (6) - d_p@bigmir.net (6) - eikeller@wctc.net (6) - eileen.ceisel@pearsoned.com (6) - franklin@pip.ru (6) [more]
NUM
High DNS count
High SMTP count
Mostly MX Servers


NetWitness Investigator 8
Collection Edit View Bookmarks History Help
All Data
BOTExamination
Welcome
BOTExamination
2009-07-17 14:24
2009-07-18 08:48
E-mail Address (20 of 2367 items)
jerry@osu.edu (9) - sgazdik@westriv.com (9) - gak@mlode.com (8) - mac
nelov@quintiles.com (8) - sonn.nguyen@alconlabs.com (8) - yakov@cisco.com (8) - dawn.buey.price@towersperrin.com (7) - geerd.philipsen@t-online.de (7) -
wiens@cs.rice.edu (7) - alexeytim@null.ru (6) - anh.dung.nguyen@philips.com (6) - asullivan@atsystemsinc.com (6) - bchapman@davidchapmanagency.com (6) - borgesma51@ms24.hinet.net (6) - c101j@soecon.ru (6) - craigg@airmail.ne
(6) - d_p@bigmir.net (6) - eikeller@wctc.net (6) - eileen.ceisel@pearsoned.com (6) - franklin@pip.ru (6) [more]
Extension
<none> (749) - png (288) - htm (247) - php (17) - dll (8) - gif (7) - jpg (7) - js (6) - css (2) - exe (1)
2300+ email addresses
Content Type (10 items)
message/rfc822 (614) - text/html (438) - application/x-www-form-urlencoded (217) - image/gif (8) - image/jpeg (6) - application/x-javascript (4) - image/png (2) - text/css (2) - text/javascript (2) - application/octet-stream (1)
Client Application (2 items)
mozilla (774) - mozilla/4.0 (34)
DNS Record Type (7 items)
QUERY (19,294) - A (17,356) - NS (12,527) - MX (6,415) - SOA (913) - AAAA (503) - CNAME (79)
DNS Record Count (20 of 33 items)
2 (16,932) - 1 (4,941) - 5 (3,466) - 0 (2,108) - 16 (1,670) - 7 (1,306) - 8 (1,016) - 6 (921) - 9 (845) - 15 (723) - 12 (643) - 4 (536) - 28 (372) - 10 (371) - 13 (332) - 3 (329) - 11 (260) - 22 (241) - 18 (218) - 14 (163) [more]
Source IP Address (20 of 259 items)
192.168.1.107 (37,275) - 192.168.1.131 (1,598) - 63.247.96.3 (197) - 208.229.189.160 (67) - 207.178.128.21 (62) - 192.168.1.132 (22) - 207.69.189.217 (21) - 207.69.189.220 (18) - 207.69.189.218 (17) - 207.69.189.219 (17) -
192.168.1.1 (16) - 98.137.54.237 (11) - 193.238.110.165 (10) - 65.55.92.136 (9) - 68.142.202.247 (7) - 66.196.97.250 (6) - 65.55.37.104 (5) - 76.96.62.116 (5) - 205.188.109.56 (5) - 206.190.53.191 (5) [more]
Destination IP address (20 of 3591 items)
63.247.96.3 (10,002) - 208.229.189.160 (4,749) - 207.178.128.21 (3,390) - 192.168.1.107 (2,381) - 206.10.30.101 (817) - 207.69.189.217 (562) - 207.69.189.218 (559) - 207.69.189.220 (547) - 207.69.189.219 (546) - 192.168.1.131
(537) - 216.39.53.1 (334) - 67.195.168.31 (323) - 98.137.54.237 (301) - 65.55.37.120 (227) - 65.55.37.88 (221) - 216.39.53.3 (205) - 66.196.97.250 (204) - 206.190.53.191 (201) - 209.191.88.247 (200) - 65.55.37.104 (199) [more]
TCP Destination Port (20 of 480 items)
25 (smtp) (15,266) - 80 (http) (1,779) - 139 (netbios-ssn) (1,643) - 993 (imaps) (2) - 1488 (2) - 1587 (2) - 1710 (2) - 2040 (2) - 2243 (2) - 2367 (2) - 2909 (2) - 2934 (2) - 3099 (2) - 3181 (2) - 3518 (2) - 3605 (2) - 4180 (2) - 4252 (2) - 4352
(2) - 443 (https) (1) [more]
UDP Target Port (20 of 757 items)
53 (domain) (18,967) - 138 (netbios-dgm) (80) - 137 (netbios-ns) (37) - 17681 (21) - 67 (bootps) (3) - 1207 (2) - 1268 (2) - 1309 (2) - 1414 (2) - 1862 (2) - 1956 (2) - 2353 (2) - 2849 (2) - 2922 (2) - 3413 (2) - 3558 (2) - 4090 (2) - 4387 (2
54567 (2) - 1035 (1) [more]
Ethernet Source (5 items)
00:0B:DB:9A:30:A7 (37,275) - 00:26:08:E0:45:4E (1,598) - 00:16:01:12:CE:68 (759) - 00:0C:29:CB:98:42 (22) - 00:14:BF:5C:38:FC (2)
Ethernet Destination (7 items)
00:16:01:12:CE:68 (36,594) - 00:0B:DB:9A:30:A7 (2,381) - 00:26:08:E0:45:4E (537) - FF:FF:FF:FF:FF:FF (97) - 00:0C:29:CB:98:42 (44) - 00:1A:92:6F:4C:37 (2) - 00:14:BF:5C:38:FC (1)
Ethernet Protocol (1 item)
IP (39,656)
Single email subject
Randomly generated filenames
IP Protocol (3 items)
UDP (19,874) - TCP (19,181) - ICMP (601)
Directory [open]
Filename (20 items)
index.php (14) - adsadclient31.dll (7) - acafuuvt.png (2) - agaiwj.png (2) - aimtsv.htm (2) - akawwtv.png (2) - anhpvamif.png (2) - arvfwybuinq.png (2) - aurdtuywp.png (2) - axlumks.htm (2) - belfdvthrbd.png
(2) - bfk.png (2) - bkelznaeioat.htm (2) - bkzlclczwch.png (2) - bledvo.htm (2) - brqlpq.htm (2) - bssox.png (2) [more]
Subject (1 item)
welcome brother! (614)
NUM

NetWitness Reconstruction for session ID: 4382 (Source 192.168.1.107 : 1463, Target 64.18.4.14
Time 7/18/2009 7:22:11 to 7/18/2009 7:22:14 Size 1,031 bytes Protocol 2048/6/25

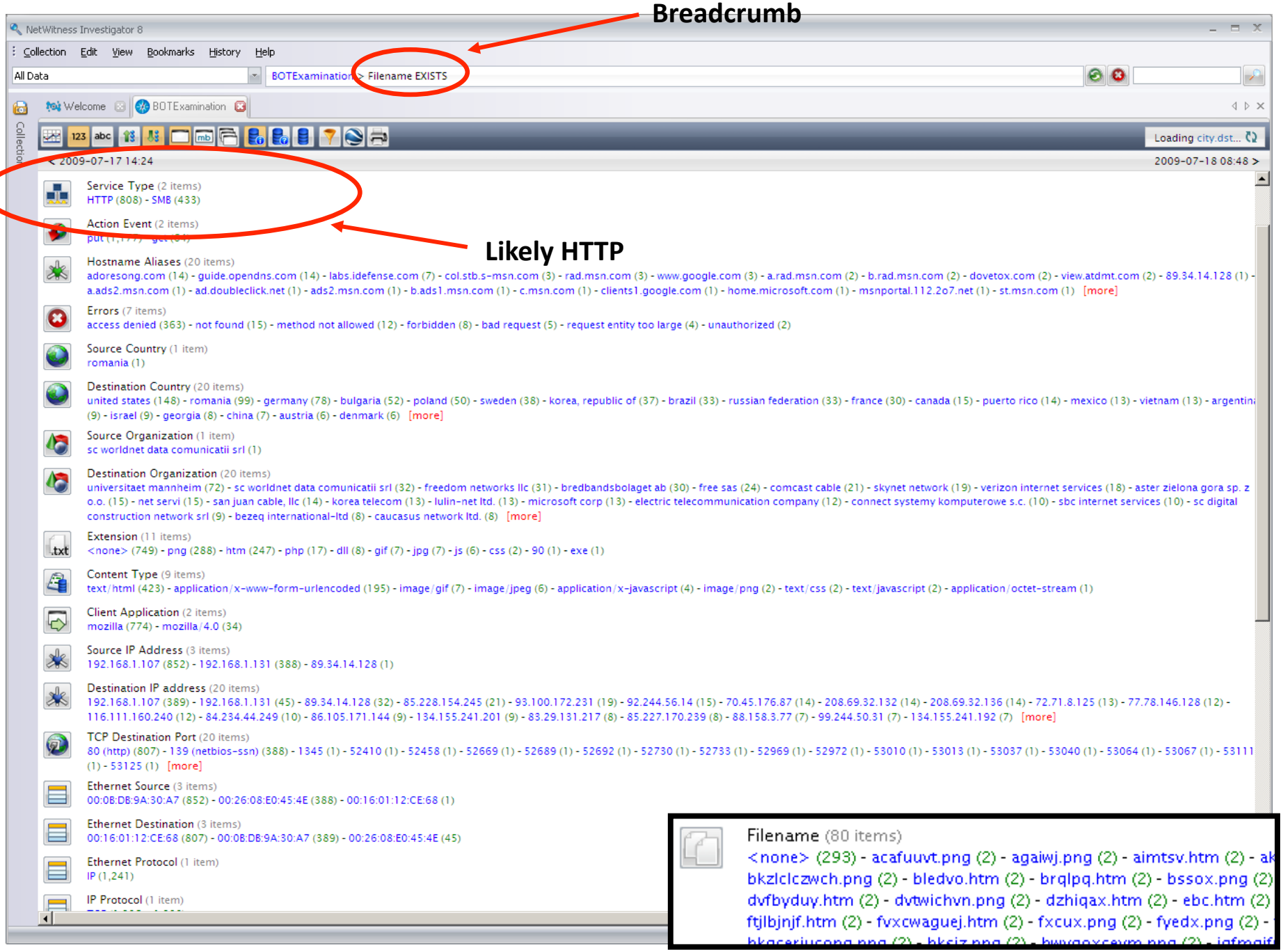
From: "Dennis Dillard" <magnelov@quintiles.com>
To: <sgazdik@westriv.com>
Subject: Welcome brother!
Date: Sat, 18 Jul 2009 07:21:24 -0500
more

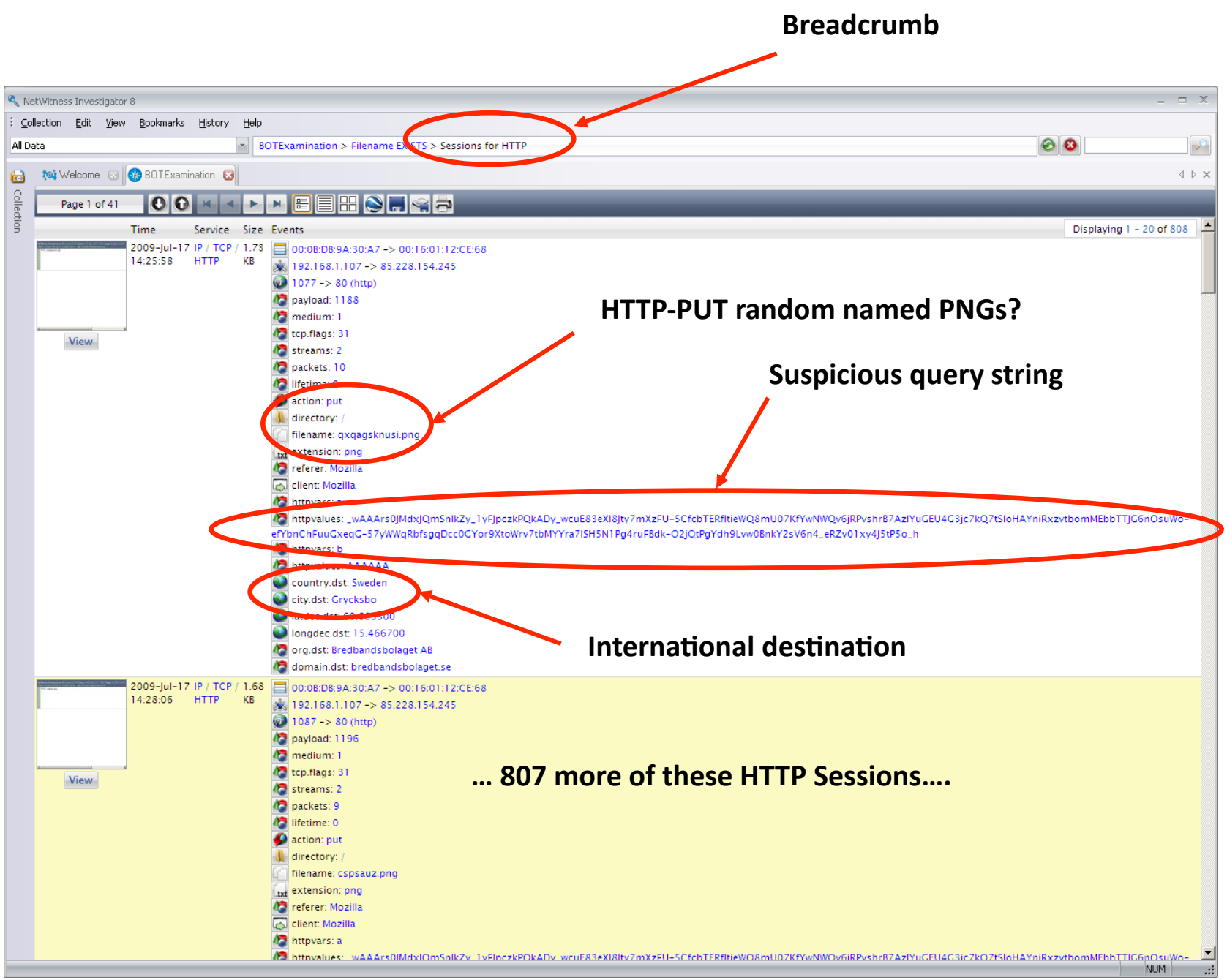
Greetings brother!

The White Nationalism community would like to Welcome you
to our new Whites-only web forum.

Here we discuss ways to deal with the jewish menace
and the mud people invasion.

Click the link below to visit our site:
http://f2bbs.com/


Breadcrumb
NetWitness Investigator 8
Collection Edit View Bookmarks History Help
All Data
BOTExamination > Filename EXISTS
Welcome
BOTExamination
Loading city.dst...
< 2009-07-17 14:24
2009-07-18 08:48 >
Likely HTTP
Service Type (2 items)
HTTP (808) - SMB (433)
Action Event (2 items)
Hostname Aliases (20 items)
adoresong.com (14) - guide.opendns.com (14) - labs.idefense.com (7) - col.stb.s-msn.com (3) - rad.msn.com (3) - www.google.com (3) - a.rad.msn.com (2) - b.rad.msn.com (2) - dovetox.com (2) - view.atdmt.com (2) - 89.34.14.128 (1) - a.ads2.msn.com (1) - ad.doubleclick.net (1) - ads2.msn.com (1) - b.ads1.msn.com (1) - c.msn.com (1) - clients1.google.com (1) - home.microsoft.com (1) - msnportal.112.2o7.net (1) - st.msn.com (1) [more]
Errors (7 items)
access denied (363) - not found (15) - method not allowed (12) - forbidden (8) - bad request (5) - request entity too large (4) - unauthorized (2)
Source Country (1 item)
romania (1)
Destination Country (20 items)
united states (148) - romania (99) - germany (78) - bulgaria (52) - poland (50) - sweden (38) - korea, republic of (37) - brazil (33) - russian federation (33) - france (30) - canada (15) - puerto rico (14) - mexico (13) - vietnam (13) - argentina (9) - israel (9) - georgia (8) - china (7) - austria (6) - denmark (6) [more]
Source Organization (1 item)
sc worldnet data comunicatii srl (1)
Destination Organization (20 items)
universitaet mannheim (72) - sc worldnet data comunicatii srl (32) - freedom networks llc (31) - bredbandsbolaget ab (30) - free sas (24) - comcast cable (21) - skynet network (19) - verizon internet services (18) - aster zielona gora sp. z o.o. (15) - net servi (15) - san juan cable, llc (14) - korea telecom (13) - lulin-net ltd. (13) - microsoft corp (13) - electric telecommunication company (12) - connect systemy komputerowe s.c. (10) - sbc internet services (10) - sc digital construction network srl (9) - bezeq international-ltd (8) - caucasus network ltd. (8) [more]
Extension (11 items)
<none> (749) - png (288) - htm (247) - php (17) - dll (8) - gif (7) - jpg (7) - js (6) - css (2) - 90 (1) - exe (1)
Content Type (9 items)
text/html (423) - application/x-www-form-urlencoded (195) - image/gif (7) - image/jpeg (6) - application/x-javascript (4) - image/png (2) - text/css (2) - text/javascript (2) - application/octet-stream (1)
Client Application (2 items)
mozilla (774) - mozilla/4.0 (34)
Source IP Address (3 items)
192.168.1.107 (852) - 192.168.1.131 (388) - 89.34.14.128 (1)
Destination IP address (20 items)
192.168.1.107 (389) - 192.168.1.131 (45) - 89.34.14.128 (32) - 85.228.154.245 (21) - 93.100.172.231 (19) - 92.244.56.14 (15) - 70.45.176.87 (14) - 208.69.32.132 (14) - 208.69.32.136 (14) - 72.71.8.125 (13) - 77.78.146.128 (12) - 116.111.160.240 (12) - 84.234.44.249 (10) - 86.105.171.144 (9) - 134.155.241.201 (9) - 83.29.131.217 (8) - 85.227.170.239 (8) - 88.158.3.77 (7) - 99.244.50.31 (7) - 134.155.241.192 (7) [more]
TCP Destination Port (20 items)
80 (http) (807) - 139 (netbios-ssn) (388) - 1345 (1) - 52410 (1) - 52458 (1) - 52669 (1) - 52689 (1) - 52692 (1) - 52730 (1) - 52733 (1) - 52969 (1) - 52972 (1) - 53010 (1) - 53013 (1) - 53037 (1) - 53040 (1) - 53064 (1) - 53067 (1) - 53111 (1) - 53125 (1) [more]
Ethernet Source (3 items)
00:0B:DB:9A:30:A7 (852) - 00:26:08:E0:45:4E (388) - 00:16:01:12:CE:68 (1)
Ethernet Destination (3 items)
00:16:01:12:CE:68 (807) - 00:0B:DB:9A:30:A7 (389) - 00:26:08:E0:45:4E (45)
Ethernet Protocol (1 item)
IP (1,241)
IP Protocol (1 item)
Filename (80 items)
<none> (293) - acafuuvt.png (2) - agaiwj.png (2) - aimtsv.htm (2) - ak
bkzlclczwch.png (2) - bledvo.htm (2) - brqlpq.htm (2) - bssox.png (2)
dvfbyduy.htm (2) - dvtwichvn.png (2) - dzhiqax.htm (2) - ebc.htm (2)
ftjlbjnjf.htm (2) - fvxcwaguej.htm (2) - fxcux.png (2) - fyedx.png (2) -

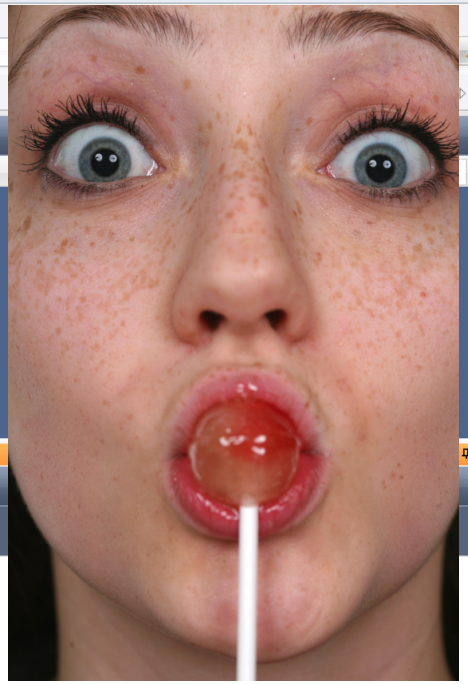

Breadcrumb
NetWitness Investigator 8
Collection Edit View Bookmarks History Help
All Data
BOTExamination > Filename EXISTS > Sessions for HTTP
Welcome
BOTExamination
Page 1 of 41
Displaying 1 - 20 of 808
Time Service Size Events
2009-Jul-17 14:25:58 IP / TCP / HTTP 1.73 KB
View
00:0B:DB:9A:30:A7 -> 00:16:01:12:CE:68
192.168.1.107 -> 85.228.154.245
1077 -> 80 (http)
payload: 1188
medium: 1
tcp.flags: 31
streams: 2
packets: 10
action: put
directory: /
filename: qxqagsknusi.png
extension: png
referer: Mozilla
client: Mozilla
httpvalues: _wAAArs0JMdxJQmSnlkZy_1yFJpczkPQkADy_wcuE83eXI8Jty7mXzFU-5CfcbTERfltieWQ8mU07KfYwNWQv6jRPvshrB7AzlYuGEU4G3jc7kQ7tSloHAYniRxzvtbomMEbbTTJG6nOsuWo-efYbnChFuuGxeqG-57yWWqRbfsgqDcc0GYor9XtoWrv7tbMYYra7ISH5N1Pg4ruFBdk-O2jQtPgYdh9Lvw0BnkY2sV6n4_eRZv01xy4J5tP5o_h
httpvars: b
country.dst: Sweden
city.dst: Grycksbo
longdec.dst: 15.466700
org.dst: Bredbandsbolaget AB
domain.dst: bredbandsbolaget.se
HTTP-PUT random named PNGs?
Suspicious query string
International destination
2009-Jul-17 14:28:06 IP / TCP / HTTP 1.68 KB
View
00:0B:DB:9A:30:A7 -> 00:16:01:12:CE:68
192.168.1.107 -> 85.228.154.245
1087 -> 80 (http)
payload: 1196
medium: 1
tcp.flags: 31
streams: 2
packets: 9
lifetime: 0
action: put
directory: /
filename: cspsauz.png
extension: png
referer: Mozilla
client: Mozilla
httpvars: a
... 807 more of these HTTP Sessions....
NUM

Breadcrumb

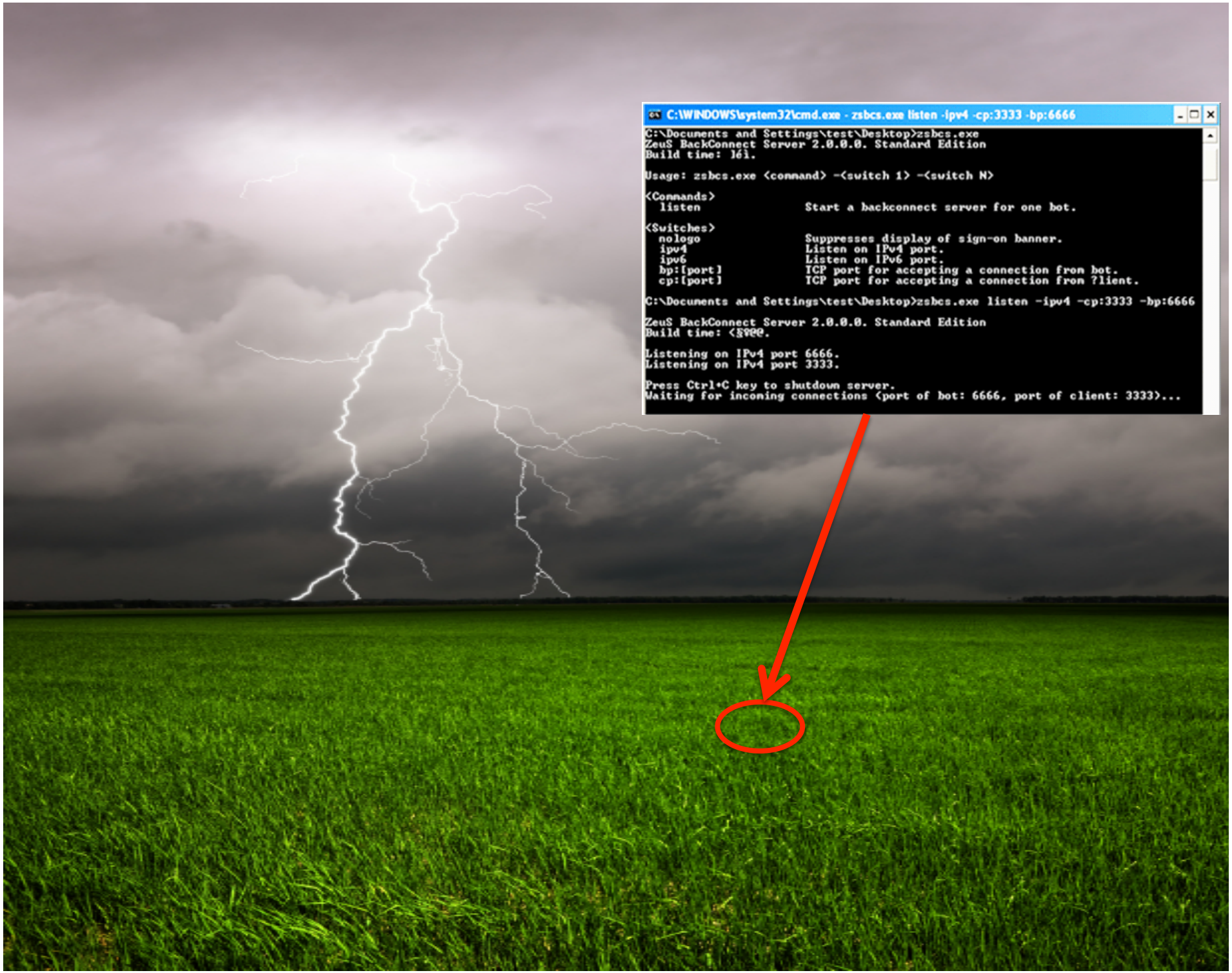
HTTP Put

Encoded/Encrypted content

It didn't suck this time...




Help
Directions
Add Content
and click on
below, to
Examination
Destination
ollection
outes
.168.1.107
60
(OTHER)
60
.168.1.107
22, 7289
(OTHER)
22, 7289
els
s
t
N
© 2009 Tele Atlas
© 2009 LeadDog Consulting
© 2009 Europa Technologies
© 2009 Google
34°40'49.89" N 75°13'48.44" W elev -1512 m
©2009 Google
Eye alt 9127.80 km


C:\WINDOWS\system32\cmd.exe - zsbcs.exe listen -ipv4 -cp:3333 -bp:6666
C:\Documents and Settings\test\Desktop>zsbcs.exe
ZeuS BackConnect Server 2.0.0.0. Standard Edition
Build time: Jéi.
Usage: zsbcs.exe <command> -<switch 1> -<switch N>
<Commands>
listen Start a backconnect server for one bot.
<Switches>
nologo Suppresses display of sign-on banner.
ipv4 Listen on IPv4 port.
ipv6 Listen on IPv6 port.
bp:[port] TCP port for accepting a connection from bot.
cp:[port] TCP port for accepting a connection from ?lient.
C:\Documents and Settings\test\Desktop>zsbcs.exe listen -ipv4 -cp:3333 -bp:6666
ZeuS BackConnect Server 2.0.0.0. Standard Edition
Build time: <§ee.
Listening on IPv4 port 6666.
Listening on IPv4 port 3333.
Press Ctrl+C key to shutdown server.
Waiting for inconing connections (port of bot: 6666, port of client: 3333)...

Subject: DPRK has carried out nuclear missile attack on Japan

Office of the Director of National Intelligence
INTELLIGENCE BULLETIN
UNCLASSIFIED//FOR OFFICIAL USE ONLY

(U//FOUO) DPRK has carried out nuclear missile attack on Japan

05 March 2010

(U//FOUO) Prepared by Defense Intelligence Agency

(U//FOUO) Today, March 05, 2010 at 01.41 AM local time (UTC/GMT -5 hours), US seismographic stations recorded seismic activity in the area of Okinawa Island (Japan). According to National Geospatial-Intelligence Agency, Democratic People's Republic of Korea has carried out an average range missile attack with use of nuclear warhead. The explosion caused severe destructions in the northern part of the Okinawa island. Casualties among the personnel of the US military base are being estimated at the moment.

(U//FOUO) In connection with the occurred events, it is necessary for the personnel of the services listed below to be ready for immediate mobilization:

CENTRAL INTELLIGENCE AGENCY
Phone: (703) 482-0623

DEFENSE INTELLIGENCE AGENCY
Phone: (202) 231-8601
Email: DIA-PAO@dia.mil

DEPARTMENT OF ENERGY:
OFFICE OF INTELLIGENCE AND COUNTERINTELLIGENCE
Phone: 1-202-586-5000
Email: The.Secretary@hq.doe.gov

DEPARTMENT OF HOMELAND SECURITY:
OFFICE OF INTELLIGENCE AND ANALYSIS
Phone: (202) 282-8000

DEPARTMENT OF STATE:
BUREAU OF INTELLIGENCE AND RESEARCH
Phone: (202) 647-4000

DEPARTMENT OF THE TREASURY:
OFFICE OF INTELLIGENCE AND ANALYSIS
Phone: (202) 622-2000

DRUG ENFORCEMENT ADMINISTRATION:
OFFICE OF NATIONAL SECURITY INTELLIGENCE
Phone: (202) 307-1000

FEDERAL BUREAU OF INVESTIGATION
NATIONAL SECURITY BRANCH
Phone: (202) 324-3000

NATIONAL GEOSPATIAL-INTELLIGENCE AGENCY
Phone: (703) 755-5900

NATIONAL RECONNAISSANCE OFFICE
Phone: (703) 808-1198

NATIONAL SECURITY AGENCY
Phone: 1-800-688-6115
Email: NIASC@nsa.gov

UNITED STATES AIR FORCE
Phone: (251) 441-6215/6211

UNITED STATES ARMY
Phone: 1-888-550-2769

UNITED STATES COAST GUARD
Phone: (202) 372-2100

UNITED STATES MARINE CORPS
Phone: (202) 372-4411

UNITED STATES NAVY
Phone: (202) 372-2020

(U//FOUO) Additional information can be found in the following report:

http://dnicenter.com/docs/report.zip

Office of the Director of National Intelligence
Washington, D.C. 20511

File **report.exe** received on **2010.03.05 14:01:07 (UTC)**
Current status: **finished**
Result: **1/42 (2.38%)**

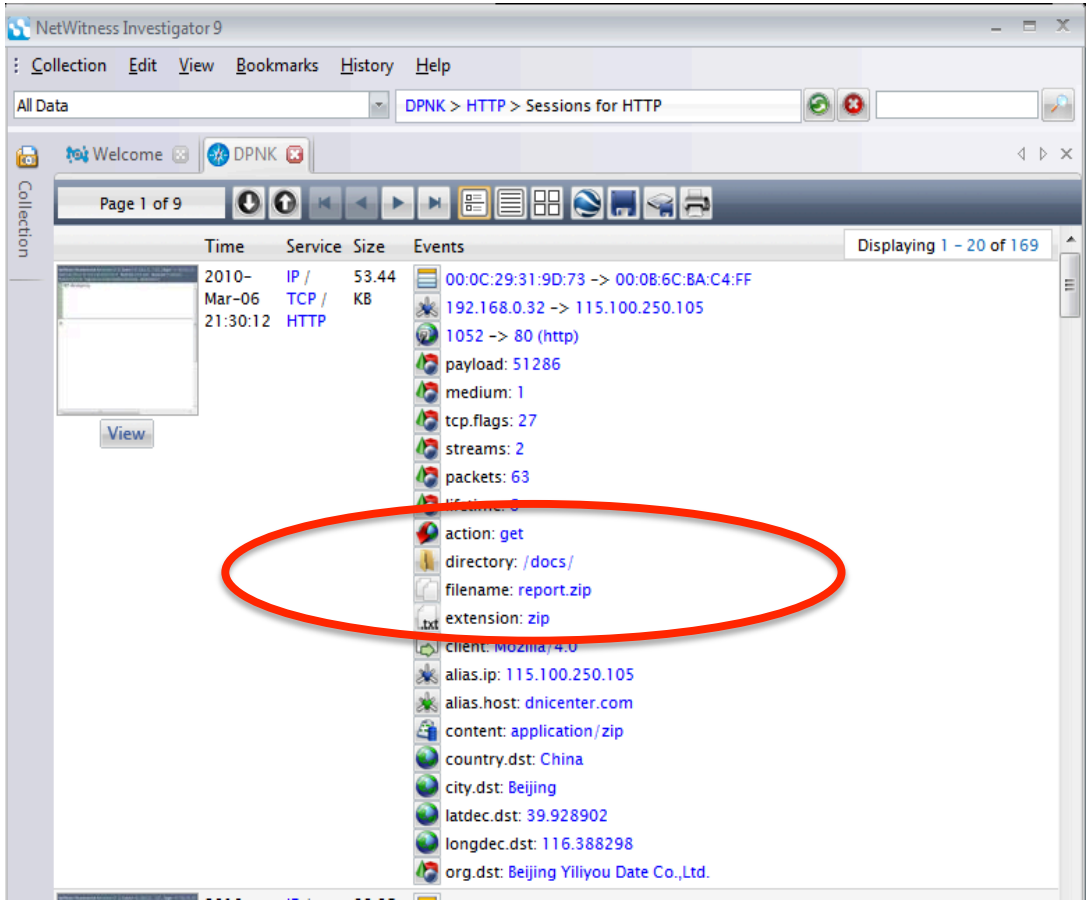
Compact | Print results

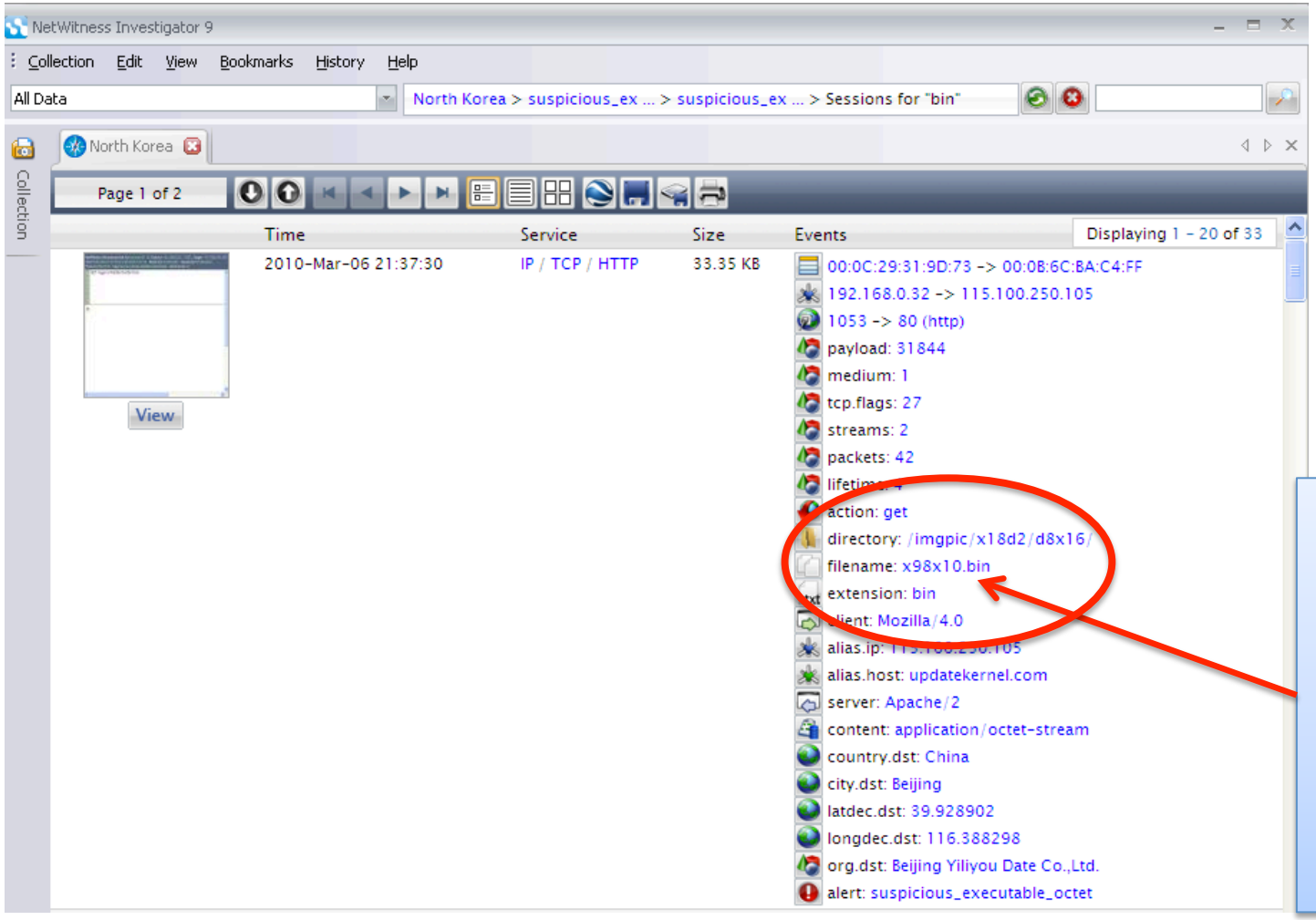
Antivirus	Version	Last Update	Result
a-squared	4.5.0.50	2010.03.05	-
AhnLab-V3	5.0.0.2	2010.03.05	-
AntiVir	8.2.1.180	2010.03.05	-
Antiy-AVL	2.0.3.7	2010.03.05	-
Authentium	5.2.0.5	2010.03.05	-
Avast	4.8.1351.0	2010.03.05	-
Avast5	5.0.332.0	2010.03.05	-
AVG	9.0.0.730	2010.03.05	-
BitDefender	7.2	2010.03.05	-
CAT-QuickHeal	10.00	2010.03.05	-
ClamAV	0.96.0.0-git	2010.03.05	-
Comodo	4091	2010.02.28	-
DrWeb	5.0.1.12222	2010.03.05	-
eSafe	7.0.17.0	2010.03.04	-
eTrust-Vet	35.2.7341	2010.03.05	-
F-Prot	4.5.1.85	2010.03.04	-
F-Secure	9.0.15370.0	2010.03.05	-
Fortinet	4.0.14.0	2010.03.04	-
GData	19	2010.03.05	-
Ikarus	T3.1.1.80.0	2010.03.05	-
Jiangmin	13.0.900	2010.03.05	-
K7AntiVirus	7.10.990	2010.03.04	-
Kaspersky	7.0.0.125	2010.03.05	-

Which AV Product Sucks the BEST!!! ?

```
# Copyright (c) 1993-1999 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#      102.54.94.97     rhino.acme.com          # source server
#       38.25.63.10     x.acme.com              # x client host

127.0.0.1       localhost
127.0.0.1 downloads-eu1.kaspersky-labs.com
127.0.0.1 downloads2.kaspersky-labs.com
127.0.0.1 downloads4.kaspersky-labs.com
127.0.0.1 downloads1.kaspersky-labs.com
127.0.0.1 downloads-us1.kaspersky-labs.com
127.0.0.1 rads.mcafee.com
127.0.0.1 liveupdate.symanteclive update.com
127.0.0.1 liveupdate.symantec.com
127.0.0.1 liveupdate.symantec.d4p.net
127.0.0.1 update.symantec.com
127.0.0.1 download7.avast.com
127.0.0.1 download6.avast.com
127.0.0.1 download5.avast.com
127.0.0.1 download4.avast.com
127.0.0.1 download3.avast.com
127.0.0.1 download2.avast.com
127.0.0.1 download1.avast.com
127.0.0.1 avu.zonelabs.com
127.0.0.1 retail.sp.f-secure.com
127.0.0.1 retail01.sp.f-secure.com
127.0.0.1 retail02.sp.f-secure.com
127.0.0.1 acs.pandasoftware.com
127.0.0.1 pccreg.antivirus.com
127.0.0.1 dl1.antivir.de
127.0.0.1 dl2.antivir.de
127.0.0.1 dl3.antivir.de
127.0.0.1 dl4.antivir.de
127.0.0.1 fr.mcafee.com
127.0.0.1 mcafee.com
127.0.0.1 antivirus.cai.com
127.0.0.1 ftp.esafe.com
127.0.0.1 ftp.europe.f-secure.com
127.0.0.1 ftp.symantec.com
127.0.0.1 us.mcafee.com
127.0.0.1 security.symantec.com
127.0.0.1 download.mcafee.com
127.0.0.1 shop.symantec.com
127.0.0.1 dispatch.mcafee.com
127.0.0.1 f-secure.com
127.0.0.1 kaspersky.com
127.0.0.1 mast.mcafee.com
127.0.0.1 secure.nai.com
```





- ZeuS configuration file download
- This type of problem recognition can be automated

ZeuS configs

config	dateadded (UTC)	lastupdated (UTC)	filesize	MD5 hash	file download
updatekernel.com/imgpic/x18d2/d8x16/x98x10.bin	2010-02-07 20:55:12	2010-03-07 15:18:30	31'397	2f6d6c2a306fb0104086745909141087	download

ZeuS binaries

binary	AV detection	dateadded (UTC)	lastupdated (UTC)	filesize	MD5 hash	file download
updatekernel.com/stat/dot/stat.exe	6%	2010-02-13 19:41:52	2010-03-07 15:18:31	900'366	ebb30bb01e25f06d3e0a28ed439a21b3	download

< 2010-03-06 20:24 2010-03-08

User Account (1 item)
mao2 (1)

Password [open]

Service Type (1 item)
FTP (1)

Source IP Address (1 item)
192.168.0.32 (1)

Destination IP address (1 item)
86.57.246.177 (1)

Action Event (2 items)
put (1) - login (1)

Extension (4 items)
xls (1) - pdf (1) - doc (1) - dll (1)

Filename (20 items)
1051a1iowadems.pdf (1) - 780e0e91ccb6cdbf6e_6udymvin7.pdf (1) - _c.dll (1) - _hslib.dll (1) - _users.dll (1) - a8dfc36246b3dcc3cb_iem6bxpgh.pdf (1) - afl-cio-obama.pdf (1) - excel9.xls (1) - jul08b-elec.pdf (1) - katrinafactsheetfinal.pdf (1) - naralpollmemo061608.pdf (1) - obama-full-text-8-28-2008.pdf (1) - obama.pdf (1) - obamablueprintforchange.pdf (1) - pc_08_obama.pdf ppp_penn_release_040208.pdf (1) - senator_obama.pdf (1) - vbatest_word2k.doc (1) - winword8.doc (1) - xplaned_obama_fundraising.pdf (

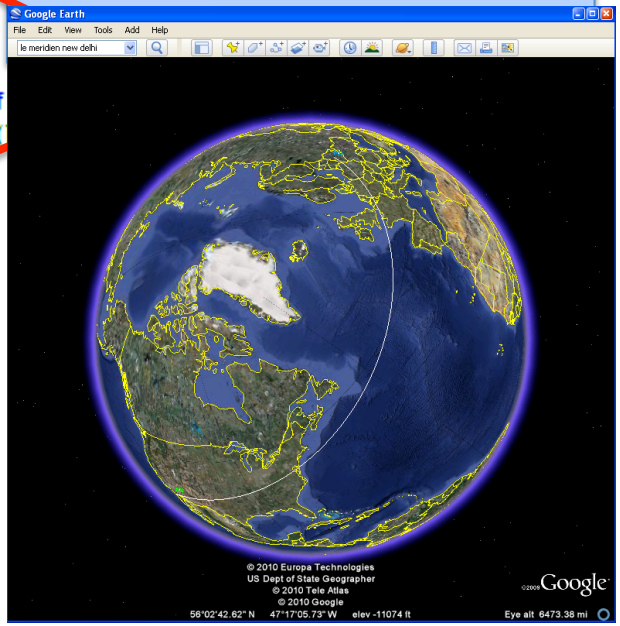
Directory (1 item)
./yzzttbhchrlkkdjf/ (1)

TCP Destination Port (1 item)
21 (ftp) (1)

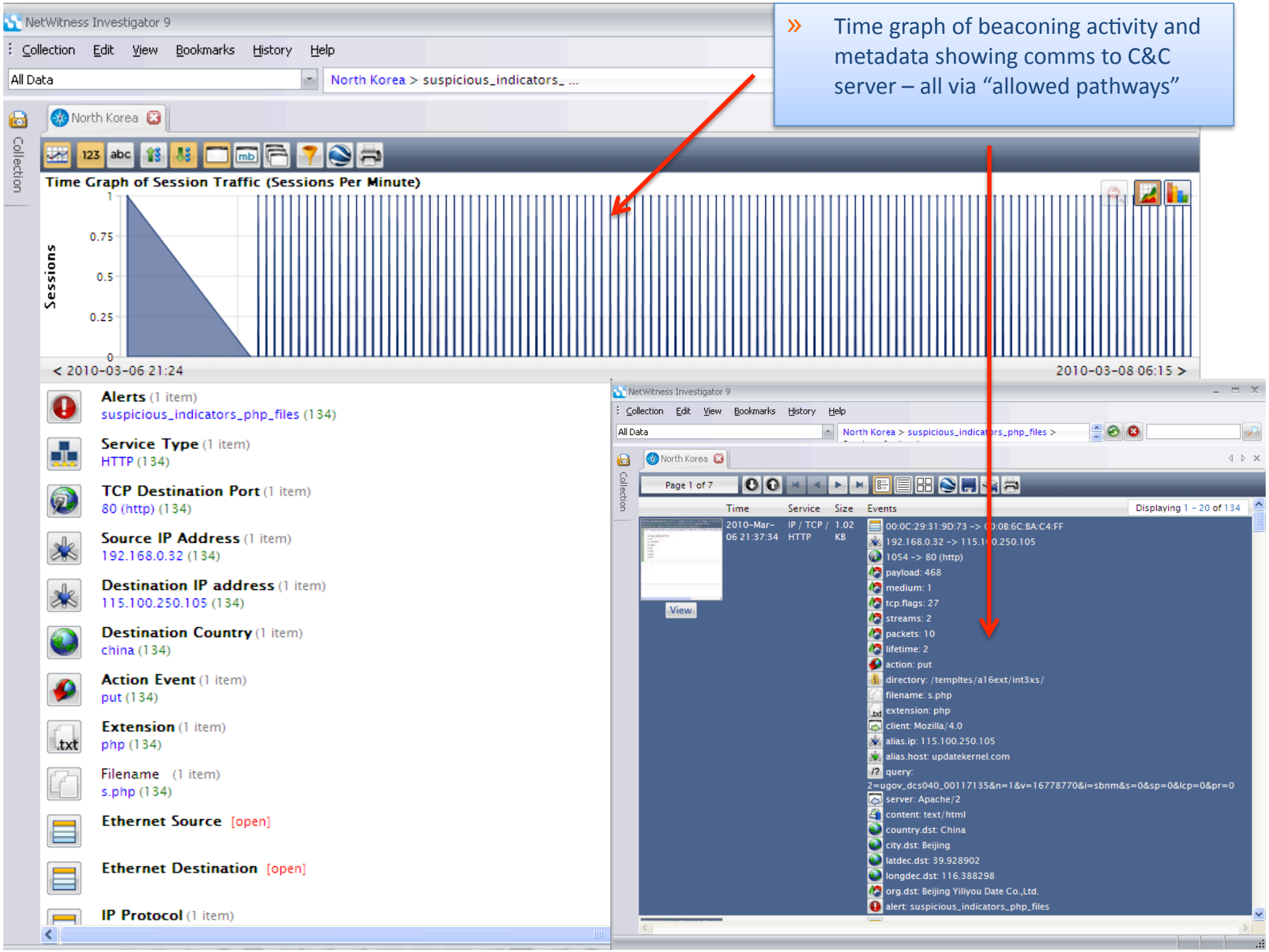
Ethernet Protocol (1 item)
IP (1)

IP Protocol (1 item)
TCP (1)

- Malware stealing files of interest to the drop server in Minsk
- FTP drop server still is resolving to same address
- Early on March 8, 2010, server cleaned out and account disabled
- username: mao2 password: [captured]




```
ls
250 OK. Current directory is /
ftp> ls
227 Entering Passive Mode (86,57,246,177,40,224)
150 Accepted data connection
drwxr-xr-x   16 942      925          4096 Mar  7 15:51 .
drwxr-xr-x   16 942      925          4096 Mar  7 15:51 ..
drwxr-xr-x    2 942      925          4096 Mar  7 09:41 1mKQgNAtcs2SpAx9
drwxr-xr-x    2 942      925          4096 Mar  7 15:14 3LxlXUmDK8ZJNglZ
drwxr-xr-x    2 942      925          4096 Mar  7 08:33 Ci70rpQKSUwoLJIb
drwxr-xr-x    2 942      925          4096 Mar  7 07:59 ELuSOBh9FXvajc87
drwxr-xr-x    2 942      925          4096 Mar  7 08:18 GsR40giKFGLnYruy
drwxr-xr-x    2 942      925          4096 Mar  7 07:38 Jk9zGlldWGrDSvyp
drwxr-xr-x    2 942      925          4096 Mar  7 15:53 MNnPUZYIBqCslKkP
drwxr-xr-x    2 942      925          4096 Mar  7 10:24 VfwG9ZcOE8Fd9Jly
drwxr-xr-x    2 942      925          4096 Mar  7 13:03 hMomRfEWnnCYoWGD
drwxr-xr-x    2 942      925          4096 Mar  7 11:05 mPm4J8knriULLwue
drwxr-xr-x    2 942      925          4096 Mar  7 07:57 qkOtD4Qp7Wd6Ww1w
drwxr-xr-x    2 942      925          4096 Mar  7 07:38 uzs0BPaXU3BiZEQR
drwxr-xr-x    2 942      925          4096 Mar  7 06:59 yzZTtbhcHRlKKdJf
drwxr-xr-x    2 942      925          4096 Mar  7 07:07 z5wyTnAz7CQ9fniY
226-Options: -a -l
226 16 matches total
ftp> cd yzZTtbhcHRlKKdJf
250 OK. Current directory is /yzZTtbhcHRlKKdJf
ftp> ls
227 Entering Passive Mode (86,57,246,177,109,14)
150 Accepted data connection
drwxr-xr-x    2 942      925          4096 Mar  7 06:59 .
drwxr-xr-x   16 942      925          4096 Mar  7 15:51 ..
-rw-r--r--    1 942      925         39904 Mar  7 06:54 1051aIowaDems.pdf
-rw-r--r--    1 942      925         65307 Mar  7 06:54 780e0e91ccb6cdbf6e_6udymvin7.pdf
-rw-r--r--    1 942      925        452141 Mar  7 06:55 AFL-CIO-Obama.pdf
-rw-r--r--    1 942      925         11776 Mar  7 06:55 EXCEL9.XLS
-rw-r--r--    1 942      925         92795 Mar  7 06:55 JUL08B-Elec.pdf
-rw-r--r--    1 942      925         41011 Mar  7 06:55 KatrinaFactSheetFinal.pdf
-rw-r--r--    1 942      925         54895 Mar  7 06:56 Obama.pdf
-rw-r--r--    1 942      925        335765 Mar  7 06:56 ObamaBlueprintForChange.pdf
-rw-r--r--    1 942      925         40639 Mar  7 06:56 PC_08_Obama.pdf
-rw-r--r--    1 942      925         66601 Mar  7 06:56 PPP_Penn_Release_040208.pdf
-rw-r--r--    1 942      925        237882 Mar  7 06:57 Senator_Obama.pdf
-rw-r--r--    1 942      925         97792 Mar  7 06:57 VBATest_Word2K.doc
-rw-r--r--    1 942      925         10752 Mar  7 06:57 WINWORD8.DOC
-rw-r--r--    1 942      925       1066858 Mar  7 06:59 XPLANED_Obama_Fundraising.pdf
-rw-r--r--    1 942      925           828 Mar  7 06:59 _C.dll
-rw-r--r--    1 942      925            16 Mar  7 06:59 _hslib.dll
-rw-r--r--    1 942      925            80 Mar  7 06:59 _users.dll
-rw-r--r--    1 942      925        124409 Mar  7 06:54 a8dfc36246b3dcc3cb_iem6bxpgh.pdf
-rw-r--r--    1 942      925         43583 Mar  7 06:55 naralpollmemo061608.pdf
-rw-r--r--    1 942      925         57402 Mar  7 06:56 obama-full-text-8-28-2008.pdf
226-Options: -a -l
226 22 matches total
ftp>
```


» Time graph of beaconing activity and metadata showing comms to C&C server – all via “allowed pathways”
NetWitness Investigator 9
Collection Edit View Bookmarks History Help
All Data
North Korea > suspicious_indicators_ ...
North Korea
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 >
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
Page 1 of 7
Displaying 1 - 20 of 134
Time Service Size Events
2010-Mar-06 21:37:34 IP / TCP / HTTP 1.02 KB
View
00:0C:29:31:9D:73 ->
192.168.0.32 ->
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:
2=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 Yiliyou Date Co.,Ltd.
alert: suspicious_indicators_php_files

Eddie's Incident Telemetry Suck-O-Meter™

Sucks Most

Sucks Least

Data Source	Description
Firewalls, Gateways, etc.	Overwhelming amounts of data with little context, but can be valuable when used within a SEIM and in conjunction with full packet capture and network forensics reviews.
IDS and AV	Sometimes the first indicator of a problem, for known exploits. Can produce false positives and is signature based.
NetFlow	Network performance management and network behavioral anomaly detection (NBAD) tools. Indicators of changes in traffic flows within a given time slice.
DLP	Data leakage protection based on defined data types and security policies. Limited to specific protocols and contexts.
SEIM	Correlates IDS and other network and security event data and dramatically improves signal to noise ratio. Is valuable to the extent that data sources have useful information and are properly integrated.
Real-time Network Forensics	Collects the richest network data. Provides a deeper level of advanced threat identification and analysis and traffic reconstruction.

Security Doesn't Have To Suck…

But If It Does, Make It Count

Q&A
Thanks for your time…

- eddie@netwitness.com
- http://download.netwitness.com
- Twitter: @eddieschwartz
- Blog: http://www.networkforensics.com