Targeted Attacks: Analysis and Investigation

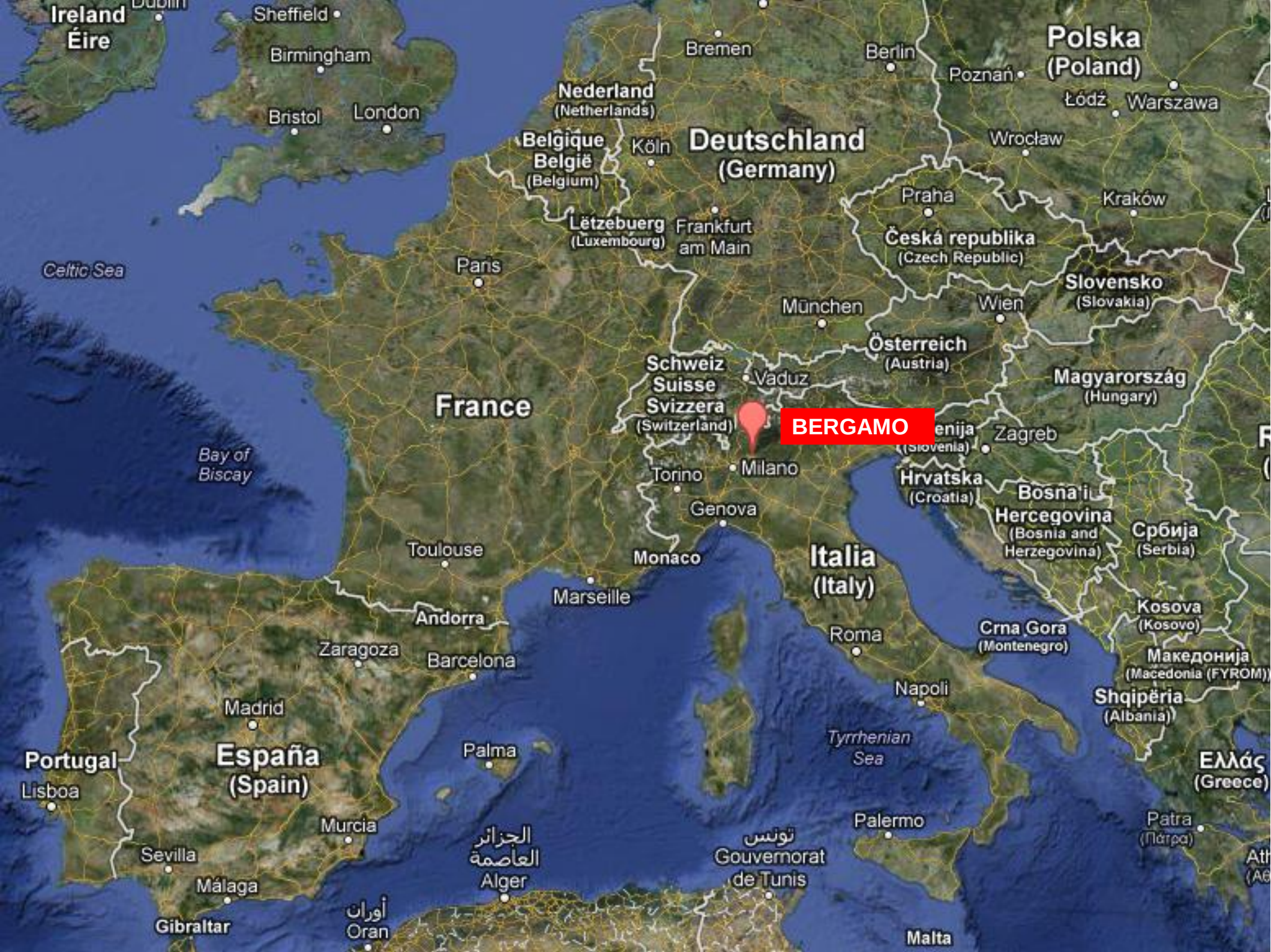
Building Trust in the Information Age

Summer School on Computer Security & Privacy
16th of September 2014
Dr. Marco Balduzzi

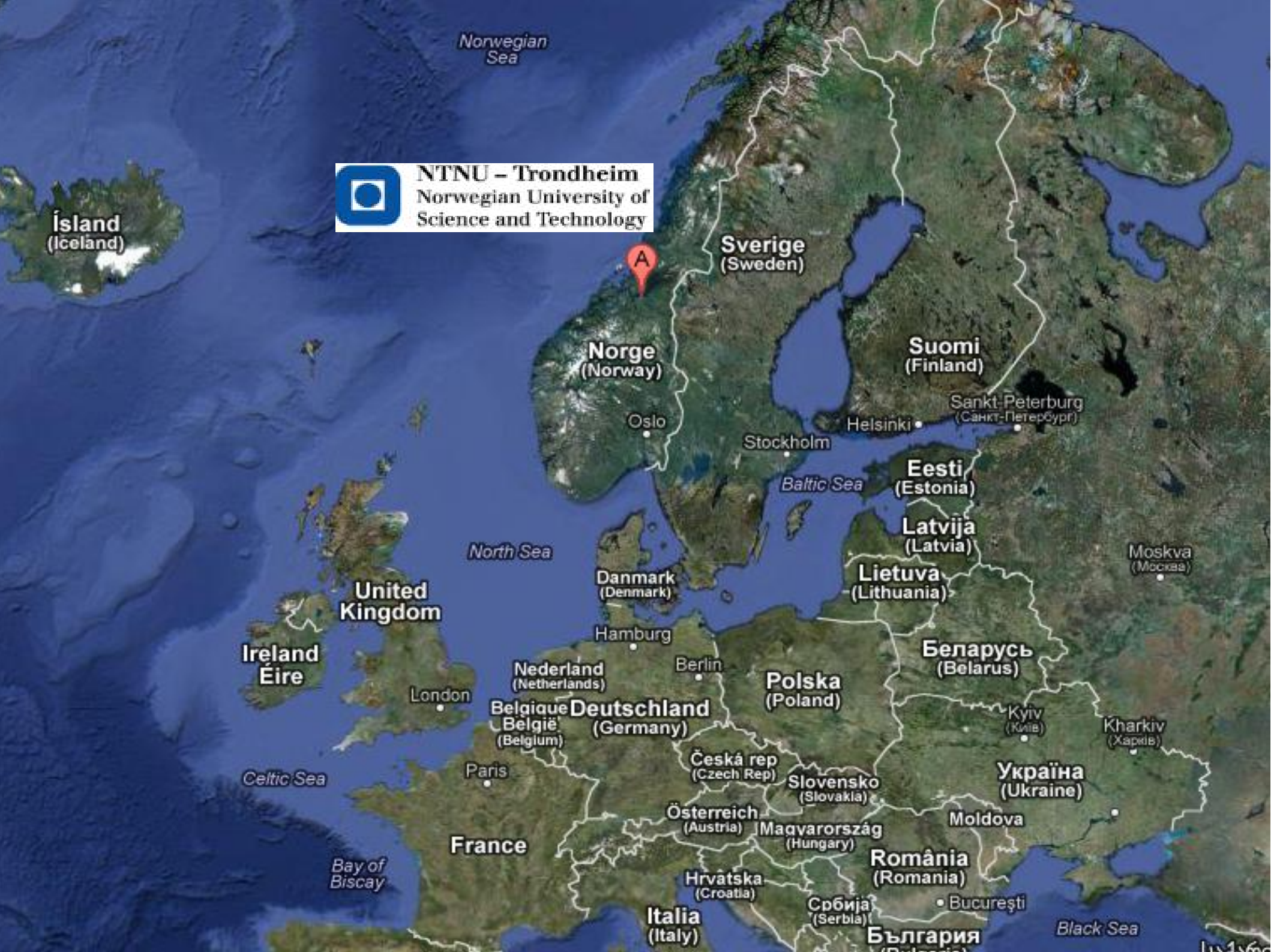
Course Outline

- Who am I and research in the industry
- Target Attacks & Success Stories
- Investigative Approach
- Pseudo-Automated Approach
- Discussion
- Questions

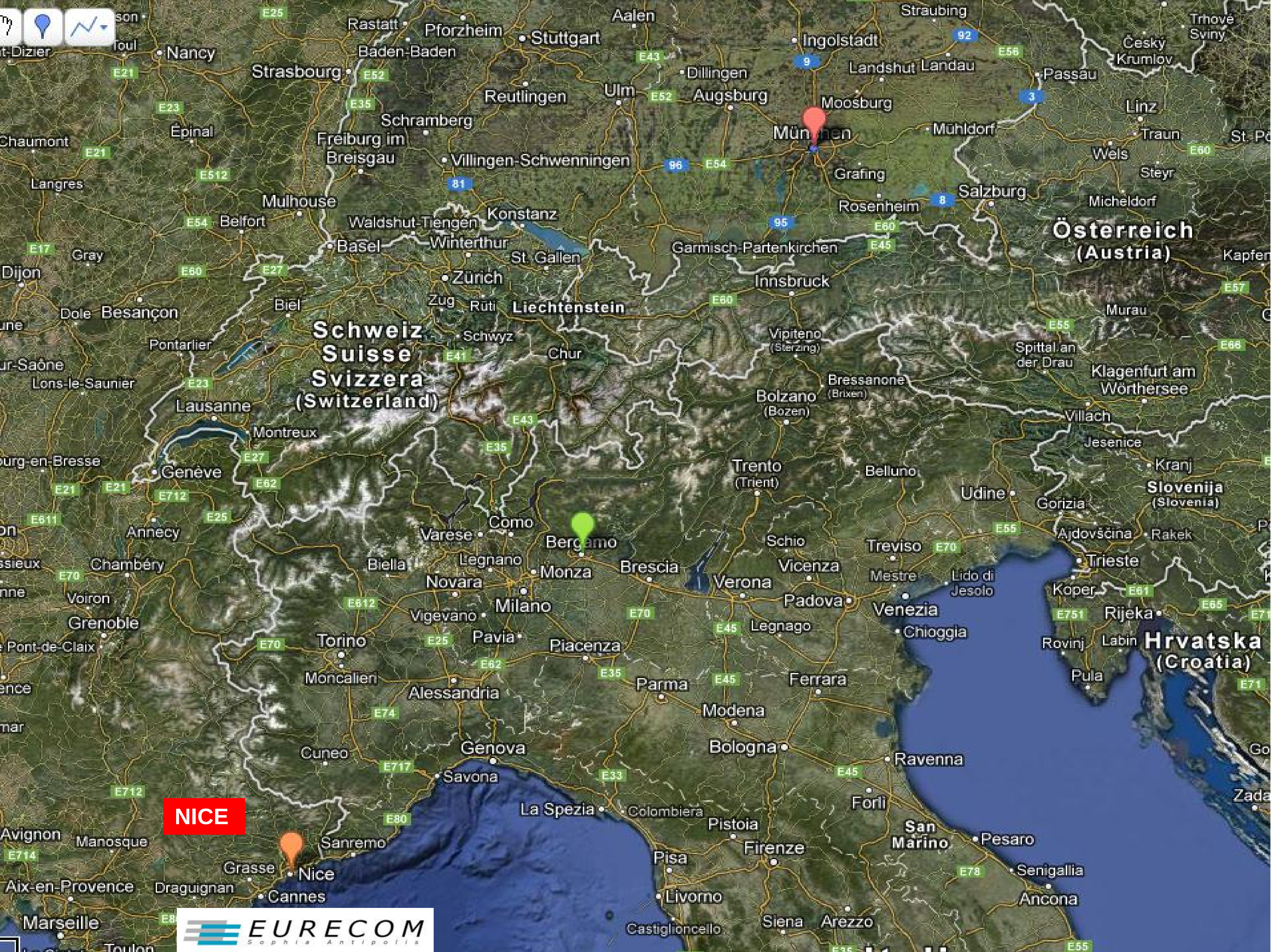
Who is Marco Balduzzi (embyte)


BERGAMO
Ireland
Éire
Dublin
Sheffield
Birmingham
Bristol
London
Celtic Sea
Bay of
Biscay
Nederland
(Netherlands)
Bremen
Berlin
Polska
(Poland)
Poznań
Łódź
Warszawa
Wrocław
Belgique
België
(Belgium)
Köln
Deutschland
(Germany)
Praha
Kraków
Česká republika
(Czech Republic)
Lëtzebuerg
(Luxembourg)
Frankfurt
am Main
Paris
France
München
Wien
Slovensko
(Slovakia)
Österreich
(Austria)
Schweiz
Suisse
Svizzera
(Switzerland)
Vaduz
Magyarország
(Hungary)
Zagreb
Torino
Milano
Hrvatska
(Croatia)
Bosna i
Hercegovina
(Bosnia and
Herzegovina)
Србија
(Serbia)
Genova
Toulouse
Monaco
Marseille
Italia
(Italy)
Andorra
Zaragoza
Barcelona
Roma
Crna Gora
(Montenegro)
Kosova
(Kosovo)
Македонија
(Macedonia (FYROM))
Napoli
Shqipëria
(Albania)
Madrid
Portugal
España
(Spain)
Lisboa
Palma
Tyrrhenian
Sea
Ελλάς
(Greece)
Murcia
Sevilla
Málaga
Gibraltar
الجزائر
العاصمة
Alger
تونس
Gouvernorat
de Tunis
Palermo
Patra
(Πάτρα)
أوران
Oran
Malta


WWW.MOBOTIX.COM
2009-11-03 CET 08:38:47


NTNU – Trondheim
Norwegian University of Science and Technology
A
Norwegian Sea
Ísland
(Iceland)
Sverige
(Sweden)
Norge
(Norway)
Suomi
(Finland)
Oslo
Helsinki
Sankt-Peterburg
(Санкт-Петербург)
Stockholm
Baltic Sea
Eesti
(Estonia)
Latvija
(Latvia)
North Sea
Moskva
(Москва)
Danmark
(Denmark)
Lietuva
(Lithuania)
United Kingdom
Hamburg
Беларусь
(Belarus)
Ireland
Éire
Nederland
(Netherlands)
Berlin
Polska
(Poland)
London
Belgique
België
(Belgium)
Deutschland
(Germany)
Kyiv
(Київ)
Kharkiv
(Харків)
Česká rep
(Czech Rep)
Celtic Sea
Paris
Slovensko
(Slovakia)
Україна
(Ukraine)
Österreich
(Austria)
Moldova
Magyarország
(Hungary)
France
România
(Romania)
Bay of Biscay
Hrvatska
(Croatia)
Србија
(Serbia)
București
Italia
(Italy)
Black Sea
България


secunet
MUNICH
Österreich
(Austria)
Schweiz
Suisse
Svizzera
(Switzerland)
Liechtenstein
Hrvatska
(Croatia)
Slovenija
(Slovenia)
Munich
Stuttgart
Augsburg
Ulm
Reutlingen
Konstanz
Zürich
Innsbruck
Salzburg
Linz
Passau
Strasbourg
Nancy
Basel
Lausanne
Genève
Montreux
Bern
Chur
Bolzano
(Bozen)
Trento
(Trient)
Milano
Como
Bergamo
Brescia
Verona
Venezia
Padova
Torino
Genova
Nice
Cannes
Marseille
Monaco
Sanremo
Bologna
Ravenna
Firenze
Pisa
Livorno
Ancona
Trieste
Rijeka
Zagreb


NICE
Nancy
Strasbourg
Rastatt
Baden-Baden
Pforzheim
Stuttgart
Aalen
Straubing
Ingolstadt
Landshut
Landau
Passau
Český Krumlov
Trnové Sviny
Dillingen
Augsburg
Ulm
Reutlingen
Schramberg
Freiburg im Breisgau
Villingen-Schwenningen
Moosburg
München
Mühldorf
Linz
Traun
Wels
Steyr
Grafing
Rosenheim
Salzburg
Micheldorf
Épinal
Chaumont
Langres
Mulhouse
Belfort
Konstanz
Waldshut-Tiengen
Basel
Winterthur
St. Gallen
Zürich
Garmisch-Partenkirchen
Innsbruck
Österreich
(Austria)
Gray
Dijon
Dole
Besançon
Biel
Zug
Rüti
Liechtenstein
Schwyz
Chur
Vipiteno
(Sterzing)
Murau
Spittal an der Drau
Klagenfurt am Wörthersee
Villach
Pontarlier
Lons-le-Saunier
Schweiz
Suisse
Svizzera
(Switzerland)
Lausanne
Montreux
Bressanone
(Brixen)
Bolzano
(Bozen)
Jesenice
Kranj
Genève
Trento
(Trient)
Belluno
Udine
Slovenija
(Slovenia)
Gorizia
Annecy
Como
Varese
Bergamo
Schio
Treviso
Ajdovščina
Rakek
Chambéry
Biella
Legnano
Monza
Brescia
Verona
Vicenza
Mestre
Lido di Jesolo
Trieste
Koper
Voiron
Novara
Milano
Padova
Venezia
Rijeka
Grenoble
Vigevano
Pavia
Legnago
Chioggia
Rovinj
Labin
Hrvatska
(Croatia)
Pont-de-Claix
Torino
Piacenza
Pula
Moncalieri
Parma
Ferrara
Alessandria
Modena
Bologna
Cuneo
Genova
Ravenna
Savona
La Spezia
Colombiera
Forlì
Avignon
Manosque
Sanremo
Pistoia
San Marino
Pesaro
Grasse
Nice
Pisa
Firenze
Senigallia
Aix-en-Provence
Draguignan
Cannes
Livorno
Ancona
Marseille
Toulon
Castiglioncello
Siena
Arezzo
EURECOM
Sophia Antipolis


© Gilles Ehrentrant www.nice-photographe.com ©

Back in the '80s – My First PC

Back in the '90s

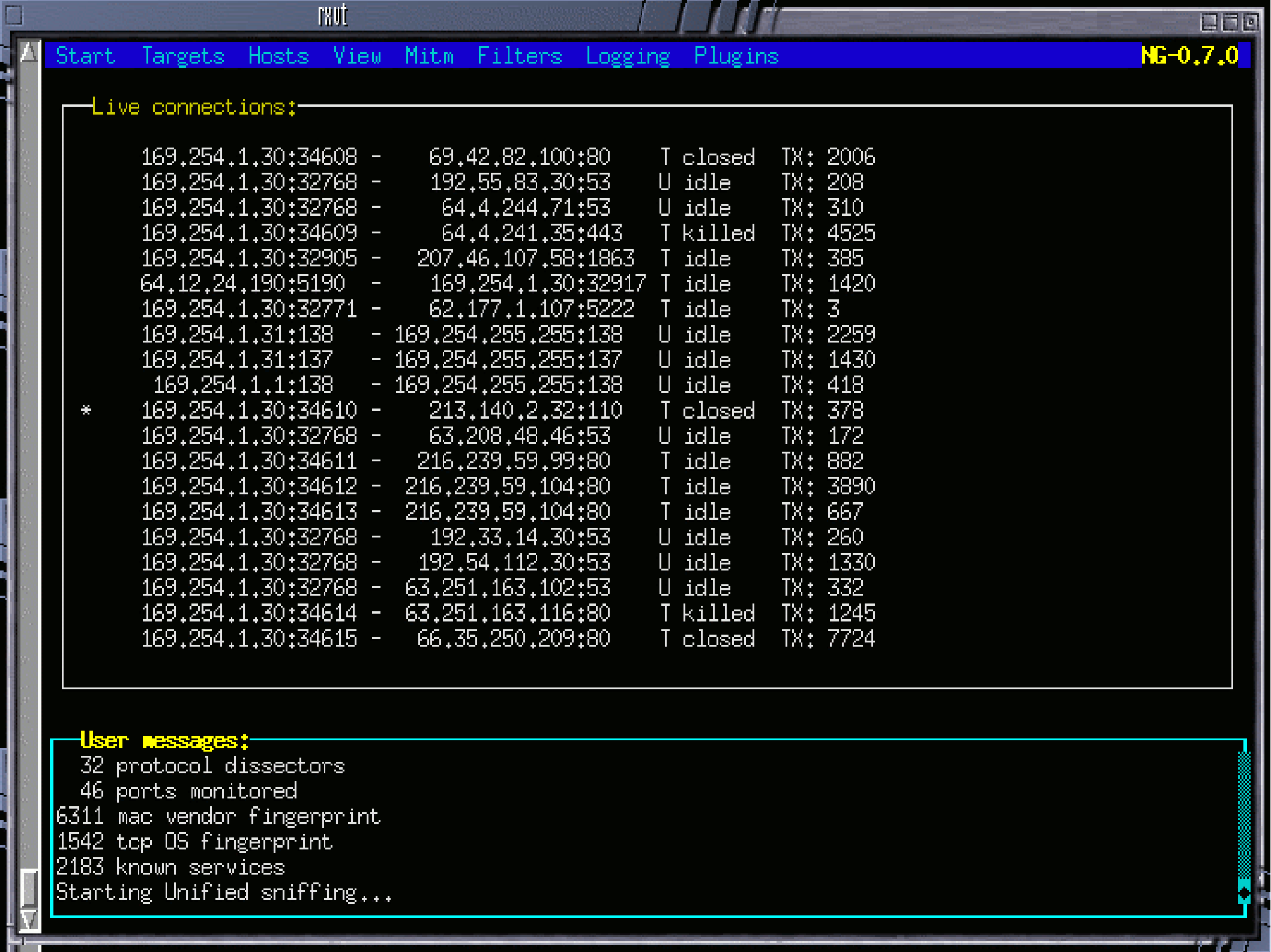
Welcome to FreeBSD!

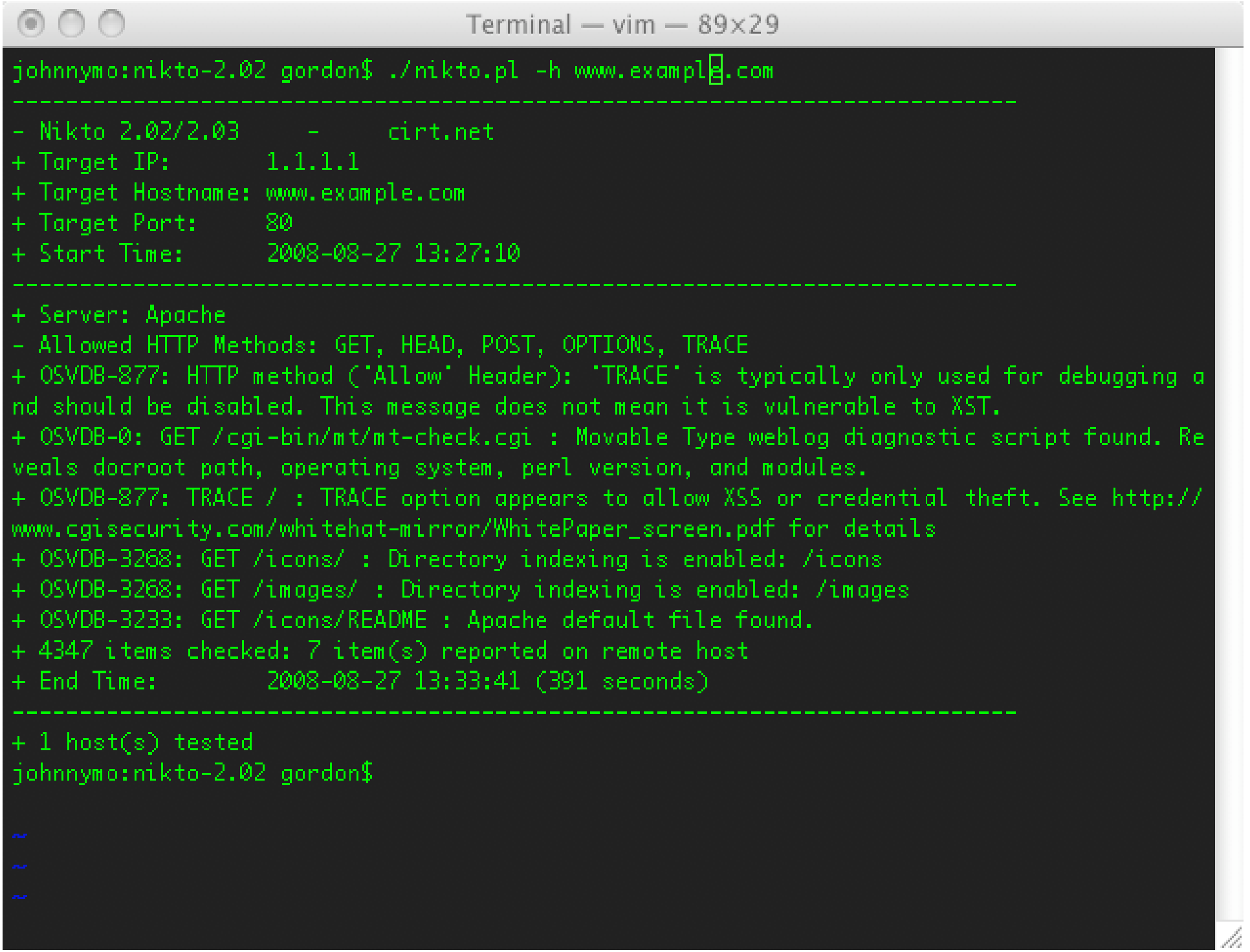
1. Boot FreeBSD [default]
2. Boot FreeBSD with ACPI disabled
3. Boot FreeBSD in Safe Mode
4. Boot FreeBSD in single user mode
5. Boot FreeBSD with verbose logging
6. Escape to loader prompt
7. Boot FreeBSD with USB keyboard
8. Reboot

Select option, [Enter] for default
or [Space] to pause timer 9

$ whoami
embyte


DEFCON
CTF

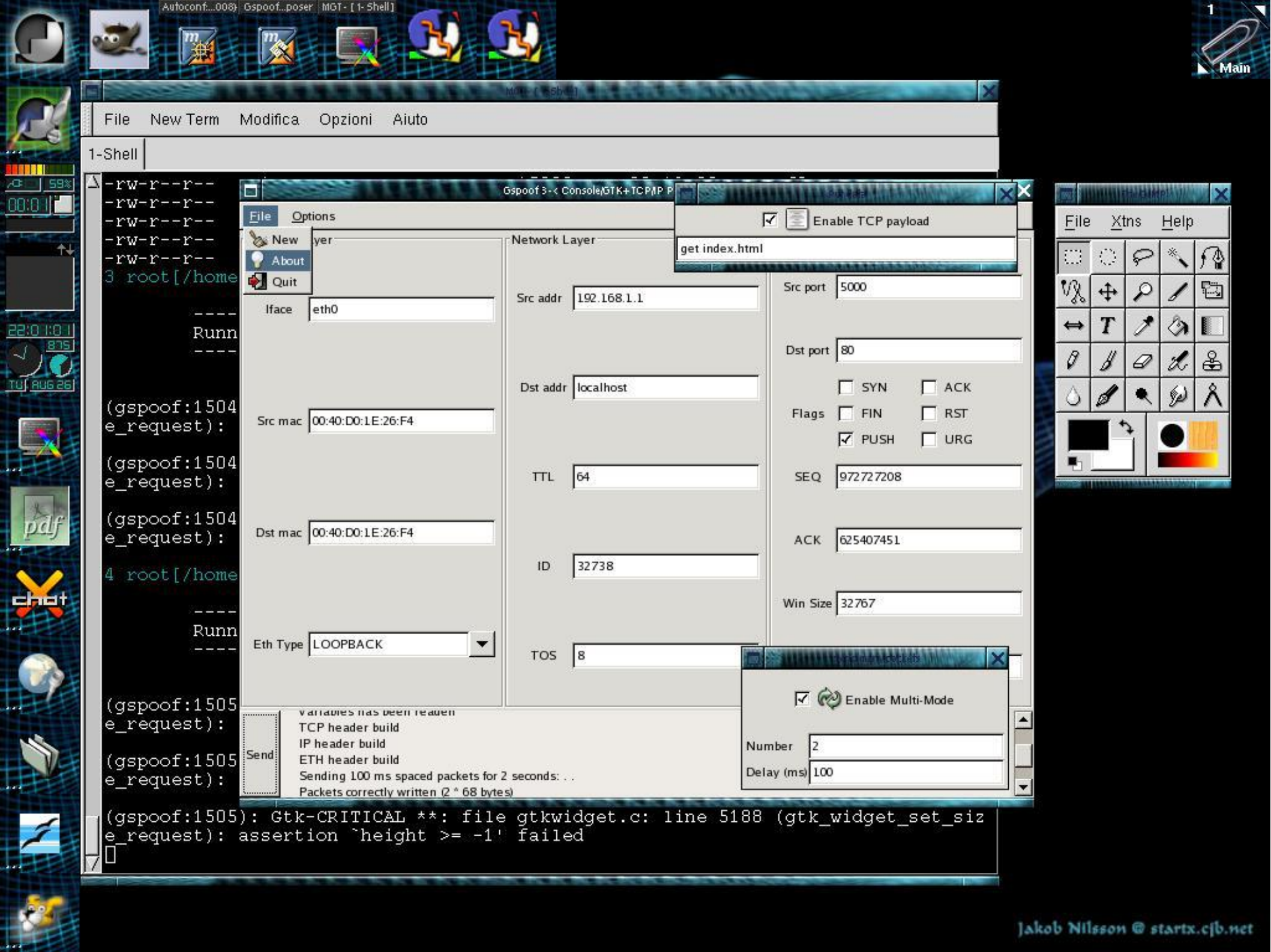

rxvt
Start Targets Hosts View Mitm Filters Logging Plugins
NG-0.7.0
Live connections:
169.254.1.30:34608 - 69.42.82.100:80 T closed TX: 2006
169.254.1.30:32768 - 192.55.83.30:53 U idle TX: 208
169.254.1.30:32768 - 64.4.244.71:53 U idle TX: 310
169.254.1.30:34609 - 64.4.241.35:443 T killed TX: 4525
169.254.1.30:32905 - 207.46.107.58:1863 T idle TX: 385
64.12.24.190:5190 - 169.254.1.30:32917 T idle TX: 1420
169.254.1.30:32771 - 62.177.1.107:5222 T idle TX: 3
169.254.1.31:138 - 169.254.255.255:138 U idle TX: 2259
169.254.1.31:137 - 169.254.255.255:137 U idle TX: 1430
169.254.1.1:138 - 169.254.255.255:138 U idle TX: 418
* 169.254.1.30:34610 - 213.140.2.32:110 T closed TX: 378
169.254.1.30:32768 - 63.208.48.46:53 U idle TX: 172
169.254.1.30:34611 - 216.239.59.99:80 T idle TX: 882
169.254.1.30:34612 - 216.239.59.104:80 T idle TX: 3890
169.254.1.30:34613 - 216.239.59.104:80 T idle TX: 667
169.254.1.30:32768 - 192.33.14.30:53 U idle TX: 260
169.254.1.30:32768 - 192.54.112.30:53 U idle TX: 1330
169.254.1.30:32768 - 63.251.163.102:53 U idle TX: 332
169.254.1.30:34614 - 63.251.163.116:80 T killed TX: 1245
169.254.1.30:34615 - 66.35.250.209:80 T closed TX: 7724
User messages:
32 protocol dissectors
46 ports monitored
6311 mac vendor fingerprint
1542 tcp OS fingerprint
2183 known services
Starting Unified sniffing...

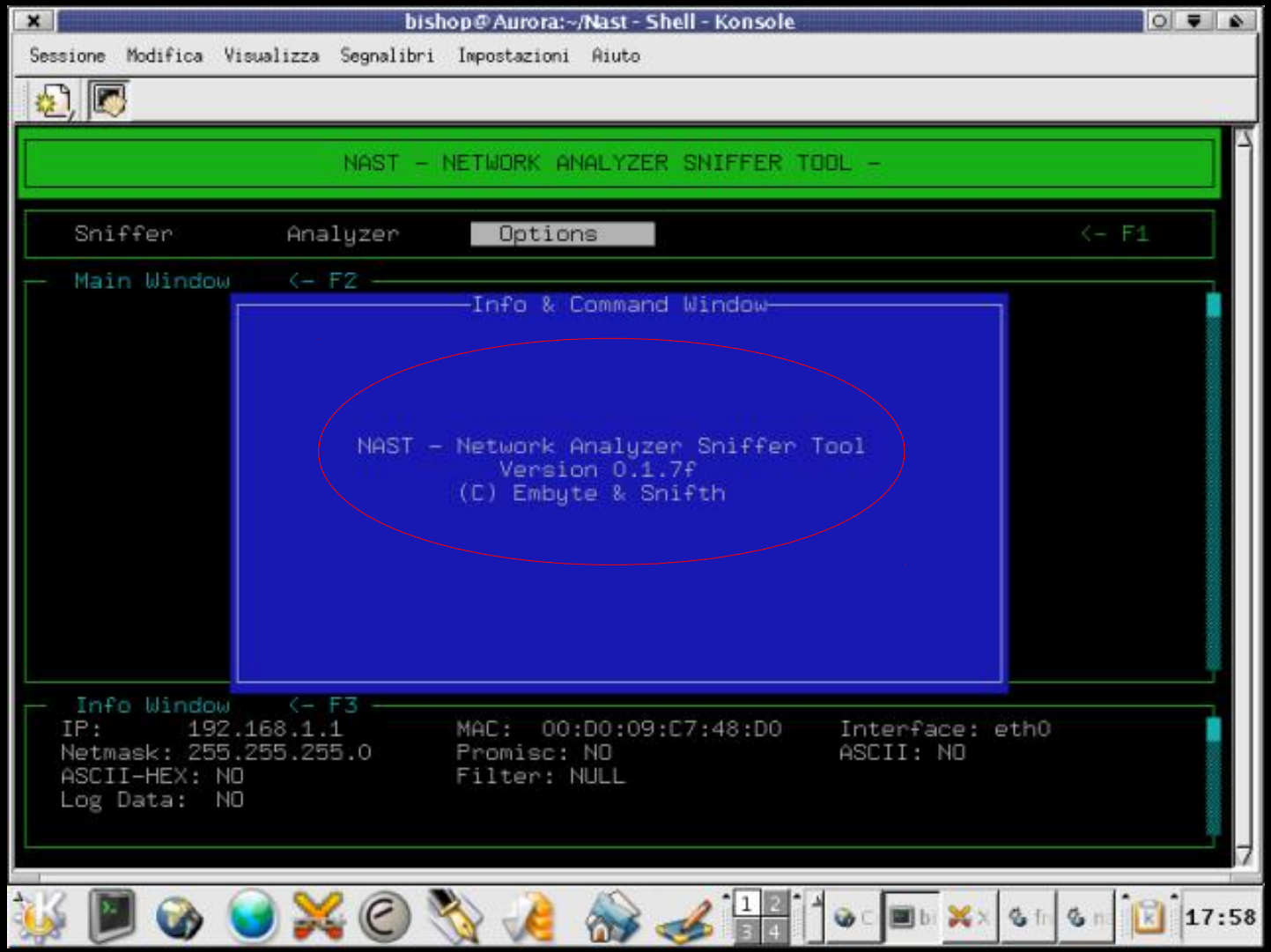

Terminal — vim — 89×29
johnnymo:nikto-2.02 gordon$ ./nikto.pl -h www.example.com

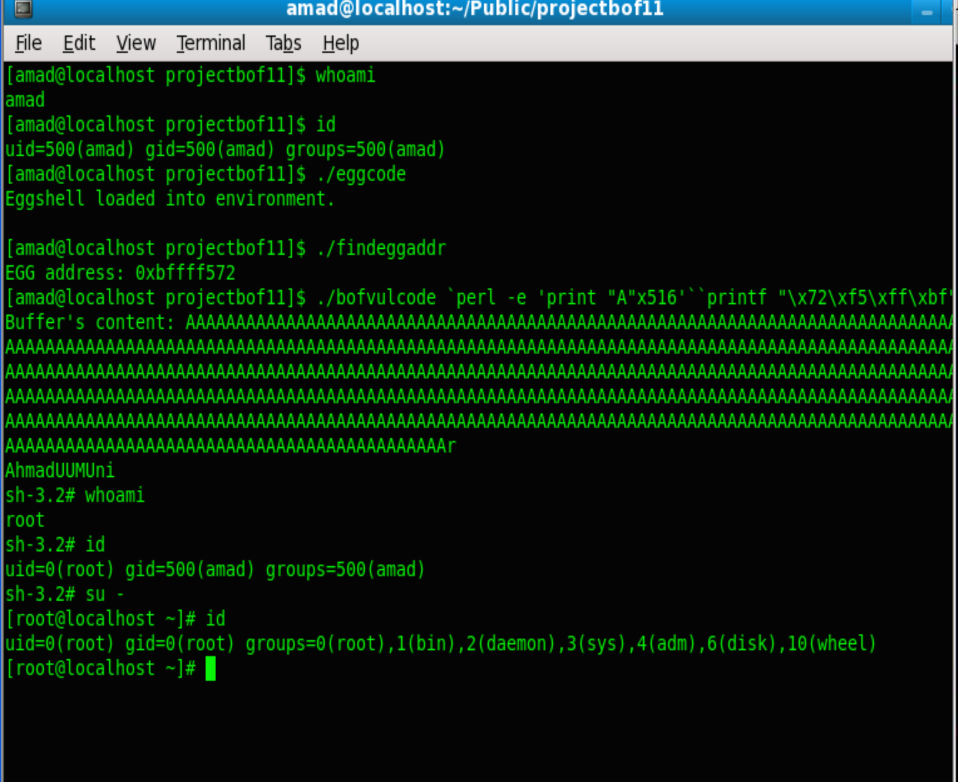
- Nikto 2.02/2.03   -   cirt.net
+ Target IP: 1.1.1.1
+ Target Hostname: www.example.com
+ Target Port: 80
+ Start Time: 2008-08-27 13:27:10

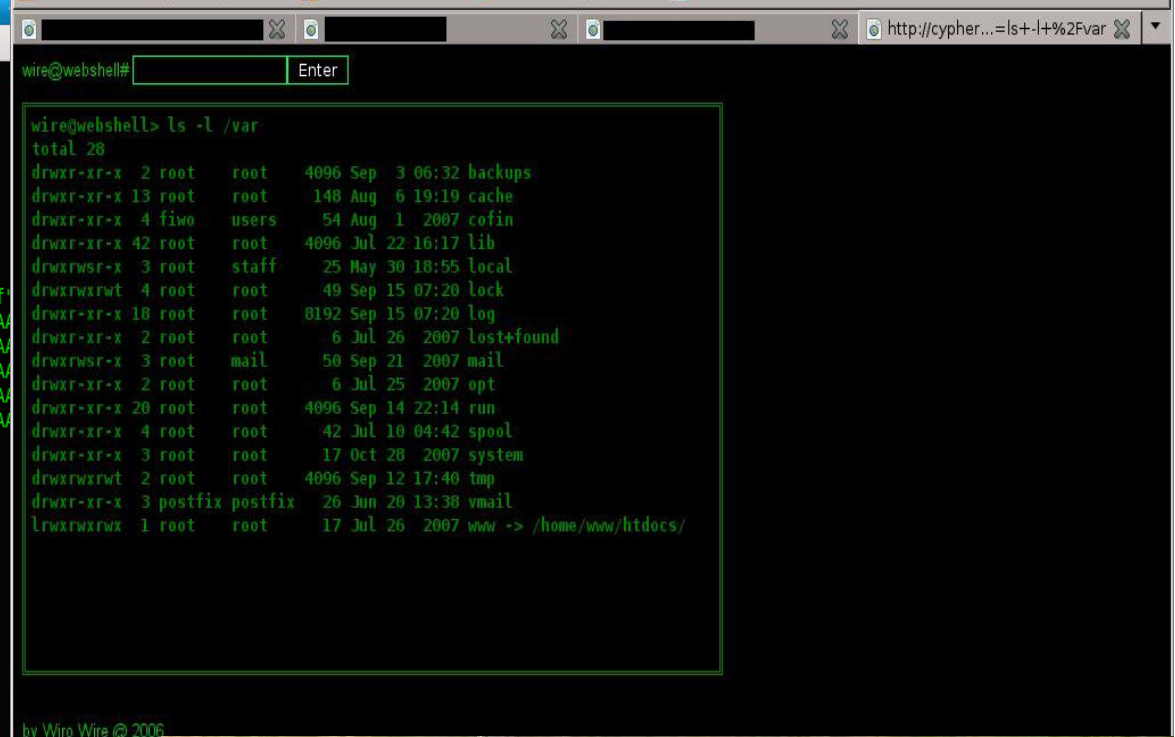
+ Server: Apache
- Allowed HTTP Methods: GET, HEAD, POST, OPTIONS, TRACE
+ OSVDB-877: HTTP method ('Allow' Header): 'TRACE' is typically only used for debugging a
nd should be disabled. This message does not mean it is vulnerable to XST.
+ OSVDB-0: GET /cgi-bin/mt/mt-check.cgi : Movable Type weblog diagnostic script found. Re
veals docroot path, operating system, perl version, and modules.
+ OSVDB-877: TRACE / : TRACE option appears to allow XSS or credential theft. See http://
www.cgisecurity.com/whitehat-mirror/WhitePaper_screen.pdf for details
+ OSVDB-3268: GET /icons/ : Directory indexing is enabled: /icons
+ OSVDB-3268: GET /images/ : Directory indexing is enabled: /images
+ OSVDB-3233: GET /icons/README : Apache default file found.
+ 4347 items checked: 7 item(s) reported on remote host
+ End Time: 2008-08-27 13:33:41 (391 seconds)

+ 1 host(s) tested
johnnymo:nikto-2.02 gordon$
~
~
~


File New Term Modifica Opzioni Aiuto
1-Shell
Gspoof 3-< Console/GTK+TCP/IP P
File Options
New
About
Quit
Iface eth0
Src mac 00:40:D0:1E:26:F4
Dst mac 00:40:D0:1E:26:F4
Eth Type LOOPBACK
Network Layer
Src addr 192.168.1.1
Dst addr localhost
TTL 64
ID 32738
TOS 8
Enable TCP payload
get index.html
Src port 5000
Dst port 80
Flags SYN ACK FIN RST PUSH URG
SEQ 972727208
ACK 625407451
Win Size 32767
Enable Multi-Mode
Number 2
Delay (ms) 100
Send
TCP header build
IP header build
ETH header build
Sending 100 ms spaced packets for 2 seconds: . .
Packets correctly written (2 * 68 bytes)
File Xtns Help
(gspoof:1505): Gtk-CRITICAL **: file gtkwidget.c: line 5188 (gtk_widget_set_size_request): assertion `height >= -1' failed
Jakob Nilsson @ startx.cjb.net


bishop@Aurora:~/Nast - Shell - Konsole
Sessione Modifica Visualizza Segnalibri Impostazioni Aiuto
NAST - NETWORK ANALYZER SNIFFER TOOL -
Sniffer
Analyzer
Options
<- F1
Main Window <- F2
Info & Command Window
NAST - Network Analyzer Sniffer Tool
Version 0.1.7f
(C) Embyte & Snifth
Info Window <- F3
IP: 192.168.1.1
MAC: 00:D0:09:C7:48:D0
Interface: eth0
Netmask: 255.255.255.0
Promisc: NO
ASCII: NO
ASCII-HEX: NO
Filter: NULL
Log Data: NO
17:58


amad@localhost:~/Public/projectbof11
File Edit View Terminal Tabs Help
[amad@localhost projectbof11]$ whoami
amad
[amad@localhost projectbof11]$ id
uid=500(amad) gid=500(amad) groups=500(amad)
[amad@localhost projectbof11]$ ./eggcode
Eggshell loaded into environment.
[amad@localhost projectbof11]$ ./findeggaddr
EGG address: 0xbffff572
[amad@localhost projectbof11]$ ./bofvulcode `perl -e 'print "A"x516'``printf "\x72\xf5\xff\xbf
Buffer's content: AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAr
AhmadUUMUni
sh-3.2# whoami
root
sh-3.2# id
uid=0(root) gid=500(amad) groups=500(amad)
sh-3.2# su -
[root@localhost ~]# id
uid=0(root) gid=0(root) groups=0(root),1(bin),2(daemon),3(sys),4(adm),6(disk),10(wheel)
[root@localhost ~]#


[redacted]
[redacted]
[redacted]
http://cypher...=ls+-l+%2Fvar
wire@webshell#
Enter
wire@webshell> ls -l /var
total 28
drwxr-xr-x 2 root root 4096 Sep 3 06:32 backups
drwxr-xr-x 13 root root 148 Aug 6 19:19 cache
drwxr-xr-x 4 fiwo users 54 Aug 1 2007 cofin
drwxr-xr-x 42 root root 4096 Jul 22 16:17 lib
drwxrwsr-x 3 root staff 25 May 30 18:55 local
drwxrwxrwt 4 root root 49 Sep 15 07:20 lock
drwxr-xr-x 18 root root 8192 Sep 15 07:20 log
drwxr-xr-x 2 root root 6 Jul 26 2007 lost+found
drwxrwsr-x 3 root mail 50 Sep 21 2007 mail
drwxr-xr-x 2 root root 6 Jul 25 2007 opt
drwxr-xr-x 20 root root 4096 Sep 14 22:14 run
drwxr-xr-x 4 root root 42 Jul 10 04:42 spool
drwxr-xr-x 3 root root 17 Oct 28 2007 system
drwxrwxrwt 2 root root 4096 Sep 12 17:40 tmp
drwxr-xr-x 3 postfix postfix 26 Jun 20 13:38 vmail
lrwxrwxrwx 1 root root 17 Jul 26 2007 www -> /home/www/htdocs/
by Wiro Wire @ 2006


Chocolate Cream Wafers
NET WT.
350g


YOU'LL NEVER
GET TO WORK
ON TIME
HAHA!!

Turning a hobby into income

Many of us have hobbies, either to destress, cultivate personal creativity or both. Wouldn't it be nice to up the ante and make money from a favourite pastime?

by Lim Siew May

FORTUNATELY, there has never been a better time to start selling your wares or services. The Internet has opened up myriad channels to reach customers, and many of these online portals are free or levy minimum rates. The best people to talk about monetising your hobby are, of course, those who have done it. We found seven such individuals whose profitable interests range from yoga and pottery to swiftlet farming. After talking to them, we found six tips on how you can monetise your hobby.

C|EH™
Certified Ethical Hacker

ict CONSULTING

securenetwork

eMaze informed security

SAP

bmcsoftware Numara Software now part of BMC

secunet

iseclab

EURECOM Sophia Antipolis

TELECOM ParisTech

- 2010
  - AsiaCCS 2010
  - DIMVA 2010
  - RAID 2010
  - TWDT 2010
- 2011
  - NDSS 2011 (2 papers)
  - LEET 2011
  - DIMVA 2011
- 2012
  - SAC 2012
  - Schloss Dagstuhl 2012
- 2013
  - PST 2013 (2 papers)
- 2014
  - ACSAC 2014
  - ISC 2014

- HackMeeting (HackIT)
  - 2003, 2004, 2014
- LinuxDay
  - 2003, 2004, 2005
- 2004
  - Security Date, Webb.it, MOCA, SatExpo
- OWASP
  - AppSec Research EU 2010, 2011, 2013
  - BeNeLux 2010, 2011
  - Italy 2013, 2014
- BlackHat
  - EU 2011, USA 2012, ASIA 2014
  - WebCast 2011 & 2012
- HITB (Hack In The Box)
  - KUL 2011, EU 2012, EU 2014
- Latin America
  - Security Zone Colombia 2011, 2012
  - 8.8 Chile 2011, 2012
- Others
  - MOHP 2007
  - Swiss Cyber Storm 2011
  - Etc...

Topics of Interest

- Real problems
- Web and Browser Security
- Vulnerability Code Analysis
- Botnets Detection (Network Security)
- Cybercrime Investigation and Research
- Privacy and Threats in Social Networks, and New Technologies
- Malware and Intrusion Detection Systems

Real Topics of Interest

So, what am I doing now?

Senior Research Scientist

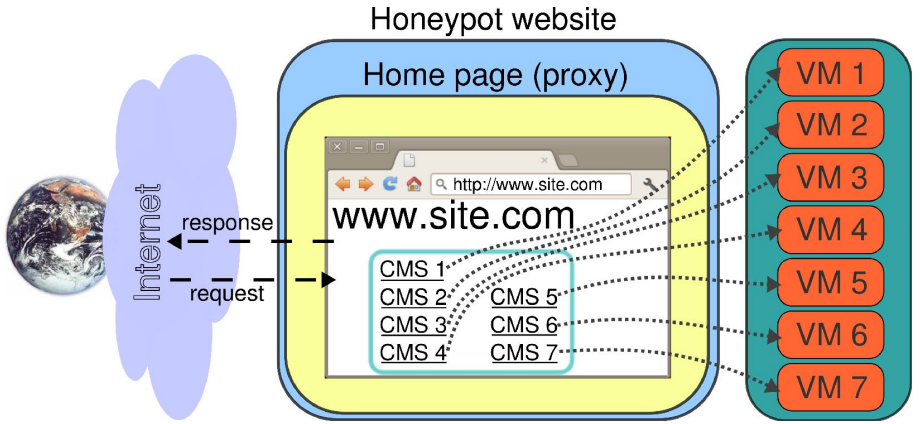
FTR Mission

- Forward-Looking Threat Research
- Considered the “elite” research team within Trend Micro

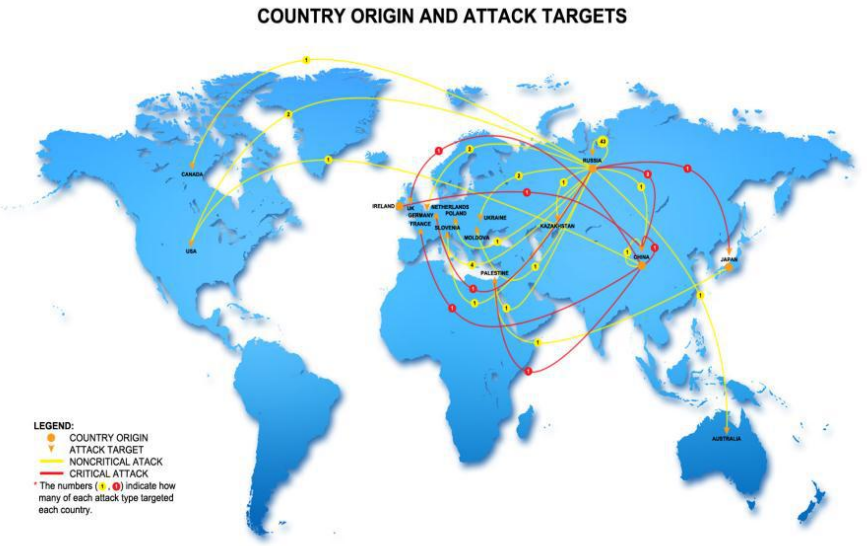
International Coverage

Honeypots Research

- Yes, we **love** data ;-)
- Web Honeypot. Joint-research project with EURECOM

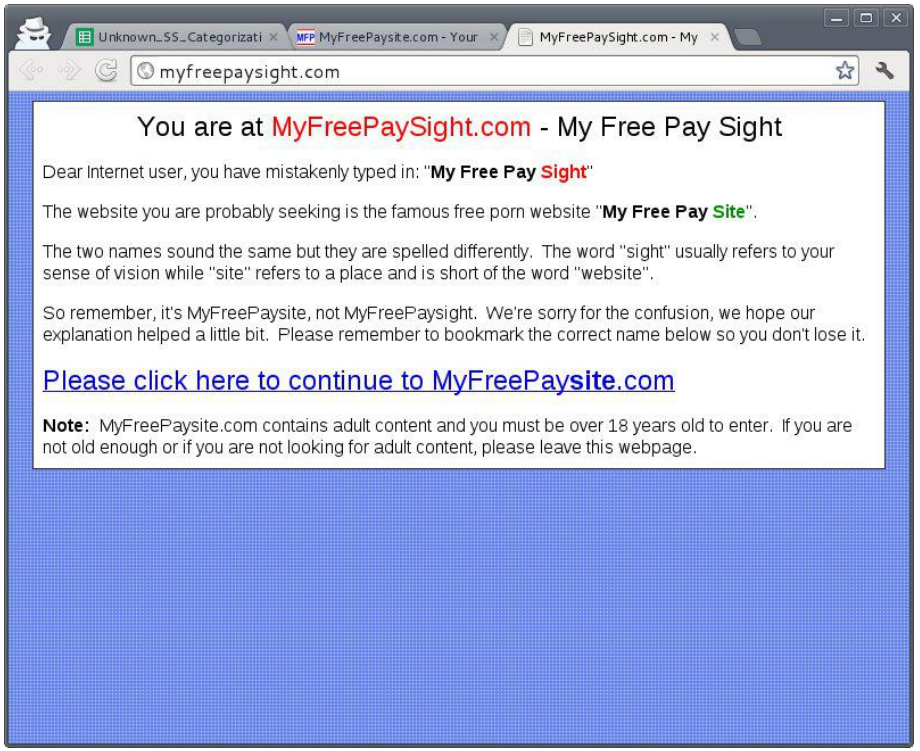


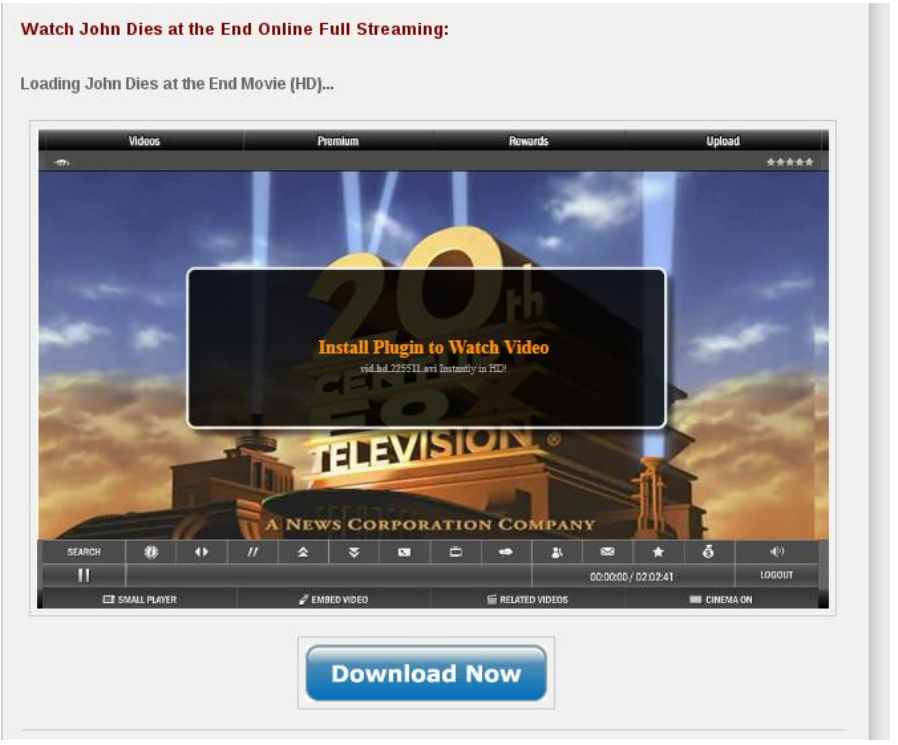
- ICS Honeypot.



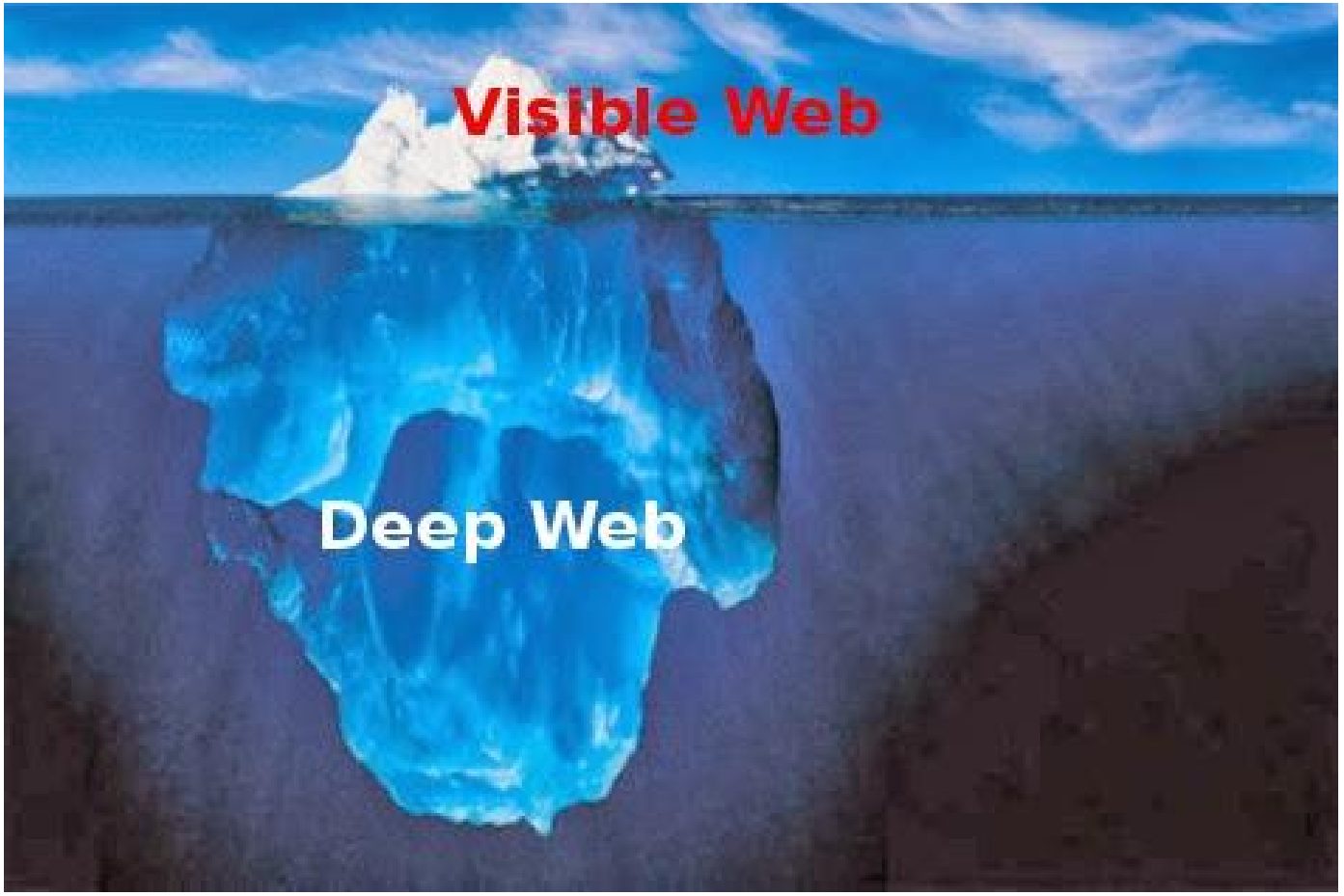
Web Research

- Soundsquatting: Uncovering the use of homophones in domain squatting
  - Joint-research project with KUL. @ISC2014





Scouting the DeepWeb



Marketplaces & exchanged goods

Table 1: Prices of Different Types of Goods

Site name	Address	Type of good	Cost	Normalized Cost (US$)
CloneCard	http://kpmp444tubeirwan.onion/board/int/src/1368387371226.jpg	EU/US credit cards	1 BTC	US$126
Mister V	http://wd5pbd4odd7jmm46.onion/	EU credit cards	€40–80	US$54–100
CC-Planet Fullz	http://tr36btffdmdmavbi.onion	EU/US credit cards	UA$40	US$54
CC 4 ALL	http://qhkt6cqo2dfs2llt.onion/	EU/US credit cards	€25–35	US$33–47
Cloned credit cards	http://mxdcyv6gjs3tvt5u.onion/products.html	EU/US credit cards	€40	US$54
NSD CC Store	http://4vq45ioqq5cx7u32.onion	EU/US credit cards	US$10	US$10
Carders Planet	http://wihwaoykcdzabadd.onion/	EU/US credit cards	US$60–150	US$60–150
HakPal	http://pcdyurvcdiz66qjo.onion/	PayPal accounts	1 BTC for US$1,000	US$126 for US$1,000
Onion identity	http://abbujjh5vqtq77wg.onion/	Fake IDs/passports	€1,000–1,150 (ID) €2,500–4,000 (passport)	US$1,352–1,555 (ID) US$3,380–5,400 (passport)
U.S. citizenship	http://ayjkg6ombrsahbx2.onion/silkroad/home	U.S. citizenship	US$10,000	US$10,000
U.S. fake driver's licenses	http://en35tuzqmn4lofbk.onion/	Fake U.S. driver's license	US$200	US$200
U.K. passports	http://vfqnd6mieccqyiit.onion/	U.K. passports	£2,500	US$4,000
Guttemberg prints	http://kpmp444tubeirwan.onion/board/int/src/1366833727802.jpg	Counterfeit money	1/2 of the monetary value	1/2 of the monetary value
High-quality Euro replicas	http://y3fpieiezy2sin4a.onion/	Counterfeit Euro banknotes	€500 for 2,500 CEUR €1,000 for 3,000 CEUR €1,900 for 6,000 CEUR	US$676 for 2,500 CEUR US$1,352 for 3,000 CEUR US$2,570 for 6,000 CEUR

Table 2: Sample Russian Underground Offerings and Prices

Address	Type of Good	Cost
http://forum.prologic.su/index.php?showtopic=7468	U.S. credit cards	US$2.5
http://xek.name/showthread.php?t=10519	U.S. credit cards EU credit cards	US$25–40 US$70–120
http://r00t.in/showthread.php?t=18510'	U.S. credit cards EU credit cards	US$2–3 US$10
http://brute.name/threads/8643/	U.S. credit cards EU credit cards	US$2–3 US$8–9
http://carding.cc/showthread.php?t=6030	Credit card scans	US$14
http://exploit.in/forum/index.php?showtopic=38917'	PayPal accounts	US$2–15
http://carding.cc/showthread.php?t=2548	PayPal accounts	US$10 for US$0–200 account US$20 for US$20–200 account US$50 for US$200–1,000 account US$100 for US$1,000–2,000 account US$150 for US$3,000–4,000 account
http://brute.name/threads/8643/	PayPal accounts	US$200 for US$2,000 account US$500 for US$8,000 account US$1,000 for US$15,000 account
http://www.xaker.name/forvb/showthread.php?t=21284	Russian passports	US$250

Cybercriminals' infrastructures

⊖	/gate.php	367	2013-12-09	2014-04-25

Domain breakdown

Scheme	Hostname	Port	# Rep	First seen	Last seen
-	egzh3ktnywjwabxb.onion	80	213	2013-12-09...	2014-01-17...
http	akrnfve5eifqygwr.onion	80	154	2014-02-23...	2014-04-25...

New ZeuS Banking Trojan Targets 64-Bit Systems, Leverages Tor

The notorious ZeuS Trojan is now armed with a 64-bit version that uses the Tor network to communicate with its command-and-control infrastructure.

"*The more people switch to 64-bit platforms, the more 64-bit malware appears,*" blogs Kaspersky Lab researcher Dmitry Tarakanov. "*We have been following this process for several years now.*"

It's a new twist for ZeuS, to be sure, but also a confusing one because 64-bit browsers are not widely used by the public.

"*ZeuS is mostly intended to intercept data passing through browsers and modify that data, allowing the operator to steal information related to online banking, to wire transactions, or to cover his tracks,*" Tarakanov writes. "*But nowadays people still use 32-bit browsers-- even on 64-bit operating systems. So 32-bit versions of ZeuS have been sufficient to keep the thieves satisfied with their earnings.*"

Fortinet's Richard Henderson agreed, calling 64-bit malware "*very uncommon.*" The real question, however, is how long it will be until it is not the exception, but the norm.

"*Typically, malware is written in order to cast as wide of a net as possible, and that means sticking with what has the greatest chance of capturing the largest number of infections,*" says Henderson, security strategist for Fortinet's FortiGuard Threat Research and Response Labs.

"*Win32 64-bit Windows still run 32-bit applications, and as the analysis mentioned, the vast majority of 64-bit Windows users are still running 32-bit internet browsers. It's also the main reason why we don't see a lot of Mac malware in the wild-- the number of computers out there running 32-bit Windows or 64-bit Windows with the ability to run 32-bit software is orders of magnitude larger.*"

The 64-bit version of the malware has been in the wild for at least 6 months. According to Kaspersky Lab, the 64-bit version was actually found inside a 32-bit ZeuS sample that injected malicious code into target processes and injected the 64-bit version into the process as if it belonged to a 64-bit application. If the process belongs to a 32-bit application, then the malware pushes the 32-bit version.

The 64-bit version behaves like any other variant of ZeuS, installing files into folders with randomly generated names placed inside of the %APPDATA% directory.

"*Interestingly, the configuration file for this version of ZeuS includes a long list of programs that the malware can function on if they are found on the infected system,*" Tarakanov blogs. "*There are different types of programs, but all of them contain valuable private information that cybercriminals would love to steal-- login credentials, certificates and so on. Don't forget that ZeuS is capable of intercepting key strokes and data before encryption/after decryption that is sent/received on a network with the use of some typical system API functions. So, when operating inside these programs ZeuS is able to intercept and forward a lot of valuable information to the botnet operator.*"

In addition to the 64-bit component, this version of ZeuS maintains a tor.exe utility from the 0.2.3.25 version inside its body, he adds.

"*Tor.exe is launched indirectly-- ZeuS starts the system svchost.exe application in suspended mode, then injects the tor.exe code into this suspended svchost.exe process, tunes the code to run properly and resumes execution of the suspended svchost,*" Tarakanov explains. "*As a result, instead of the system svchost.exe, the process actually starts executing tor.exe. The Tor utility under the cover of the svchost.exe process creates an HTTP proxy server listening to the TCP port 9050.*"

ZeuS variants using Tor, however, is nothing new; in actuality, Kaspersky Lab has tracked samples with signs of Tor communications as far back as 2012. Step-by-step instructions are even on the internet on how to use tor.exe to pass ZeuS or SpyEye traffic via the Tor network, as well as how to create onion domain hosting for command-and-control for these banking Trojans.

"*But these earlier samples mostly had CnC-- command and control-- domains specified in their bodies as localhost or 127.0.0.1 meaning that samples of ZeuS or Spyeye themselves were not tied too strictly with Tor communications, whereas the version of ZeuS described here has CnC onion domain egzh3ktnywjwabxb.onion defined in its internal block of settings,*" the Kaspersky researcher notes.

"*And tor.exe is included directly in its body and is run by ZeuS itself. So Tor communications and the 64-bit version are inseparable parts of this ZeuS sample, with the functionality included at the very development stage.*"

Technology Research – AIS

- Joint-project with external researcher

Ship Tracking Hack Makes Tankers Vanish from View

A system used by ships worldwide to broadcast their location for safety purposes lacks security controls and is vulnerable to spectacular spoofing attacks, researchers show.

By Tom Simonite on October 18, 2013

Off course: Spoof radio signals convinced an online ship tracking service that this fake craft had traveled on a path near Italy that spelled out the hacker term "pwned," which describes a system that has been compromised by an attacker.

A system used to track shipping vessels worldwide has been shown to be easily hijacked. Researchers found that it is possible to cause fake vessels to appear, real ones to disappear, and to issue false emergency alerts using cheap radio equipment.

Researchers with the computer security company Trend Micro discovered the problem, which stems from a lack of security controls in a technology known as Automatic Identification System, or AIS, used by an estimated 400,000 ships worldwide. Ships using the system transmit a radio signal with their location and some other details, so that other vessels and port authorities can view a map with all nearby craft shown in real time. International Maritime Organization rules make AIS mandatory on passenger vessels and on cargo ships over a certain size. Lighthouses, buoys, and other marine fixtures also transmit their location using the system.

"We were really able to compromise this system from the root level," says Kyle Wilhoit, a researcher with Trend Micro's Future Threat Research team. By purchasing a 700-euro piece of AIS equipment and connecting it to a computer in the vicinity of a port, the researchers could intercept signals from nearby craft and send out modified versions to make it appear to other AIS users that a vessel was somewhere it was not.

Technology Research

GLOBAL

INTERPOL

IMPACT

APAC

防衛省・自衛隊
MINISTRY OF DEFENSE

経済産業省
Ministry of Economy, Trade and Industry

Australian Government
Department of Defence

京都府警察
Kyoto Prefectural Police

MIC
Ministry of Internal Affairs and Communications

法務省
MINISTRY OF JUSTICE

NORTH AMERICA

SFECTF

Homeland Security

Public Safety Canada

Sécurité publique Canada

EUROPE

EUROPOL

SOCA

MINISTRY OF DEFENCE

POLITIE

POLIS

LKA

Bundeskriminalamt

Gendarmerie nationale

LATIN AMERICA

registro.br
Registro de Domínios para a Internet no Brasil

CAIS

RNP

Operation Ghost Click

- 4 Millions bots, 100 C&C servers (#1 history)
- Steal clicks (replacing ads, hijacking search results)
- Collaboration between FBI, Estonian Police and FTR
- 2-years operation
- Vladimir Tsastsin, CEO of Rove Digital (ISP)
- 6+ years arrested

Hamza Bendelladj (BX1)

- SpyEye co-author (#1 banking trojan)
- Algerian in Thailand (XMas)
- https://www.youtube.com/watch?v=OAhSW-l0-Xk

Reveton Ransomware

- Locks you out. Demands money to let you back in :)

- http://www.northeastern.edu/securenu/wp-content/uploads/2012/09/multiple_ransomware_warnings.gif
- https://www.youtube.com/watch?v=wBMyaOa4Xnw

BUT, Are these Targeted Attacks?

NO!

Targeted Attacks (MKT likes APT)

- Internet Security Threat Report:
  - Spam volume is decreased, but...
  - Web-based attacks increased **30%**
  - 5,291 new vulnerabilities discovered in 2012
  - The number of phishing pages spoofing social networks increased 125%
- **42%** increase in targeted attacks in

Shift

- World dominated by widespread malware that infects indiscriminately, to a more **selectively targeted approach**
- Just-for-fun era is over?
- Espionage, nation-driven, criminal organizations
- Specific targets / industries
  - e.g. civil society organizations, business enterprises, critical infrastructures, government and military assets

Modus Operandi

- High-selective Reconnaissance
- Use of Social Engineering
- Emails and IMs as attack-vectors
- Malicious PDF, DOC, Flash
- Persistence and Lateral Movements
- Data Ex-filtration

2009: Operation Aurora

Cyber-attack on U.S. firms, Google traced to Chinese

By Bill Gertz - *The Washington Times - Wednesday, March 24, 2010*

The cyber-attack on Google and other U.S. companies was part of a suspected Chinese government operation launched last year that used human intelligence techniques and high-technology to steal corporate secrets, according to U.S. government and private-sector cybersecurity specialists.

More worrying, however, is the likelihood that the cyber-attacks that led Google this week to end its cooperation with Beijing-controlled censorship and move its search engine service to Hong Kong included planting undetectable software on American company networks that could allow further clandestine access or even total control of computers in the future.

An Obama administration official said the U.S. government was able, with some confidence, to link the attack, first discovered last summer, to Chinese government organs. However, the official declined to provide details to avoid making future Chinese cyber-attack identification more difficult.

"The attack was very targeted. It targeted engineers and quality assurance developers, people with very high levels of access into the organization," said George Kurtz, chief technology officer for computer security firm McAfee who investigated the attack for several of the affected companies.

Ongoing since 2004 (at the least)

Strategic industries should go on high alert

THURSDAY, 10 FEBRUARY 2011 16:07

A frightening pattern of targeted espionage reports has a new entry provided by McAfee. The Night Dragon report, issued today, details a concerted effort to harvest oil and gas reserve information and other highly confidential information from the executives of at least five major oil, gas, and energy companies. Reserve trading and SCADA information was also compromised. McAfee provides strong attribution that the attacks came from China (strong, not conclusive, which would require a believable source taking credit for the attacks).

The pattern indicates that China engages in focused projects that target particular industries or governments. A brief timeline with ever increasing attribution:

2004 Titan Rain (Slideshare presentation)

2006 British MPs targeted. (Guardian, Smash and Grab, the High Tech Way)

2007 German Chancellery compromised and China accused of being the perpetrator. (Der Spiegel, Merkel's China Visit Marred by Hacking Allegations)

2007 US Pentagon email servers compromised for an extended period. Cost to recover $100 million. p { margin-bottom: 0.08in; }(Paul, Ryan. "Pentagon e-mail taken down by hackers." *Ars Technica*. 22 June 2007)

2007 Oak Ridge National Laboratory targeted by Chinese hackers (Stiennon, Haephratic Technique Used to Crack US Research Lab)

2009 Ghostnet report from SecDev on Chinese infiltration of Dalai Lama's office. (Scribd presentation: Tracking GhostNet)

2009 Three largest resource companies in Australia, including Rio Tinto compromised.(Rio Tinto hacked at time of Hu arrest)

2009 Google Aurora attacks target user data and source code. (McAfee blog)

2010 Corollary Aurora attacks against Marathon Oil, ExxonMobil, and ConocoPhillips (Christian Science Monitor, US oil industry hit by cyberattacks: Was China involved?p { margin-bottom: 0.08in; })

2010 Shadows in the Cloud report from SecDev on successful attacks against India's military networks. (Scribd report: Shadows in the Cloud)

2010: StuxNet
Critical Infrastructures

Edward Snowden: U.S., Israel 'Co-Wrote' Cyber Super Weapon Stuxnet

By Lee Ferran @leeferran
Jul 9, 2013 2:22pm

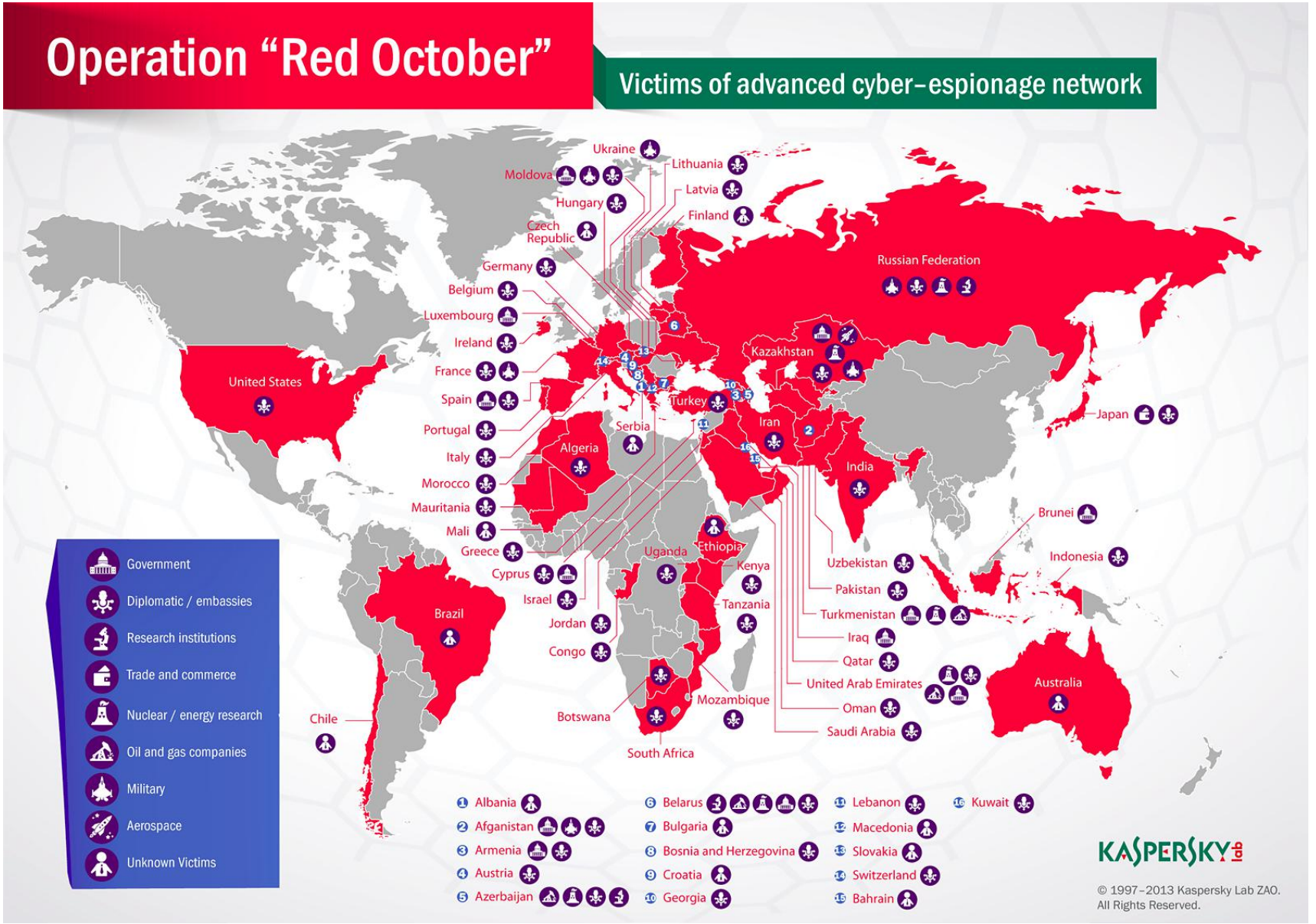
Kirit Radia @KiritRadia_ABC

The former National Security Agency contractor on the run from U.S. authorities halfway around the world said that Stuxnet, an unprecedented cyber weapon that targeted Iran's nuclear program, was the product of a joint American-Israeli secret operation.

Before Edward Snowden became a household name, he conducted an interview via encrypted emails with cyber security expert Jacob Appelbaum and was asked about the game-changing computer code, according to the interview published in the German newspaper Der Spiegel Monday.

"NSA [U.S. National Security Agency] and Israel co-wrote it," Snowden said.

2012-07: Cyberespionage program



NEWS

Targeted cyber attacks cost up to £1.6m

Warwick Ashford
Thursday 25 July 2013
09:37

Targeted cyber attacks could cost up to £1.6m, the 2013 Global Corporate IT Security Risks survey by B2B International and security firm Kaspersky Lab has revealed.

According to the report, £1.4m stems directly from the incident itself in losses from critical data leakages, business interruptions and expenses for remediation specialist services.

Companies face an additional bill of about £146,000 for actions taken to prevent such incidents from taking place again in the future, including updating software and hardware, and hiring and training staff.

Company losses resulting from targeted attacks on small and medium enterprises (SMEs) are lower, at around £60,000 per incident.