New School Information Gathering

Chris Gates

http://carnal0wnage.blogspot.com

http://www.learnsecurityonline.com

Who Am I?

- Penetration Tester
- LearnSecurityOnline.com
- Security Blogger
- EthicalHacker.net columnist
- Alphabet Soup if you care

Carnal Ownage

11/10/94
Classified by [redacted] b7c
Declassify on: OADR

Standard Disclaimer

The standard this is me talking and not my employer disclaimer applies

Carnal Ownage

11/10/94
Classified by [redacted] b7c
Declassify on: OADR

Agenda

- New School?
- Open Source Intelligence Gathering (OSINT)
- FierceDNS
- SEAT/Goolag
- Google Mail Harvesters
- Metagoofil
- Online Tools
  - ServerSniff/DomainTools/CentralOps/Clez.net/Robtex/Spoke
- Maltego

Carnal Ownage

11/10/94
Classified by [redacted] b7c
Reclassify on: OADR

Premises

- Couple of premises to frame the talk
  - Black box approach to info gathering, meaning the customer wants you to find everything about them you can via “open source” methods.
  - Client side and social engineering attacks are going to be used, therefore its critical we gather that client information (emails & phone numbers) for the pentest.

Carnal Ownage

11/10/94
Classified by [redacted] b7c
Declassify on: OADR

This is what you get:

baytsp.com

Carnal Ownage

11/10/94
Classified by [redacted] b7c
Declassify on: OADR

Questions

- WTF is baytsp.com?
- How many web servers?
- How many mail servers?
- How many name servers?
- IP range/netblocks?
- Location(s)?
- Usernames, phone numbers, email addresses?

Carnal Ownage

11/10/94
Classified by [redacted] b7c
Declassify on: OADR

New School?

- New School, just a “new” way of looking at Information Gathering, less just discovering network blocks with whois and more take a “full spectrum” look at your target.
- OSINT, Open Source Intelligence
  - Out on the net for everyone to find, if you know what to look for
  - Domain Names
  - Files containing useful information
  - Email addresses
  - Website Source

Carnal Ownage

11/10/94
Classified by [redacted] b7c
Declassify on: OADR

OSINT

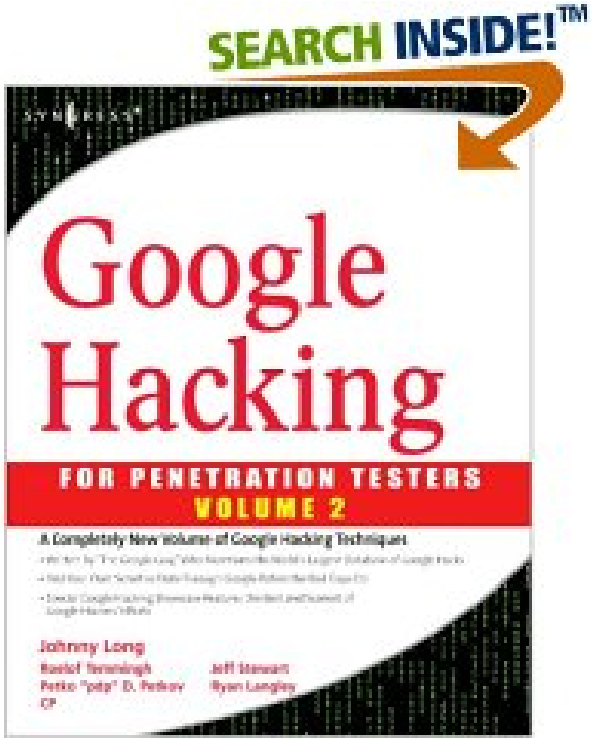
- Generally no direct contact with victim's servers OR no non-standard traffic directed toward victim
- End Result?
  - Organization's net blocks, external servers IPs and domain names, internal IP ranges, emails to send phishing attacks to, phone numbers to call, trust relationships with other organizations, & other relevant information for your audit and hopefully identifying exploitable flaws in the target's network

Carnal Ownage

11/10/94
Classified by [redacted] b7c
Declassify on: OADR

Isn't that what Google is for?

- Yeah kinda, Google-fu is important but we’re not going to talk much about Google hacking, go read the book.



Carnal Ownage

11/10/94
Classified by [redacted] b7c
Declassify on: OADR

Verify Web Presence

BayTSP - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://baytsp.com/

media sentry

The Ethical Hacker... https://www.googl...

track. secure. protect.

Solutions | Industry Focus | Press Room | About Us

SOLUTIONS FOR
DIGITAL RIGHTS HOLDERS

Internet Partners | **Client** Solutions | **Legal & Law** Enforcement

Latest News

Nikkei Electronics, 8/19/08: BayTSP offers service that monitors one million minutes of online video daily for copyright infringement, covering the top 12 video sharing sites.

MarketWatch, 8/18/08: BayTSP Content Authentication Platform increases capacity;

Movies	Secure your latest releases from pirate distribution with BayTSP.
Television	Millions will illegally upload your latest and greatest in television. Protect your IP.
Music	We provide the services to stop the distribution of your music.
Software	Software applications are downloaded illegally every second. Protect your profits.
Publishing	Scanned books, ebooks, and audio books are being downloaded everyday.
	Demand for the latest in

Received a take down notice from us?
Click here »

What we do at BayTSP
"Tracking-Security-Protection" for your digital assets.

Read the 2007 Internet Piracy Review
Read now »

Request A Demo

Carnal Ownage

Classified by [redacted] b7c
Reclassify on: OADR

Verify Web Presence

BayTSP is an innovator in digital copyright, image, trademark, music and text protection. Located in the heart of Silicon Valley, BayTSP offers a revolutionary way for digital content owners to track down their valuable online property, in order to effectively deter its theft and misuse.

http://www.aboutus.org/Baytsp.com

Carnal Ownage

11/10/94
Classified by [redacted] b7c
Declassify on: OADR

OSINT: Information Gathering & Domain Name Search

- Whois info, NS & AS Reports
- Search using target domain name
  - Target.com
  - and subdomain name
    - Vulnerable.target.com
- Who's handling mail, DNS, net blocks, web hosting, etc

Carnal Ownage

11/10/94
Classified by [redacted] b7c
Declassify on: OADR

OSINT: Information Gathering & Key Words

- Use that google-fu!
  - Password
  - Login
  - Target specific key words
  - Database/Secret/yak yak
  - Google dorks
  - Use SEAT/Goolag to audit a specific domain

Carnal Ownage

11/10/94
Classified by [redacted] b7c
Declassify on: OADR

OSINT: Information Gathering & File Search

- We're Looking for
  - Network diagrams (.vsd, .jpg, .gif)
  - Databases (.mdb)
  - Papers & documents (.doc, .pdf, .sdw)
  - Presentations (.ppt, .odp)
  - Spreadsheets (.xls, .ods, .sdc)
  - Configuration files (.txt, .rft)
- Thanks metagoofil!

Carnal Ownage

11/10/94
Classified by [redacted] b7c
Declassify on: OADR

OSINT: Information Gathering & Email addresses

- Information Gathering & Email addresses
  - Email Harvesting scripts and frameworks
- Information Gathering & Cached Data/Links
  - Archive.org, waybackmachine, Google
- Information Gathering & Source Code
  - Spider the site, look at html source and comments, file paths, file names, scripts used on the site

Carnal Ownage

11/10/94
Classified by [redacted] b7c
Declassify on: OADR

Tools of the Trade

Some, not all, plenty of others

Tools grouped by category and less by an actual order of doing things or methodology

Carnal Ownage

11/10/94
Classified by [redacted] b7c
Declassify on: OADR

Fierce DNS

- http://ha.ckers.org/fierce/
- By Rsnake from ha.ckers.org
- “It is meant specifically to locate likely targets both inside and outside a corporate network.”
- Tries your standard DNS tricks but also does some bruteforcing of domain names and tries to throw some intelligence into the searches.
- Bruteforce only as good as your wordlist.

Carnal Ownage

11/10/94
Classified by [redacted] b7c
Declassify on: OADR

Fierce DNS

- First it queries your DNS for the DNS servers of the target. It then switches to using the target's DNS server.
- Fierce then attempts to dump the SOA records for the domain in the very slim hope that the DNS server that your target uses may be misconfigured (attempts a zone transfer).*
- Once that fails (because it almost always will) it attempts to "guess" names that are common amongst a lot of different companies (hosts file).

Carnal Ownage

11/10/94
Classified by [redacted] b7c
Declassify on: OADR

Fierce DNS

- Next, if it finds anything on any IP address it will scan up and down a set amount looking for anything else with the same domain name in it using reverse lookups .
- If it finds anything on any of those it will recursively scan until it doesn't find any more.

Carnal Ownage

11/10/94
Classified by [redacted] b7c
Declassify on: OADR

Fierce DNS

```
cg@WPAD:~/evil/enumeration/dns/fierceDNS$ perl fierce.pl -dns baytsp.com
DNS Servers for baytsp.com:
        ns1.baytsp.net
        ns13.zoneedit.com
        ns2.baytsp.net

Trying zone transfer first...
        Testing 216.133.204.226
                Request timed out or transfer not allowed.
        Testing 66.223.40.121
                Request timed out or transfer not allowed.
        Testing 216.132.49.229
                Request timed out or transfer not allowed.

Unsuccessful in zone transfer (it was worth a shot)
Okay, trying the good old fashioned way... brute force

Checking for wildcard DNS...
Nope. Good.
Now performing 3149 test(s)...
216.133.204.235 dmz.baytsp.com
216.133.204.231 bayreports.baytsp.com
216.133.204.229 ftp.baytsp.com
216.133.204.224 dmz.baytsp.com
216.133.204.225 baytsp-gw.baytsp.com
216.133.204.232 cat-3000.baytsp.com
216.133.204.233 cims4.baytsp.com
216.133.204.234 dmz.baytsp.com
216.133.204.236 dmz.baytsp.com
216.133.204.239 dmz.baytsp.com
216.133.204.240 tc2.baytsp.com
216.133.204.241 dmz.baytsp.com
```

Carnal Ownage

11/10/94
Classified by [redacted] b7c
Declassify on: OADR

Fierce DNS

```
216.133.204.246 dmz.baytsp.com
216.133.204.247 dmz.baytsp.com
216.133.204.248 dmz.baytsp.com
216.133.204.249 dmz.baytsp.com
216.133.204.250 dmz.baytsp.com
216.133.204.251 dmz.baytsp.com
216.133.204.252 dmz.baytsp.com
216.133.204.253 dmz.baytsp.com
216.133.204.254 dmz.baytsp.com
216.133.204.255 dmz.baytsp.com
216.133.204.240 demo.baytsp.com
216.133.204.229 dl.baytsp.com
216.133.204.227 mail.baytsp.com
216.133.221.24  pop.baytsp.com
216.132.49.228  vpn.baytsp.com
206.135.194.198 w3.baytsp.com
216.133.221.15  webmail.baytsp.com
68.178.254.204  www.baytsp.com
68.178.254.204  .baytsp.com
```

```
Subnets found (may want to probe here using nmap or unicornscan):
        206.135.194.0-255 : 1 hostnames found.
        216.132.49.0-255 : 1 hostnames found.
        216.133.204.0-255 : 29 hostnames found.
        216.133.221.0-255 : 2 hostnames found.
        68.178.254.0-255 : 2 hostnames found.

Done with Fierce scan: http://ha.ckers.org/fierce/
Found 35 entries.
```

```
Have a nice day.
```

Carnal Ownage

Classified by [redacted] b7c
Declassify on: 20[illegible]

Search Engine Tools

Carnal Ownage

11/10/94
Classified by [redacted] b7c
Declassify on: OADR

SEAT (Search Engine Assessment Tool)

- By Midnight Research Labs
- http://midnightresearch.com/projects/search-engine-assessment-tool/
- "SEAT uses information stored in search engine databases, cache repositories, and other public resources to scan a site for potential vulnerabilities. It's multi-threaded, multi-database, and multi-search-engine capabilities permit easy navigation through vast amounts of information with a goal of system security assessment."
- Think automated GHDB on steriods ☺

Carnal Ownage

11/10/94
Classified by [redacted] b7c
Declassify on: OADR

SEAT (Search Engine Assessment Tool)

SEAT: Search Engine Assessment Tool

.:: Preparation ::. | .:: Execution ::. | .:: Analysis ::.

File Targets Queries Help

baytsp.com

Targets

- [x] baytsp.com

Queries

- [x] inurl:ospfd.conf intext:password -sample -test -tutorial -download
- [x] intitle:"Welcome Site/User Administrator" "Please
- [x] inurl:"nph-proxy.cgi" "Start browsing through this CGI-based proxy"
- [x] inurl:ipsec.conf -intitle:manpage
- [x] intitle:"lantronix web-manager"
- [x] Admin intitle:"eZ publish administration"
- [x] intitle:index.of haccess.ctl
- [x] inurl:"/becommunity/community/index.php?pageurl="
- [x] "Web Control Panel" "Enter your password here"

Description

Carnal Ownage

Classified by [redacted] b7c
Reclassify on: OADR

SEAT (Search Engine Assessment Tool)

SEAT: Search Engine Assessment Tool

.:: Preparation ::. | .:: Execution ::. | .:: Analysis ::.

File Targets Queries Search Engines Mined Help

Targets	Queries	Search Engines
☑ baytsp.com	☑ inurl:inurl:ipsec.secrets -history -bugs	☑ AltaVista
	☑ index.of.secure	☑ AllTheWeb

Mined	Results
	http://av.rds.yahoo.com/_ylt=A0geunb0_N1IhBwBNypVDqMX;_ylu
	http://av.rds.yahoo.com/_ylt=A0geunb0_N1IhBwBNipVDqMX;_ylu=
	http://av.rds.yahoo.com/_ylt=A0geunbGBd5IciABM0ZVDqMX;_ylu=

Statistics

Hits: 4
Mined: 0
Results: 3

Carnal Ownage

Classified by [redacted] b7c
Declassify on: 20[redacted]

Goolag

- Cult of Dead Cow's Goolag
- http://www.goolag.org/download.html

GoolagScanner Beta - (1418 dorks loaded)

File Edit Scan Tools Help

Available Dorks

- Dorks
  - Advisories and Vulnerabilities (216)
  - Error Messages (68)
  - Files containing juicy info (228)
  - Files containing passwords (137)
  - Files containing usernames (15)
  - Footholds (21)
  - Pages containing login portals (232)
  - Pages containing network or vulnerability data (59)
  - Sensitive Directories (60)
  - Sensitive Online Shopping Info (9)
  - Various Online Devices (202)
  - Vulnerable Files (54)
  - Vulnerable Servers (46)
  - Web Server Detection (71)

Host: nyp.org Scan Stop

Dork Info

"Powered by UPB" (b 1.0)|(1.0 final)|(Public Beta 1.0b)

"Powered by UPB" (b 1.0)|(1.0 final)|(Public Beta 1.0b)

dork: "Powered by UPB" (b 1.0)|(1.0 final)|(Public Beta 1.0b)

this is a very old vulnerability discovered by Xanthic, can't find it in GHDB
and I am surprised of how it still works...

Results

Status	Dork	URL found
Scan...	"Powered by PHP Advanced ...	...
Scan...	"powered by php icalendar" -i...	...
Scan...	"powered by php photo album...	...
Scan...	"powered by PhpBB 2.0.15" -...	...
Scan...	"Powered By phpCOIN 1.2.2"	...
Scan...	"Powered by PHP-Fusion v6....	...
Scan...	"powered by phplist" | inurl:"lis...	...
Blocked	"Powered by PowerPortal v1.3"	http://sorry.google.com/sorry/?continue=http://www.google.com/search?q=%2
Scan...	"powered by pppblog v 0.3.(.)"	...
Scan...	"powered by runcms" -runcms...	...
Scan...	"powered by sblog" +"version...	...
Scan...	"Powered by sendcard - an a...	...
Scan...	"Powered by Simplog"	...
Scan...	"powered by sphider" -exploit ...	...
Scan...	"powered by ubbthreads"	...
Scan...	"Powered by UPB" (b 1.0)|(1....	...

Carnal Ownage

Classified by [redacted] b7c
Reclassify on: OADR

Email Harvesting

Carnal Ownage

11/10/94
Classified by [redacted] b7c
Declassify on: OADR

Google Mail Harvesters

- Goog-mail.py
- theHarvester.py
- There are plenty others
- Consider changing the regex to search for different @ variations: [at] <at> (at)

Carnal Ownage

11/10/94
Classified by [redacted] b7c
Declassify on: OADR

Google Mail Harvesters

- Goog-mail.py

```
cg@WPAD:~/evil/enumeration/google$ python goog-mail.py baytsp.com


++++++++++++++++++++++++++++++++++++++++++++++++++++++
+ Google Web & Group Results:
++++++++++++++++++++++++++++++++++++++++++++++++++++++
```

```
copyright-compliance@baytsp.com
VIACOM@baytsp.com
info@baytsp.com
se...@baytsp.com
ellio...@baytsp.com
...paramount-pictures@baytsp.com
jimg@baytsp.com
andr...@baytsp.com
eve...@baytsp.com
YaKdnWAJN8-V-8vdRVn...@baytsp.com
seanr@baytsp.com
ma...@baytsp.com
compliance@baytsp.com
```

Carnal Ownage

Classified by [redacted] b7c
Declassify on: 20[illegible]

Google Mail Harvesters

- theHarvester.py
  - http://www.edge-security.com/theHarvester.php

```
cg@WPAD:~/evil/enumeration/google/theHarvester$ python theHarvester.py -d baytsp
.com -l 1000 -b google

****************************************
*TheHarvester Ver. 1.4                 *
*Coded by laramies                     *
*Edge-Security Research                *
*cmartorella@edge-security.com         *
****************************************


Searching for baytsp.com in google :
=========================================

Total results:  4410
Limit:  1000
Searching results: 0
Searching results: 100
Searching results: 200
```

Carnal Ownage

11/10/94
Classified by [redacted] b7c
Declassify on: OADR

Google Mail Harvesters

```
encontreGoogleharvester results:

marki@baytsp.com
evelyn@baytsp.com
VIACOM@baytsp.com
compliance@baytsp.com
investor@baytsp.com
dmca@baytsp.com
andreac@baytsp.com
copyright-compliance@baytsp.com
elliottk@baytsp.com
W_6dnX21wqTwt8_dRVn-hQ@baytsp.com
seanr@baytsp.com
noc@baytsp.com
paramount-pictures@baytsp.com
info@baytsp.com
BoGdnd2cesf37x7eRVn-tA@baytsp.com
baytsp.com
QZOdnYUwQpCYmPPd4p2dnA@baytsp.com
...paramount-pictures@baytsp.com
jimg@baytsp.com
ktWdnQ9AD6NnUOHeRVn-pQ@baytsp.com
Paramount.comlawrencel@baytsp.com
steves@baytsp.com
sarahb@baytsp.com
tracieg@baytsp.com
Marki@baytsp.com

Total accounts: 25
```

b7c

Document Metadata Extraction

Carnal Ownage

11/10/94
Classified by [redacted] b7c
Declassify on: OADR

Metagoofil

- Meta-what???
- MetaGoofil - Metadata analyzer, information gathering tool.
- Created by Christian Martorella of Edge Security.
- http://www.edge-security.com/metagoofil.php
- “Metagoofil is an information gathering tool designed for extracting metadata of public documents (pdf,doc,xls,ppt,odp,ods) available in the target/victim websites.

Carnal Ownage

11/10/94
Classified by [redacted] b7c
Declassify on: OADR

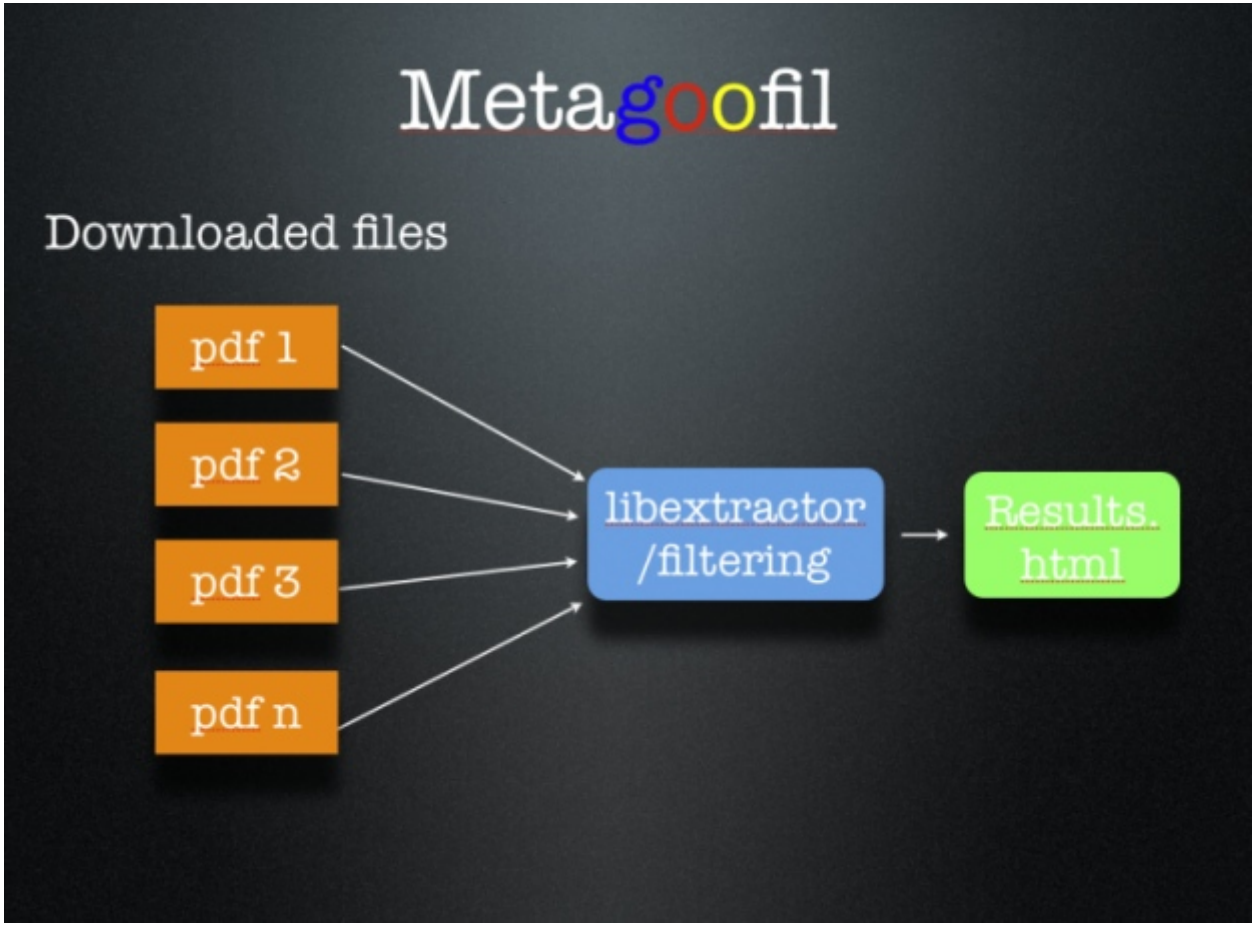
Metagoofil

- “It will generate a html page with the results of the metadata extracted, plus a list of **potential usernames** and path disclosure, can be useful for preparing a **bruteforce attack** on open services like ftp, pop3,web applications, vpn, etc.”

Carnal Ownage

11/10/94
Classified by [redacted] b7c
Declassify on: OADR

Metagoofil



Carnal Ownage

11/10/94
Classified by [redacted] b7c
Declassify on: OADR

Metagoofil

```
cg@WPAD:~/evil/info-gathering/metagoofil/metagoofil-1.4a$ python metagoofil.py -
d baytsp.com -l 1000 -f all -o baytsp-all.html -t baysp-files

*************************************
*MetaGooFil Ver. 1.4a               *
*Coded by Christian Martorella      *
*Edge-Security Research             *
*cmartorella@edge-security.com      *
*************************************


[+] Command extract found, proceeding with leeching
[+] Searching in baytsp.com for: pdf
[+] Total results in google: 3
[+] Limit:  3
[+] Searching results: 0
        [ 1/3 ] http://www.baytsp.com/pressroom/BayTSNTTpressrelease.pdf
        [ 2/3 ] http://www.baytsp.com/marketing/CAP_Datasheet.pdf
        [ 3/3 ] http://www.baytsp.com/pdf/SampleNotices2007.pdf
[+] Searching in baytsp.com for: doc
[+] Total results in google: 0
[+] Searching in baytsp.com for: xls
[+] Total results in google: 0
[+] Searching in baytsp.com for: ppt
```

Carnal Ownage

11/10/94
Classified by [redacted] b7c
Declassify on: OADR

Metagoofil

Total authors found (potential users):

```
QuarkXPress(R) 7.01
QuarkXPress(tm) 6.5
Acrobat PDFMaker 5.0 for Word
PSCRIPT.DRV Version 4.0
QuarkXPress(R) 7.0
Safenet Inc.
Tim Wheatcroft
jtabor
Mykotronx
JTABOR
JT
royals
LVXN
Grace
Season Ji
Michael
mshi
Mary Ann Burns
maburns
nnamazi
Dick Dienna
Melanie Maclin
Andy Gromada
Rwang
Andy Wang
Royals Wang
Cheryl Lai
```

Carnal Ownage

11/10/94
Classified by [redacted] b7c
Declassify on: OADR

Metagoofil

Local copy Open

Important metadata:

```
mimetype - application/msword
language - U.S. English
paragraph count - 7
line count - 28
last saved by - Dick Dienna
character count - 3363
template - Normal.dot
creation date - 2008-02-13T18:26:00Z
title - Company Name
word count - 590
page count - 1
creator - Melanie Maclin
date - 2008-02-13T18:26:00Z
generator - Microsoft Office Word
```

Carnal Ownage

11/10/94
Classified by [redacted] b7c
Declassify on: OADR

Why Metadata?

- Metadata can:
- Reveal the creator of a document, and even a possible **network username** or derive naming convention.
- Reveal the application that created the document.
- Reveal the **version** of the software that created the document.
- Reveal creation date. Document was created recently with vulnerable version.
- **We now have possible usernames, applications used by those individuals and the software versions. Now we can deliver a directed client side attack for something installed in the enterprise.**

Carnal Ownage

11/10/94
Classified by [redacted] b7c
Declassify on: OADR

Why Metadata?

- Also try running your word documents through The Revisionist by Michael Zalewski
- http://lcamtuf.coredump.cx/strikeout/
- The Revisionist can pull out deleted comments and text if the “track changes” had been used and dump the document with deleted text to an HTML file.

Carnal Ownage

11/10/94
Classified by [redacted] b7c
Declassify on: OADR

On-line Tools

Carnal Ownage

11/10/94
Classified by [redacted] b7c
Declassify on: OADR

ServerSniff.net

- http://serversniff.net/
- NS/MX Reports
- AS Reports
- Subdomains
- TLDs
- Hostnames on an IP
- Domains on webserver
- Web Tools
- HTML Comments
- HTML Code
- SSL Certificate Info
- Links within page
- Web Server Headers

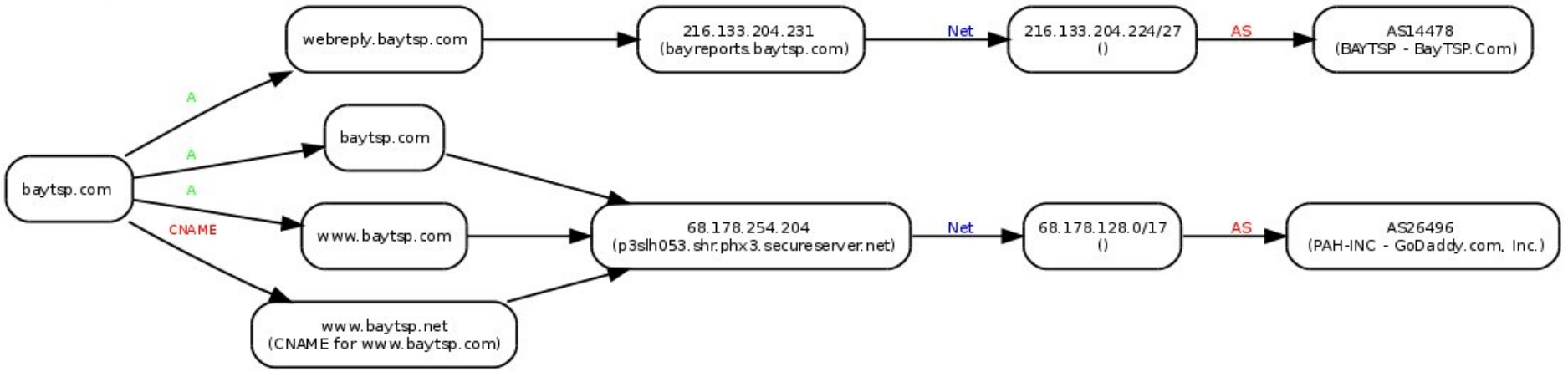
Carnal Ownage

11/10/94
Classified by [redacted] b7c
Declassify on: OADR

ServerSniff.net

- http://serversniff.net/

Hostinfo (baytsp.com):



This Domain belongs to top-leveldomain **com**.

Registration-Data for this domain may be found on whois-server: **whois.internic.net** You might query whois-information for this domain here

You might also be interested in a DNS-Report for baytsp.com

You might also be interested in these AS-Reports:

- AS-Report for AS26496
- AS-Report for AS14478

You might also be interested in these Domain- and DNS-Reports:

- Domain-Report for baytsp.com | DNS-Report for baytsp.com

Carnal Ownage

11/10/94
Classified by [redacted] b7c
Declassify on: OADR

ServerSniff.net

Domains on Nameserver

Shows other domains a nameserver is authortitative for.
Please be patient - especially on huge nameserver this might take a while...

Please enter a domainname or nameserver to lookup: baytsp.com

Optional: Show only Domainnames containing:

Query Catalog

baytsp.com has more than one nameserver, which is good! We tried to check the primary NS (**ns2.baytsp.net**).
Use these links to find out sister-domains hosted on the domain's other nameservers:

-->ns2.baytsp.net
-->ns13.zoneedit.com
-->ns1.baytsp.net

Checking for domains hosted on ns2.baytsp.net.... be patient...

1 [nscat] [dnr] [nsr] **acuityventures.com** www
2 [nscat] [dnr] [nsr] **copyrightguardian.net** www
3 [nscat] [dnr] [nsr] **assetscore.com** www
4 [nscat] [dnr] [nsr] **baytsp.com** www
5 [nscat] [dnr] [nsr] **copyright-compliance.com** www
6 [nscat] [dnr] [nsr] **copyrightspider.net** www
7 [nscat] [dnr] [nsr] **assetscore.net** www
8 [nscat] [dnr] [nsr] **ee-world.com** www
9 [nscat] [dnr] [nsr] **baytsp.net** www
10 [nscat] [dnr] [nsr] **copyrightspider.com** www
11 [nscat] [dnr] [nsr] **copyright-guardian.com** www
12 [nscat] [dnr] [nsr] **trademarkspider.com** www

Add this NS to our Research-Query (might take a few hours until results are visible!)

Carnal Ownage

11/10/94
Classified by [redacted] b7c
Declassify on: OADR

DomainTools.com

- http://www.domaintools.com/

DomainTools

Wildcard search of all current/deleted/expired whois domains.
Domain Suggestions Engine serves over 10 Billion suggestions a year.

DomainTools Live Auction closing NOW! Bid Now!

Whois | Suggestions | Domain Search | At Auction | For Sale | DNS Tools

Whois Lookup: Search

Domain Roundtable Conference "Welcome to The New Domain Industry"

Do you own high-quality generic domains? List them in the April 21st DomainTools Live Auction at the Domain Roundtable Conference in San Francisco. Want to ensure your domain is listed? Register now for the conference - every attendee has a guaranteed-acceptance slot of one domain in the Live Auction.

Submit a Domain - Sign up for the Roundtable.

Our Latest Blog Post: DomainTools Live Auction - 9 comments

- More Tools and Services — Complete collection of all tools.
- Domain History — Whois history database.
- Mark Alert — Alerts when a domain uses my trademark.
- Live reports on web hosting companies — Detailed uptime reports on providers
- Name Intelligence Awards — The 2007 awards are out, see who won.
- Reverse IP — Patent pending reverse IP search.
- DNS Tools — DNS stuff, whois, traceroute, and ping.
- Members Area — Modify account settings and options.
- Name Server Spy — Follow the transfers of a name server.
- Domain Monitor — Free tool to monitor all my domains.
- Typo Generator — Find Domain Typos on any Domain.
- Whois Applications and Toolbars — Google toolbar add-on and other applications.

Carnal Ownage

11/10/94
Classified by [redacted] b7c
Declassify on: OADR

DomainTools.com

http://whois.domaintools.com/baytsp.com

The Ethical Hacker... https://www.googl...

baytsp.com | Baytsp.com - Bay tsp

Registrar Status:	clientDeleteProhibited
Registrar Status:	clientRenewProhibited
Registrar Status:	clientTransferProhibited
Registrar Status:	clientUpdateProhibited
Name Server:	NS1.BAYTSP.NET (has 33 domains)
Name Server:	NS13.ZONEEDIT.COM (has 186,668 domains)
Name Server:	NS2.BAYTSP.NET (has 33 domains)
Whois Server:	whois.godaddy.com

Server Data

IP Address:	68.178.254.204 W R P D T
IP Location	- Arizona - Scottsdale - Godaddy.com Inc
Response Code:	200
Domain Status:	Registered And Active Website

DomainTools Exclusive

Registrant Search:	"Domains by Proxy, Inc." was found in about 7,226,158 other domains
Email Search:	baytsp.com@domainsbyproxy.com is associated with about 1 domains
Registrar History:	1 registrar
NS History:	3 changes on 4 unique name servers over 6 years.
IP History:	4 changes on 4 unique name servers over 4 years.
Whois History:	141 records have been archived since 2001-12-31.
Reverse IP:	3,482 other sites hosted on this server.
Monitor Domain:	Set Free Alerts on baytsp.com

Done

Carnal Ownage

Classified by [redacted] b7c

Reclassify on: OADR

DomainTools.com

- Hosting history: Track previous web hosts and hosting providers
- Domain history: viewing contact information before it was privatized
- Registrant Alert: Find new registrations by someone
- Registrant Search: Find all domains someone owns
- Links to Wikipedia references
- Best/Most tools on site are for pay :-(

Carnal Ownage

11/10/94
Classified by [redacted] b7c
Declassify on: OADR

CentralOps.net

- http://centralops.net/co/

CentralOps.net Advanced online Internet utilities

Utilities

Domain Dossier
Domain Check
Email Dossier
Browser Mirror

Ping
Traceroute
NsLookup
AutoWhois
TcpQuery
AnalyzePath

Hosting metrics

Shared hosting
VPS hosting
Email hosting
Dedicated hosting

Domain Dossier Investigate domains and IP addresses

domain or IP address baytsp.com

☑ domain whois record ☑ DNS records ☑ traceroute

☑ network whois record ☑ service scan go

user: 12.187.158.130 [anonymous] 49/50
log in | get account

CentralOps.net

New: See daily test results of online hosting providers.

Address lookup

canonical name **baytsp.com.**

aliases

addresses **68.178.254.204**

Domain Whois record

Queried **whois.internic.net** with "**dom baytsp.com**"...

```
Whois Server Version 2.0
```

b7c

CentralOps.net

Utilities

- Domain Dossier
- Domain Check
- Email Dossier
- Browser Mirror
- Ping
- Traceroute
- NsLookup
- AutoWhois
- TcpQuery
- AnalyzePath

Hosting metrics

- Shared hosting
- VPS hosting
- Email hosting
- Dedicated hosting

DNS records

name	class	type	data		time to live
baytsp.com	IN	SOA	server:	ns1.baytsp.net	86400s (1.00:00:00)
			email:	noc.baytsp.net	
			serial:	2008090901	
			refresh:	28800	
			retry:	14400	
			expire:	3600000	
			minimum ttl:	86400	
baytsp.com	IN	TXT	v=spf1 mx include:baytsp.net -all		86400s (1.00:00:00)
baytsp.com	IN	MX	preference:	10	86400s (1.00:00:00)
			exchange:	mail.baytsp.net	
baytsp.com	IN	A	68.178.254.204		86400s (1.00:00:00)
baytsp.com	IN	NS	ns13.zoneedit.com		86400s (1.00:00:00)
baytsp.com	IN	NS	ns1.baytsp.net		86400s (1.00:00:00)
baytsp.com	IN	NS	ns2.baytsp.net		86400s (1.00:00:00)
204.254.178.68.in-addr.arpa	IN	PTR	p3slh053.shr.phx3.secureserver.net		3600s (01:00:00)

Carnal Ownage

11/10/94
Classified by [redacted] b7c
Declassify on: OADR

CentralOps.net

Utilities

- Domain Dossier
- Domain Check
- Email Dossier
- Browser Mirror
- Ping
- Traceroute
- NsLookup
- AutoWhois
- TcpQuery
- AnalyzePath

Hosting metrics

- Shared hosting
- VPS hosting
- Email hosting
- Dedicated hosting

11	27	27	27	208.109.112.142	ip-208-109-112-142.ip.secureserver.net
12	26	27	27	216.69.188.33	ip-216-69-188-33.ip.secureserver.net
13	27	27	27	68.178.254.204	p3slh053.shr.phx3.secureserver.net

Trace complete

Service scan

FTP - 21

```
220---------- Welcome to Pure-FTPd [privsep] [TLS] ----------
220-You are user number 4 of 50 allowed.
220-Local time is now 07:52. Server port: 21.
220-This is a private system - No anonymous login
220 You will be disconnected after 3 minutes of inactivity.
220 Logout.
```

SMTP - 25

```
Error: TimedOut
```

HTTP - 80

```
HTTP/1.1 200 OK
Date: Sat, 27 Sep 2008 14:53:01 GMT
Server: Apache
Connection: close
Content-Type: text/html
```

POP3 - 110

```
Error: TimedOut
```

IMAP - 143

```
Error: TimedOut
```

-- end --

URL for this output | return to CentralOps.net, a service of Hexillion

Carnal Ownage

11/10/94
Classified by [redacted] b7c
Declassify on: OADR

CentralOps.net

Utilities

- Domain Dossier
- Domain Check
- Email Dossier
- Browser Mirror
- Ping
- Traceroute
- NsLookup
- AutoWhois
- TcpQuery
- AnalyzePath

Hosting metrics

- Shared hosting
- VPS hosting
- Email hosting
- Dedicated hosting

SMTP session

```
[Contacting mail.baytsp.net [216.133.204.227]...]
[Connected]
220 mail.baytsp.net ESMTP XWall v3.42
EHLO hexillion.com
250-mail.baytsp.net
250-ENHANCEDSTATUSCODES
250-ETRN
250-DSN
250-8BITMIME
250-PRIORITY
250-CHUNKING
250-SIZE
250-XBDATA
250 XXWALL30
VRFY jimg
553 User ambiguous
RSET
250 2.0.0 ok
EXPN jimg
502 5.5.1 command not implemented
RSET
250 2.0.0 ok
MAIL FROM:<HexValidEmail@hexillion.com>
250 2.1.0 originator <HexValidEmail@hexillion.com> ok
RCPT TO:<jimg@baytsp.com>
451 4.7.1 message delayed, see http://www.greylisting.org ; Please try again later
[Unfavorable reply code, cannot continue]
RSET
250 2.0.0 ok
QUIT
```

Carnal Ownage

11/10/94
Classified by [redacted] b7c
Declassify on: OADR

CentralOps.net

- Email Verification (failure)

CentralOps.net Advanced online Internet utilities

Utilities
- Domain Dossier
- Domain Check
- Email Dossier
- Browser Mirror
- Ping
- Traceroute
- NsLookup
- AutoWhois
- TcpQuery
- AnalyzePath

Hosting metrics
- Shared hosting
- VPS hosting
- Email hosting
- Dedicated hosting

Email Dossier Investigate email addresses

email address 20sws9001@nyp.org go

try vrfy and expn

source code: view | download CentralOps.net

Validating **20sws9001@nyp.org**...

Validation results

confidence rating: **0 - Bad address**
error : **Recipient rejected**
canonical address: **<20sws9001@nyp.org>**

MX records

preference	exchange	IP address (if included)
10	mail-gw2.med.cornell.edu	
20	mail-gw1.med.cornell.edu	
30	smtp-gw2.med.cornell.edu	

SMTP session

```
[Resolving mail-gw2.med.cornell.edu...]
[Contacting mail-gw2.med.cornell.edu [140.251.3.2]...]
[Connected]
220 mail-gw2.med.cornell.edu -- Server ESMTP (SMTP Server)
EHLO hexillion.com
250-mail-gw2.med.cornell.edu
250-8BITMIME
250-PIPELINING
250-CHUNKING
250-DSN
250-ENHANCEDSTATUSCODES
250-HELP
250-XLOOP AA7D71C0C3870C2D913E915653235725
250-ETRN
250-NO-SOLICITING
250 SIZE 102400000
VRFY 20sws9001
252 2.5.0 Possible local address <20sws9001@mail-gw2.med.cornell.edu>
RSET
250 2.5.0 Ok.
EXPN 20sws9001
550 5.7.2 EXPN command has been disabled.
RSET
250 2.5.0 Ok.
MAIL FROM:<HexValidEmail@hexillion.com>
250 2.5.0 Address Ok.
RCPT TO:<20sws9001@nyp.org>
550 5.1.1 unknown or illegal alias: 20sws9001@nyp.org
[Address has been rejected]
RSET
250 2.5.0 Ok.
```

Carnal Ownage

11/10/94 Classified by [redacted] b7c Declassify on: OADR

CentralOps.net

- Email Verification (success)

Email Dossier Investigate email addresses

email address nursingsce@nyp.org go

☑ try vrfy and expn

source code: view | download CentralOps.net

Validating **nursingsce@nyp.org**...

Validation results

confidence rating: **3 - SMTP**
The email address passed this level of validation without an error. However, it is not guaranteed to be a good address. more info

canonical address: **<nursingsce@nyp.org>**

MX records

preference	exchange	IP address (if included)
10	mail-gw2.med.cornell.edu	[140.251.3.2]
20	mail-gw1.med.cornell.edu	[140.251.3.44]
30	smtp-gw2.med.cornell.edu	[157.139.3.45]

SMTP session

```
[Contacting mail-gw2.med.cornell.edu [140.251.3.2]...]
[Connected]
220 mail-gw2.med.cornell.edu -- Server ESMTP (SMTP Server)
EHLO hexillion.com
250-mail-gw2.med.cornell.edu
250-8BITMIME
250-PIPELINING
250-CHUNKING
250-DSN
250-ENHANCEDSTATUSCODES
250-HELP
250-XLOOP AA7D71C0C3870C2D913E915653235725
250-ETRN
250-NO-SOLICITING
250 SIZE 102400000
VRFY nursingsce
252 2.5.0 Possible local address <nursingsce@mail-gw2.med.cornell.edu>
RSET
250 2.5.0 Ok.
EXPN nursingsce
550 5.7.2 EXPN command has been disabled.
RSET
250 2.5.0 Ok.
MAIL FROM:<HexValidEmail@hexillion.com>
250 2.5.0 Address Ok.
RCPT TO:<nursingsce@nyp.org>
250 2.1.5 nursingsce@nyp.org OK.
RSET
250 2.5.0 Ok.
QUIT
221 2.3.0 Bye received. Goodbye.
[Connection closed]
```

Carnal Ownage

11/10/94 Classified by [redacted] b7c
Declassify on: OADR

Clez.net

- http://clez.net/net

net.toolkit

index

net +
- .app
- .block
- .ping
- .ssl
- .tcp
- .traceroute
- .whois

string +

list +

mail +

web +

expand | collapse

net.app
what's up and running?

idn : 80 go Net Head protocol hint http

info

What's this?

Given you know an open TCP port at a host and want to know which application is waiting for connections.
In **net** mode, we try to find it out without knowing anything. It takes longer than **head**, a mode based on rough knowledge of the protocol.
Most information we gather here can be retrieved via telnet or nmap, but needs the outbound port on your client to be open.

Reason for building this service

I built this service because I occasionally appear to find myself in corporate networks not allowing me to probe any port I need.

Carnal Ownage

11/10/94
Classified by [redacted] b7c
Declassify on: OADR

Clez.net

- Query port and service scan information
- dns, ping, whois, ssl info, traceroutes
- email verification, open relay checking

net.toolkit

index

net +
- .app
- .block
- .dns
- .ping
- .ssl
- .tcp
- .traceroute
- .whois

string +

list +

mail +

web +

expand | collapse

ADD THIS

net.app
what's up and running?

idn www.baytsp.com : 80 >GO protocol hint none

info | scan result | port list (27)

Application detection

Application	Apache httpd
Protocol	**http**

HTTP HEAD Request

HTTP/1.1 200 OK

Date	Sat, 27 Sep 2008 16:20:14 GMT
Server	Apache
Connection	close
Content-Type	text/html

Elapsed time: **0.306** seconds.

Additional HTTP Methods

[redacted] b7c

Clez.net

- Email Verification

net.toolkit

index
net +
string +
list +
mail +
.rbl
.relay
.surbl
.vrfy
web +

expand | collapse

ADD THIS

mail.vrfy
Test if an email address could receive messages.

idn dmca@baytsp.com >GO smtp smtps all mx

info | vrfy result

```
basic tests:
        PASSED  syntax check
        PASSED  local part check
        PASSED  hostname is not an IDN
        PASSED  resolved hostname
        PASSED  well-known throwaway and example check
        PASSED  baytsp.com has 1 MX records set

mail exchanger mail.baytsp.net at priority 10
        PASSED  mail.baytsp.net resolves to 216.133.204.227
        PASSED  connected to mail.baytsp.net:25
        PASSED  got (E)SMTP greeter:                    220 mail.baytsp.net ESMTP XWall v3.42
        PASSED  mailbox verified by VRFY                252 Unable to VRFY user ( e.g. info is not local ), but will take message for this
        WARNING SMTPd does not support/denies EXPN      502 command not implemented
        PASSED  accepts test sender
        FAILED  mailbox unknown, mail would be rejected
```

mail verification finished, all checked mailservers rejected the recipient.

Carnal Ownage

11/10/94
Classified by [redacted] b7c
Declassify on: OADR

Clez.net

- Email Verification

net.toolkit

index
net +
string +
list +
mail +
.rbl
.relay
.surbl
.vrfy
web +

expand | collapse

ADD THIS

nursingsce@nyp.org >GO smtp smtps all mx

info | vrfy result

```
basic tests:
        PASSED  syntax check
        PASSED  local part check
        PASSED  hostname is not an IDN
        PASSED  resolved hostname
        PASSED  well-known throwaway and example check
        PASSED  nyp.org has 3 MX records set

mail exchanger mail-gw2.med.cornell.edu at priority 10
        PASSED  mail-gw2.med.cornell.edu resolves to 140.251.3.2
        PASSED  connected to mail-gw2.med.cornell.edu:25
        PASSED  got (E)SMTP greeter:                          220 mail-gw2.med.cornell.edu -- Server ESMTP (SMTP Server)
        PASSED  mailbox verified by VRFY                      252 2.5.0 Possible local address <nursingsce@nyp.org>
        WARNING EXPN is prohibited on this system             550 5.7.2 EXPN command has been disabled.
        PASSED  accepts test sender
        PASSED  accepts e-mails to nursingsce@nyp.org

mail exchanger mail-gw1.med.cornell.edu at priority 20
        PASSED  mail-gw1.med.cornell.edu resolves to 140.251.3.44
        PASSED  connected to mail-gw1.med.cornell.edu:25
        PASSED  got (E)SMTP greeter:                          220 mail-gw1.med.cornell.edu -- Server ESMTP (SMTP Server)
        PASSED  mailbox verified by VRFY                      252 2.5.0 Possible local address <nursingsce@nyp.org>
        WARNING EXPN is prohibited on this system             550 5.7.2 EXPN command has been disabled.
        PASSED  accepts test sender
        PASSED  accepts e-mails to nursingsce@nyp.org
```

Carnal Ownage

11/10/94
Classified by [redacted] b7c
Declassify on: OADR

Clez.net

- Email Verification

net.toolkit

index
net +
string +
list +
mail +
.rbl
.relay
.surbl
.vrfy
web +

expand | collapse

ADD THIS

mail.vrfy
Test if an email address could receive messages.

notthere@nyp.org >GO smtp smtps all mx

info | vrfy result

```
basic tests:
        PASSED  syntax check
        PASSED  local part check
        PASSED  hostname is not an IDN
        PASSED  resolved hostname
        PASSED  well-known throwaway and example check
        PASSED  nyp.org has 3 MX records set

mail exchanger mail-gw2.med.cornell.edu at priority 10
        PASSED  mail-gw2.med.cornell.edu resolves to 140.251.3.2
        PASSED  connected to mail-gw2.med.cornell.edu:25
        PASSED  got (E)SMTP greeter:                    220 mail-gw2.med.cornell.edu -- Server ESMTP (SMTP Server)
        PASSED  mailbox verified by VRFY                252 2.5.0 Possible local address <notthere@nyp.org>
        WARNING EXPN is prohibited on this system       550 5.7.2 EXPN command has been disabled.
        PASSED  accepts test sender
        FAILED  mailbox unknown, mail would be rejected

mail exchanger mail-gw1.med.cornell.edu at priority 20
        PASSED  mail-gw1.med.cornell.edu resolves to 140.251.3.44
        PASSED  connected to mail-gw1.med.cornell.edu:25
        PASSED  got (E)SMTP greeter:                    220 mail-gw1.med.cornell.edu -- Server ESMTP (SMTP Server)
        PASSED  mailbox verified by VRFY                252 2.5.0 Possible local address <notthere@nyp.org>
        WARNING EXPN is prohibited on this system       550 5.7.2 EXPN command has been disabled.
        PASSED  accepts test sender
        FAILED  mailbox unknown, mail would be rejected
```

Carnal Ownage

11/10/94
Classified by [redacted] b7c
Declassify on: OADR

Robtex

- http://www.robtex.com/ Similar to ServerSniff

baytsp.com

domain | graph | shared | whois | blacklists

baytsp.com is a domain controlled by three nameservers. All of them are on different IP networks. Incoming mail for baytsp.com is handled by one mailserver at baytsp.net. baytsp.com has one IP record. sfaa.us, chsm.net, dmsm.net, 33rx.info, acslc.net and at least 100 other hosts point to the same IP. gsr.se, dwdj.com, eews.com, cdbl.net, cfod.net and at least 100 other hosts share nameservers with this domain. baytsp.net, tronarx.net, assetscore.net, ladiesweekend.com, copyrightspider.net and at least seven other hosts share mailservers with this domain. 69-22-178-185.baytsp.com, 69-22-181-164.baytsp.com, 69-22-180-164.baytsp.com, 69-22-180-180.baytsp.com, 69-22-181-182.baytsp.com and at least 100 other hosts are subdomains to this hostname.

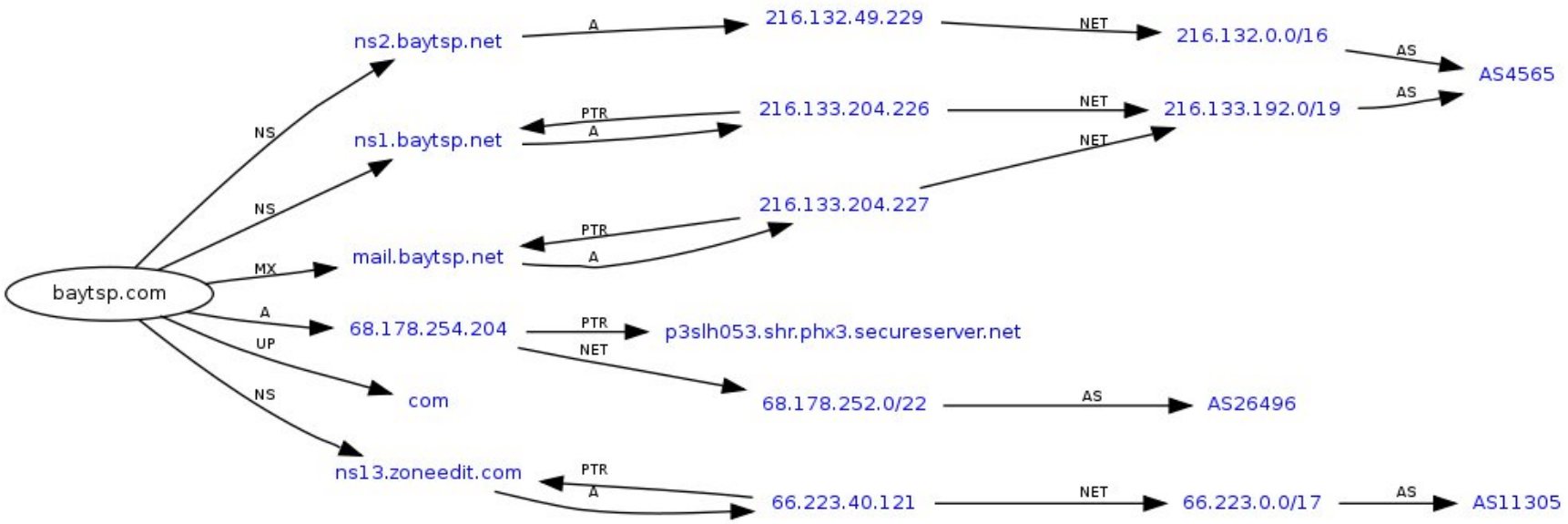
base	record	name	ip	reverse	route	as
baytsp.com	a		68.178.254.204 Apache	p3slh053.shr.phx3.secureserver.net	68.178.252.0/22	AS26496 PAH-INC Go Daddy Software, Inc.
	ns	ns13.zoneedit.com	66.223.40.121 dns	-	66.223.0.0/17 66.223.0.0~66.223.127.255	AS11305 INTERLAND-NET1 Interland Incorporated
		ns1.baytsp.net	216.133.204.226 dns		216.133.192.0/19 Megapath aggregate	AS4565 EPOCH Megapath Inc/Formerly Netifice Communications/Epoch Internet 555 Anton Blvd, 2nd Floor Costa Mesa, CA 92626 NOC: 1888 638 3696 or 1714 327 2000 nocops@netifice com Peering: @megapath com Megapath BGP customers may choose to effect our local preferen
		ns2.baytsp.net	216.132.49.229 dns		216.132.0.0/16 Megapath aggregate	
	mx	mail.baytsp.net	216.133.204.227 220 mail.baytsp.net		216.133.192.0/19 Megapath aggregate	

Carnal Ownage

11/10/94
Classified by [redacted] b7c
Declassify on: OADR

Robtex

net gtld-servers.net baytsp.net zoneedit.com phx3.secureserver.net shr.phx3.secureserver.net secureserver.net



hostnames sharing ip with a-records	hostnames beginning with baytsp	hostnames sharing ip indirectly via cnames	domains sharing mailservers	domains sharing nameservers	subdomains
1cialissource.net	baytsp.co.uk	www.hegstrom.com	assetscore.net	abeltek.com	*.baytsp.com
1cialisstop.net	baytsp.fe4-5.ar1.sfo2.infraswitch.r		baytsp.net	adsl2pluss.net	69-22-140-161.baytsp.co
1levitrasource.net	baytsp.net		copyright-compliance.com	aeonsystems.org	69-22-140-162.baytsp.co
1levitrastop.net			copyright-guardian.com	aimteam.com	69-22-140-163.baytsp.co
					69-22-140-164.baytsp.co

Carnal Ownage

11/10/94
Classified by [redacted] b7c
Declassify on: OADR

spoke.com

- Search for people locate their company
- Search for companies and retrieve names

People Search Results

Your Search: baytsp.com

Show Details | Save As... | Edit

28 total results

25 results per page | All dates (current jobs)

Add to SFA | Add to List | Add All to List | Export |

1 to 25 (of 28)

Name	Job Title		Company	Validated
Robert Sweeney	Chief Financial Officer	E-mail	Baytsp.Com Inc	6/2008
Mark Ishikawa	Chief Executive Officer	E-mail	Baytsp.Com Inc	6/2008
Leland Woo	Vp, Business Development *	E-mail	Baytsp.Com Inc *	6/2008
Richard Jorgensen	Director *	E-mail	Baytsp.Com Inc *	1/2008
Lawrence Low	Vp	E-mail	Baytsp.Com Inc	6/2008
Evelyn Espinosa	Chief Operating Officer Co-founder	E-mail	Baytsp.Com Inc	6/2008
John Salter	Vp, Product Development	E-mail	Baytsp.Com Inc	6/2008
Travis Hill	Vp, Engineering	E-mail	Baytsp.Com Inc	6/2008
Arielle Kim	Executive Administrator	E-mail	Baytsp.Com Inc	2/2005
Clifton Wong	Chief Financial Officer	E-mail	Baytsp.Com Inc	7/2007
Matt Sprague		E-mail	Baytsp.Com Inc	3/2007
Nicole Manske		E-mail	Baytsp.Com Inc	3/2008
Lloyd Payton		E-mail	Baytsp.Com Inc	2/2005

b7c

Carnal Ownage

Declassified by OADR

TouchGraph

- http://touchgraph.com
- “TouchGraph's powerful visualization solutions reveal relationships between people, organizations, and ideas.”
- Visually show the big picture on how things are tied together using Google results.

Carnal Ownage

11/10/94
Classified by [redacted] b7c
Declassify on: OADR

TouchGraph

http://www.touchgraph.com - TouchGraph Google Browser - Mozilla Firefox

Edit View Tools Display

Info Help

BayTSP

http://www.baytsp.com/

MarketWatch, 8/18/08: BayTSP Content Authentication Platform increases capacity; now scanning one million minutes of online video daily from user-generated ...

Filter

Show Hidden Name

	Name	URL	Sim#
	Glatt Plagiarism Program	plagiarism....	13
	Intellectual Property Ma...	innovation-...	10
	Envisional: FRAUD, COU...	envisional.c...	10
	BayTSP	baytsp.com	10
	Sprott Asset Management	sprott.com	1
	Plagiarism in Colleges i...	rbs2.com/...	1
	Olimpo Informatico :: In...	forum.zeus...	1
	CFL Software Developm...	copycatchg...	1
	AVG News	grisoft.com	1
	PuTTY Download Page	chiark.gree...	1
	Anti-Plagiarism Strategies	virtualsalt.c...	1
	JPlag	wwwipd.ira...	1
	CHAM	cham.org	1
	Plagiarism Detection	cs.berkeley...	1
	Welcome to West Asset ...	westassetm...	1
	Plagiarism Advisory Ser...	jiscpas.ac.uk	1
	BBC NEWS | Technology...	news.bbc.c...	1
	24 reasons why TV pir...	networks.si...	1
	The Chronicle: 5/17/2...	chronicle.c...	1
	The Intellectual Propert...	intelpropla...	1

Keywords or URL www.baytsp.com Edit Keep Hide Expand

Label Shows Title URL Text Over Icon Tools

Zoom: Spacing:

Carnal Ownage

11/10/94
Classified by [redacted] b7c
Declassify on: OADR

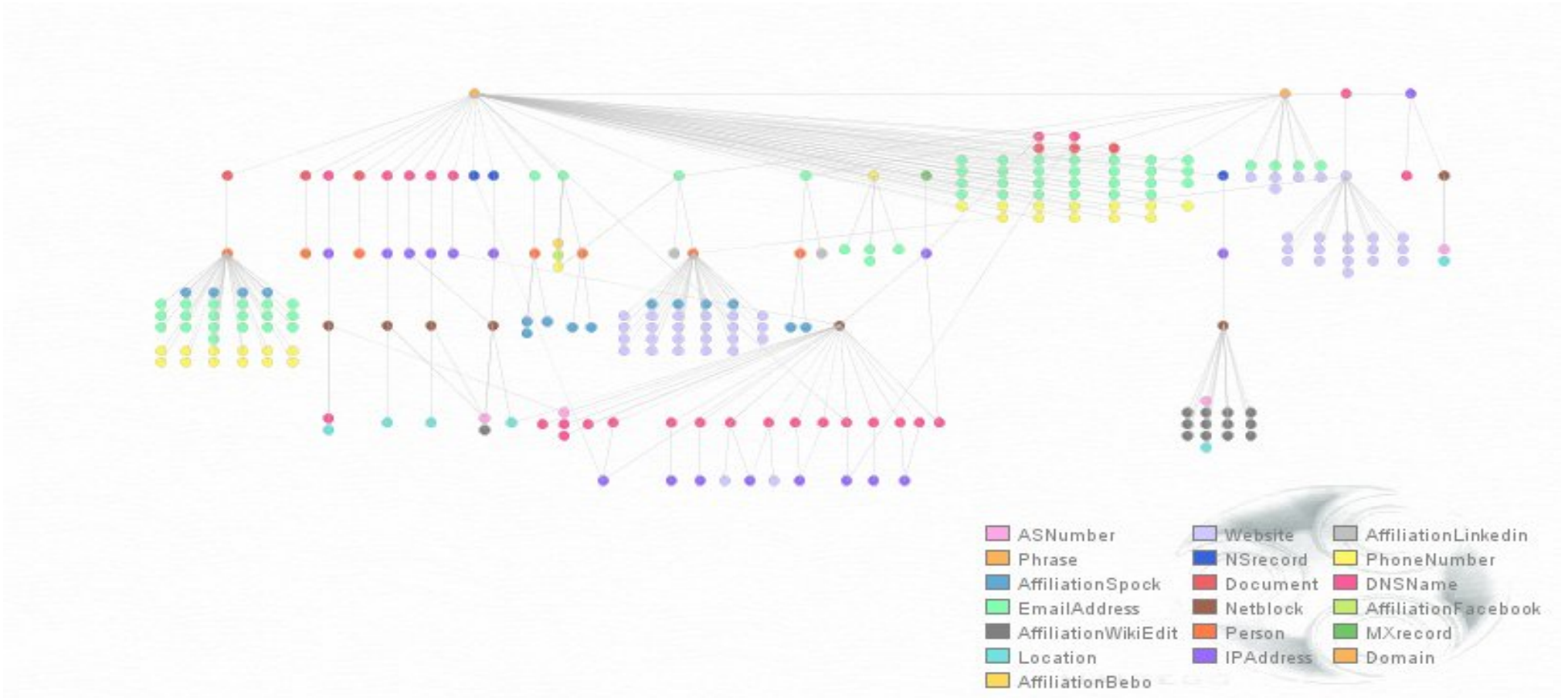
Tying it all together with Maltego

Carnal Ownage

11/10/94
Classified by [redacted] b7c
Declassify on: OADR

Maltego

- What does this tell me about our target domain?



Carnal Ownage

11/10/94
Classified by [redacted] b7c
Declassify on: OADR

Maltego

- **http://www.paterva.com/web2/Maltego/maltego.html**

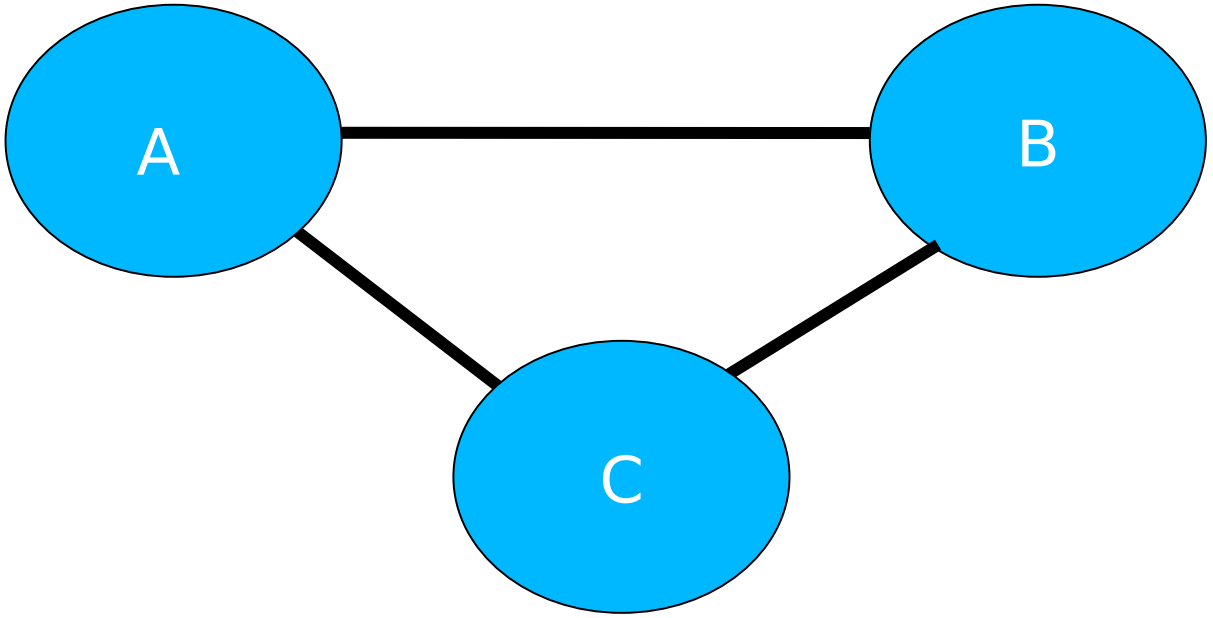
- By Roelof Temmingh from Paterva
- **<u>What is it?</u>**
- Maltego is a program that can be used to determine the relationships and real world links between:
  - People
  - Groups of people (social networks)
  - Companies
  - Organizations
  - Web sites
  - Internet infrastructure such as:
    - Domains
    - DNS names
    - Netblocks
    - IP addresses
  - Phrases
  - Affiliations
  - Documents and files
- All using open source intelligence (OSINT)

Carnal Ownage

11/10/94
Classified by [redacted] b7c
Declassify on: OADR

Maltego

- It would be good to learn or verify that A is related to B and they are both related to C, or…

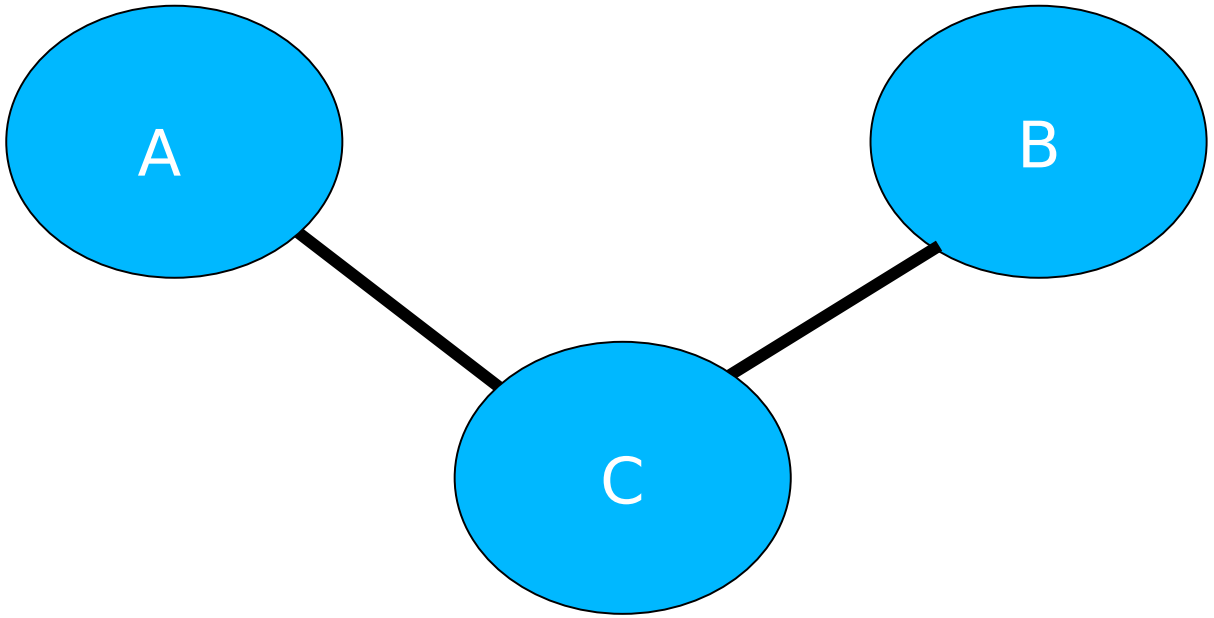


Carnal Ownage

11/10/94
Classified by [redacted] b7c
Declassify on: OADR

Maltego

- We can see that A and B are related **through** C

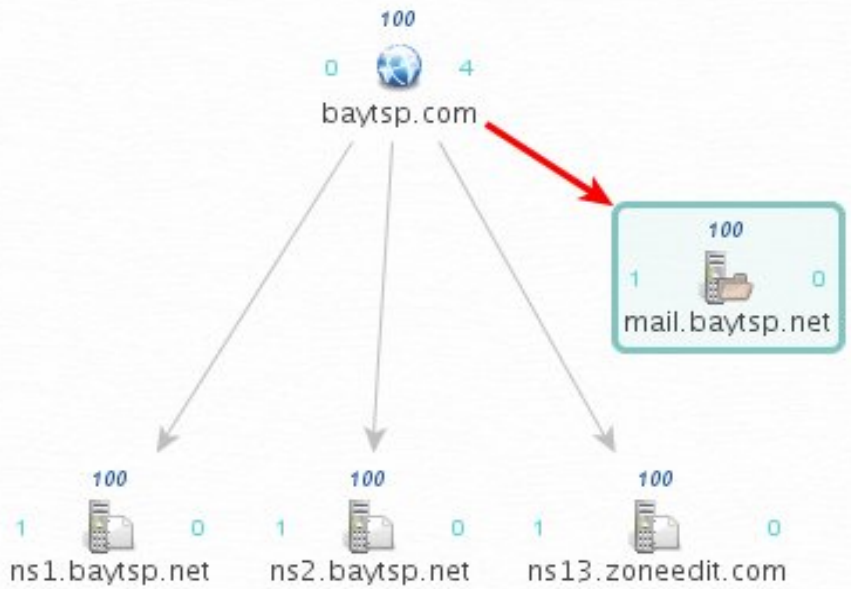


Carnal Ownage

11/10/94
Classified by [redacted] b7c
Declassify on: OADR

Maltego

- Find our MX and NS servers

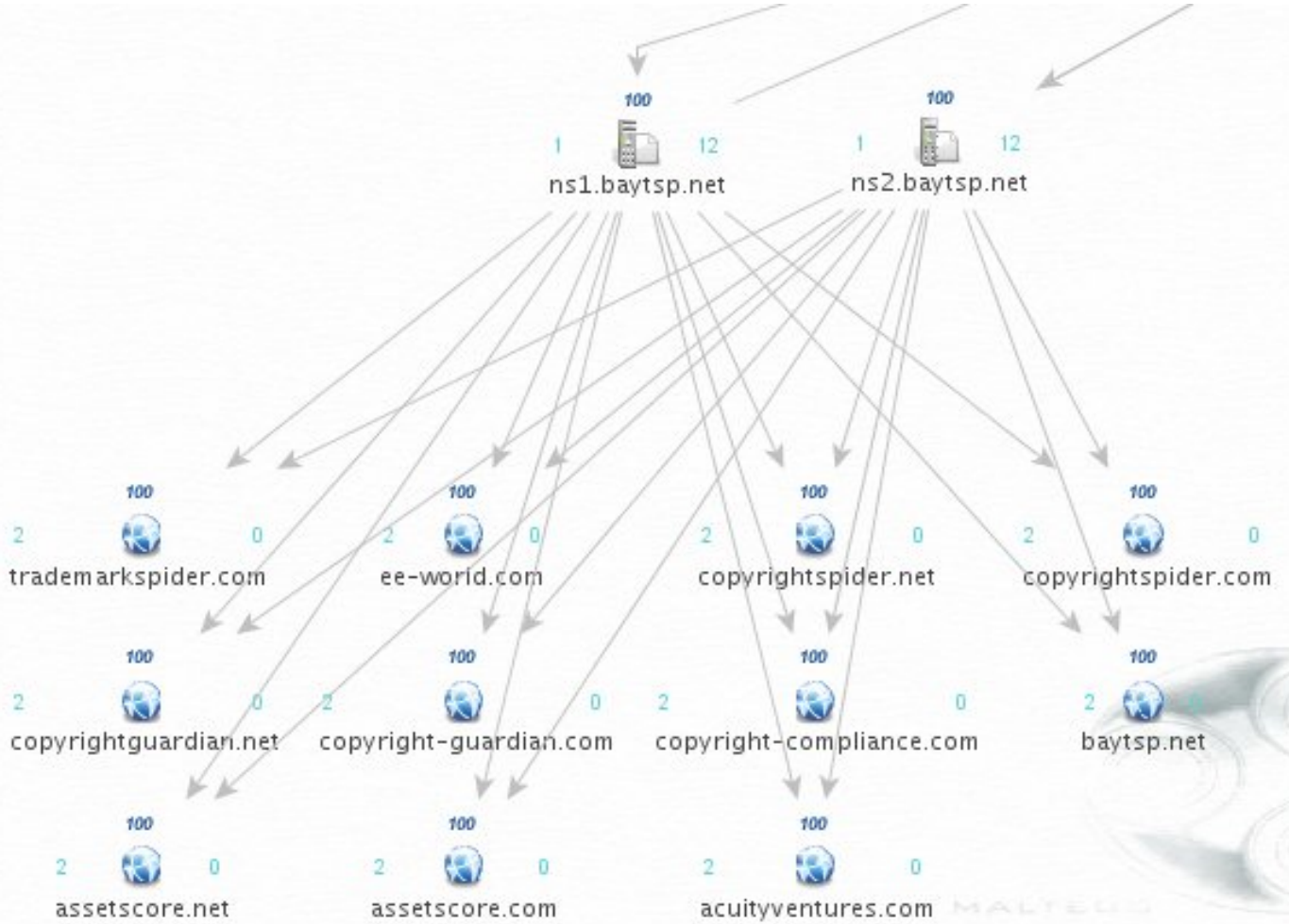


Carnal Ownage

11/10/94
Classified by [redacted] b7c
Declassify on: OADR

Maltego

- See what hostnames are shared by the DNS servers

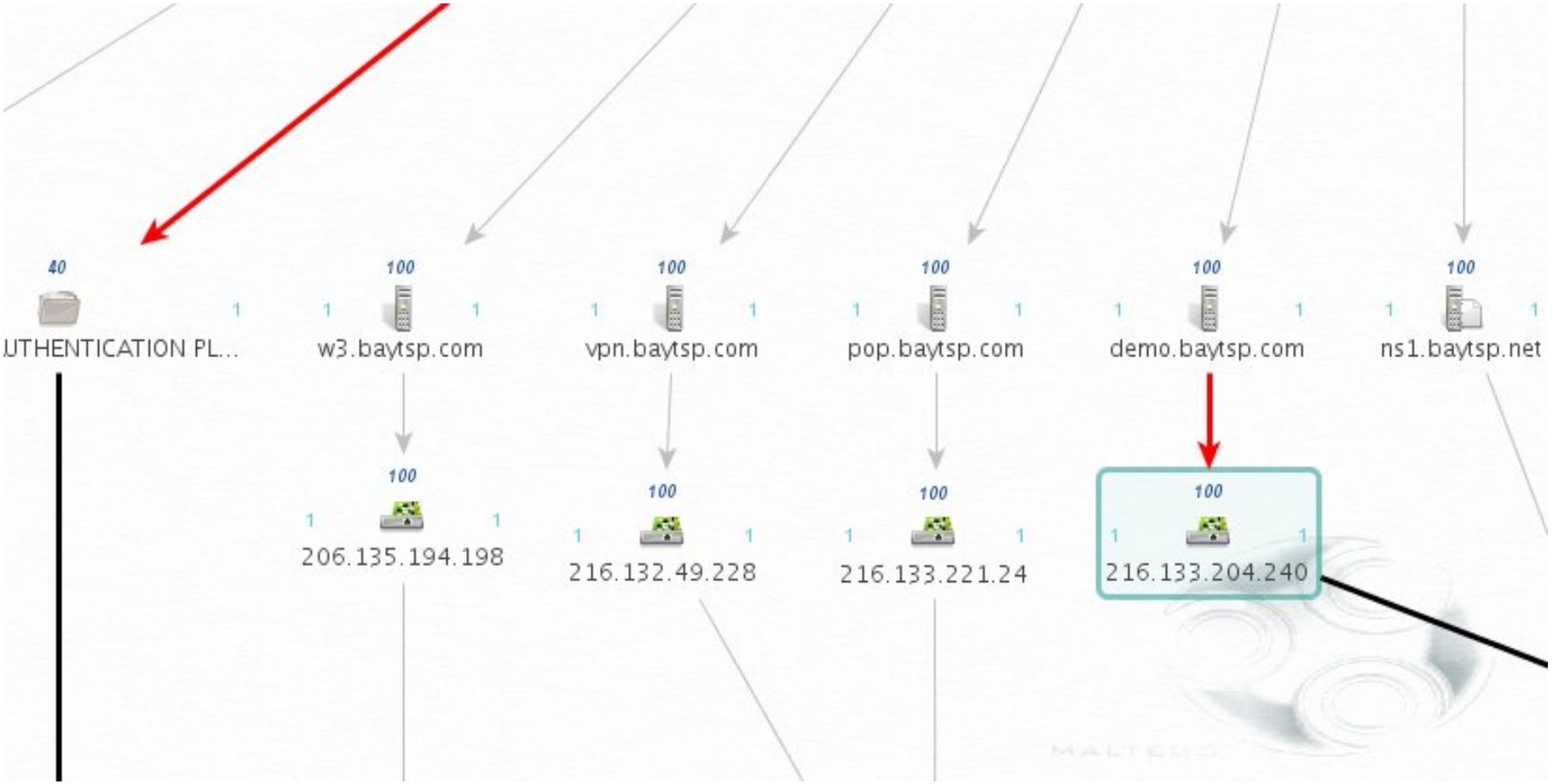


Carnal Ownage

Classified by [redacted] b7c
Reclassify on: OADR

Maltego

- Brute force our domain names and resolve them to IPs

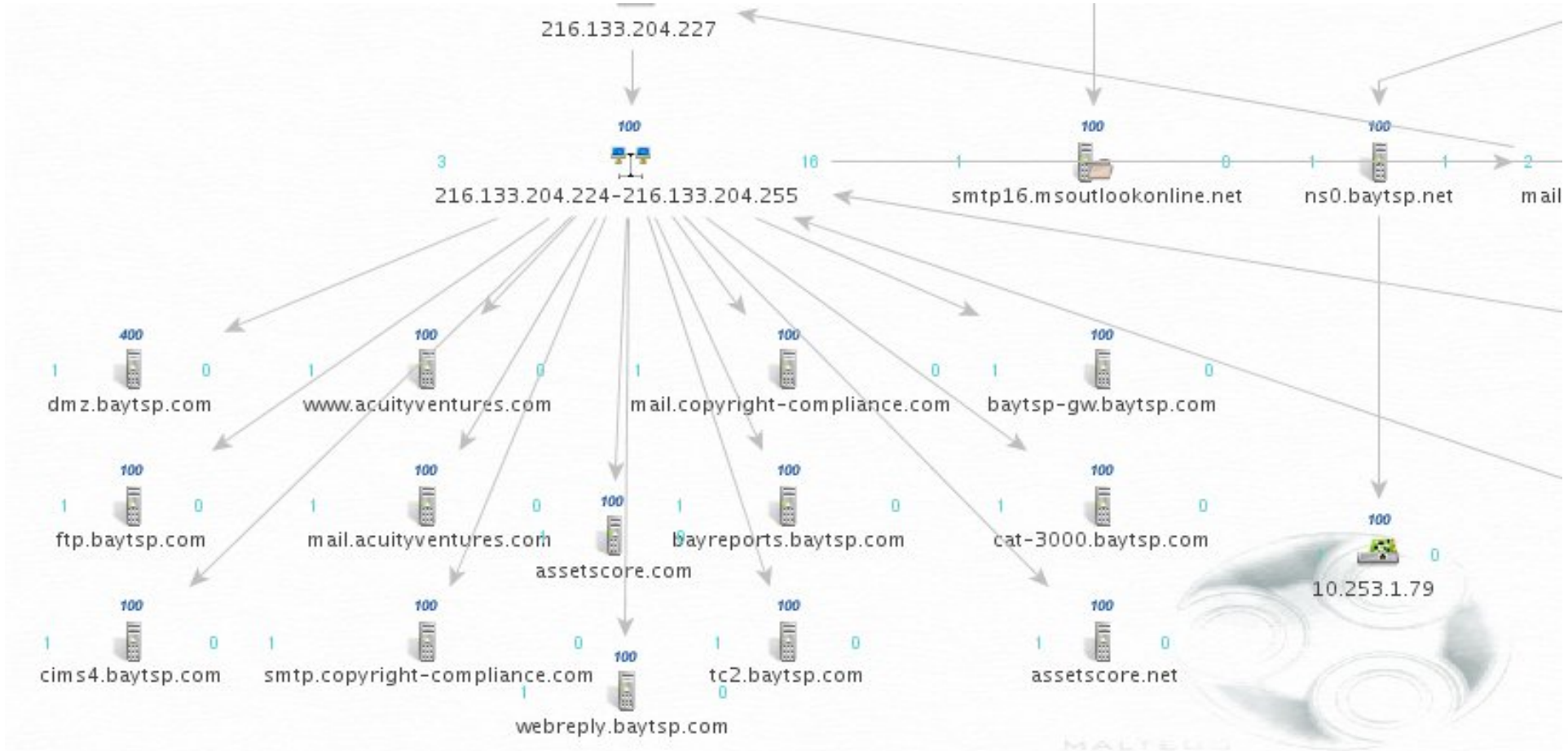


Carnal Ownage

11/10/94
Classified by [redacted] b7c
Declassify on: OADR

Maltego

- Turn each of those IPs into netblocks and do DNS lookups for each class C, you can also resolve those to IPs

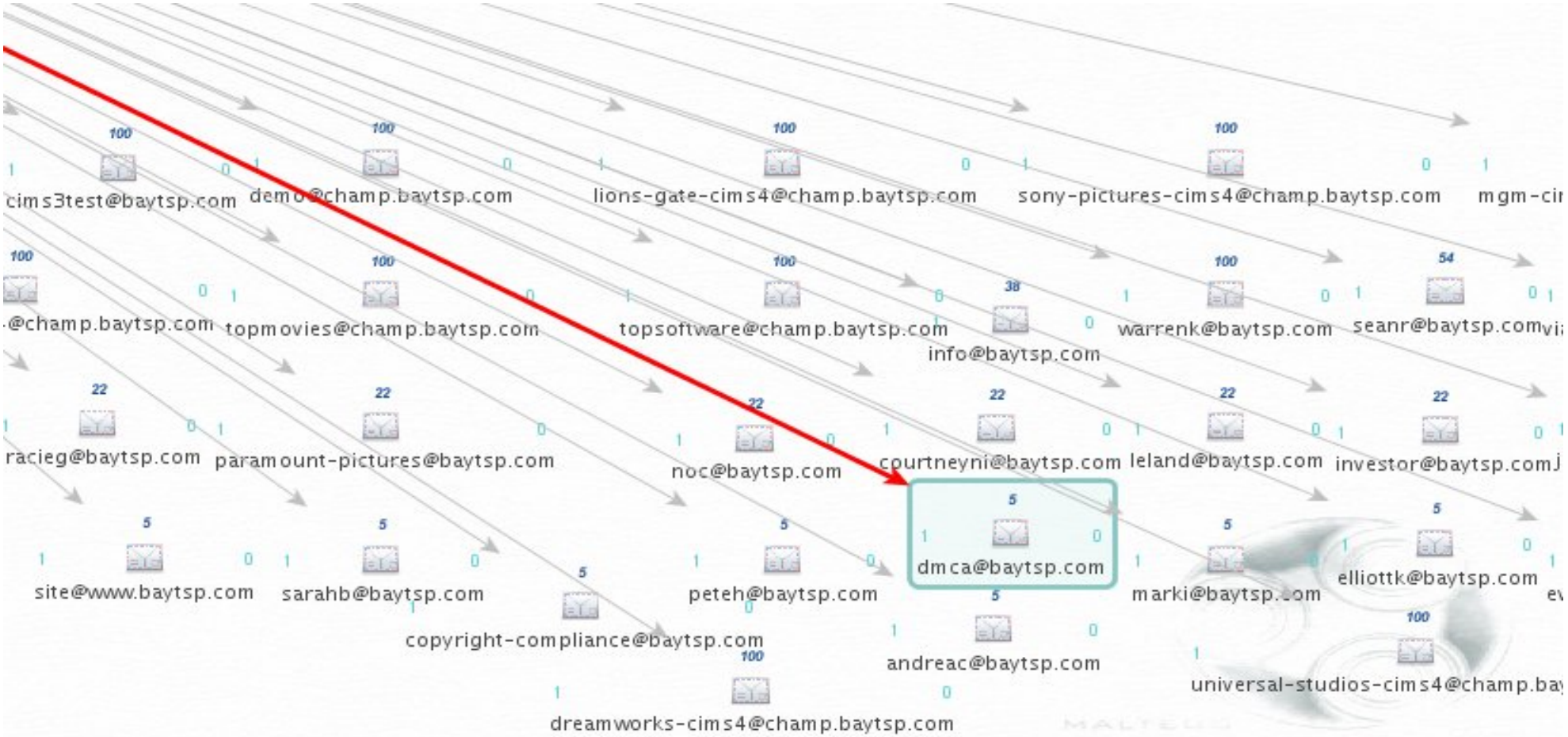


Carnal Ownage

Classified by [redacted] b7c
Reclassify on: OADR

Maltego

- Harvest emails for the domain and verify them

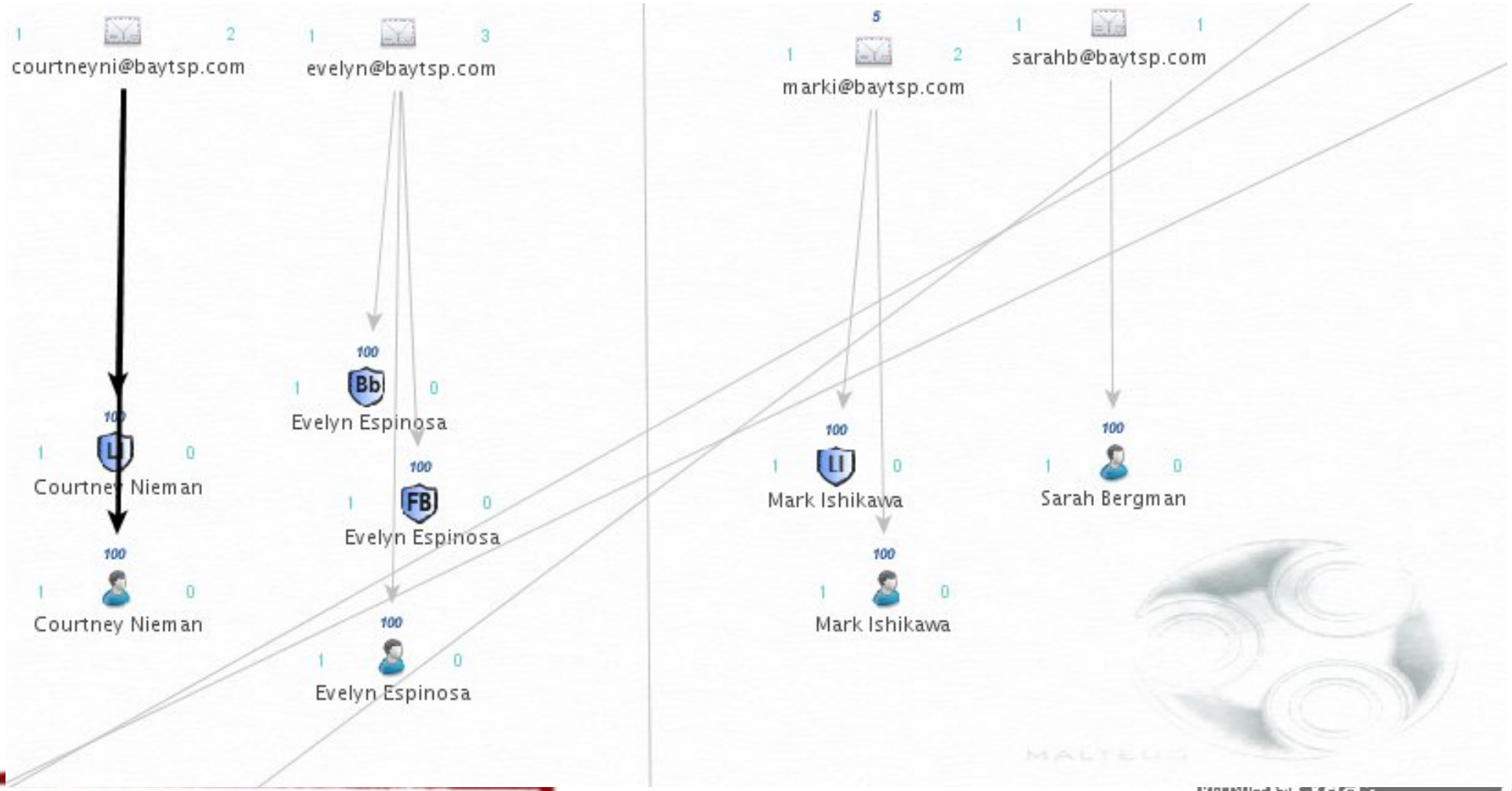


Carnal Ownage

Classified by [redacted] b7c
Declassify on: 20120

Maltego

- Turn those emails into users and their social networks

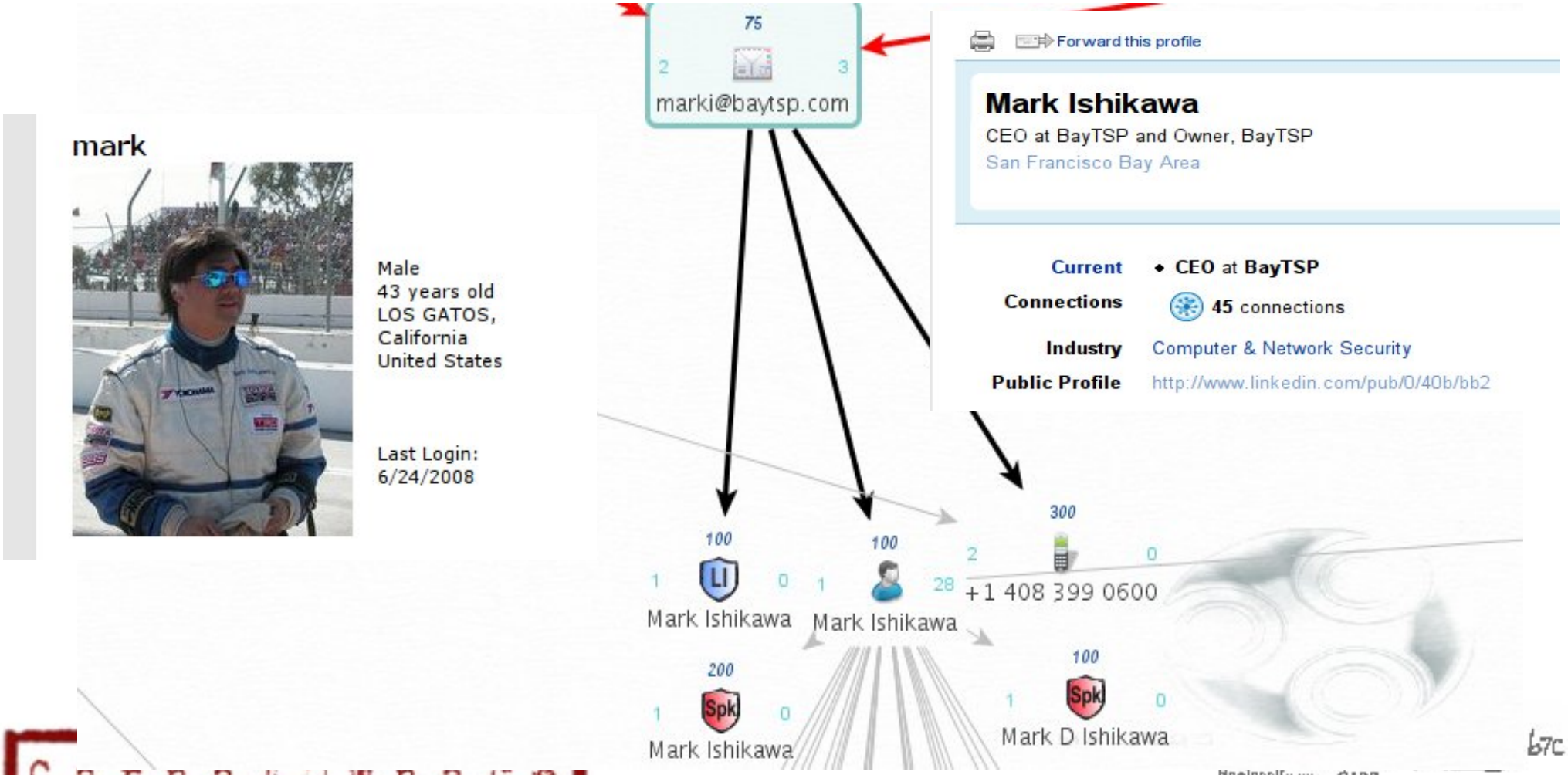


Carnal Ownage

Classified by
Reclassify on: OADR
b7c

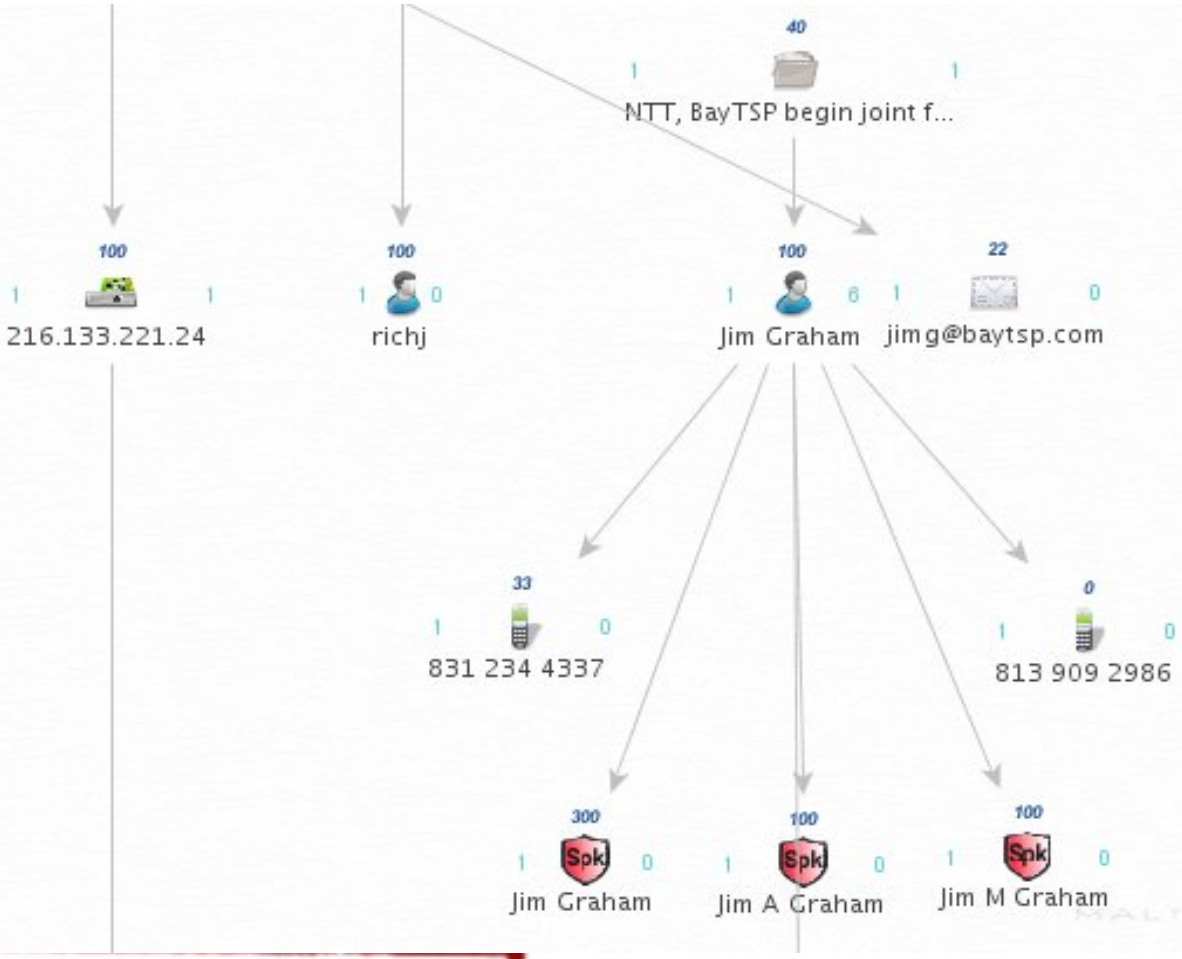
Maltego

- Take an email and derive name, phone number, social network information



Maltego

- Harvest documents for the domain and parse the metadata, get emails, usernames, phone numbers

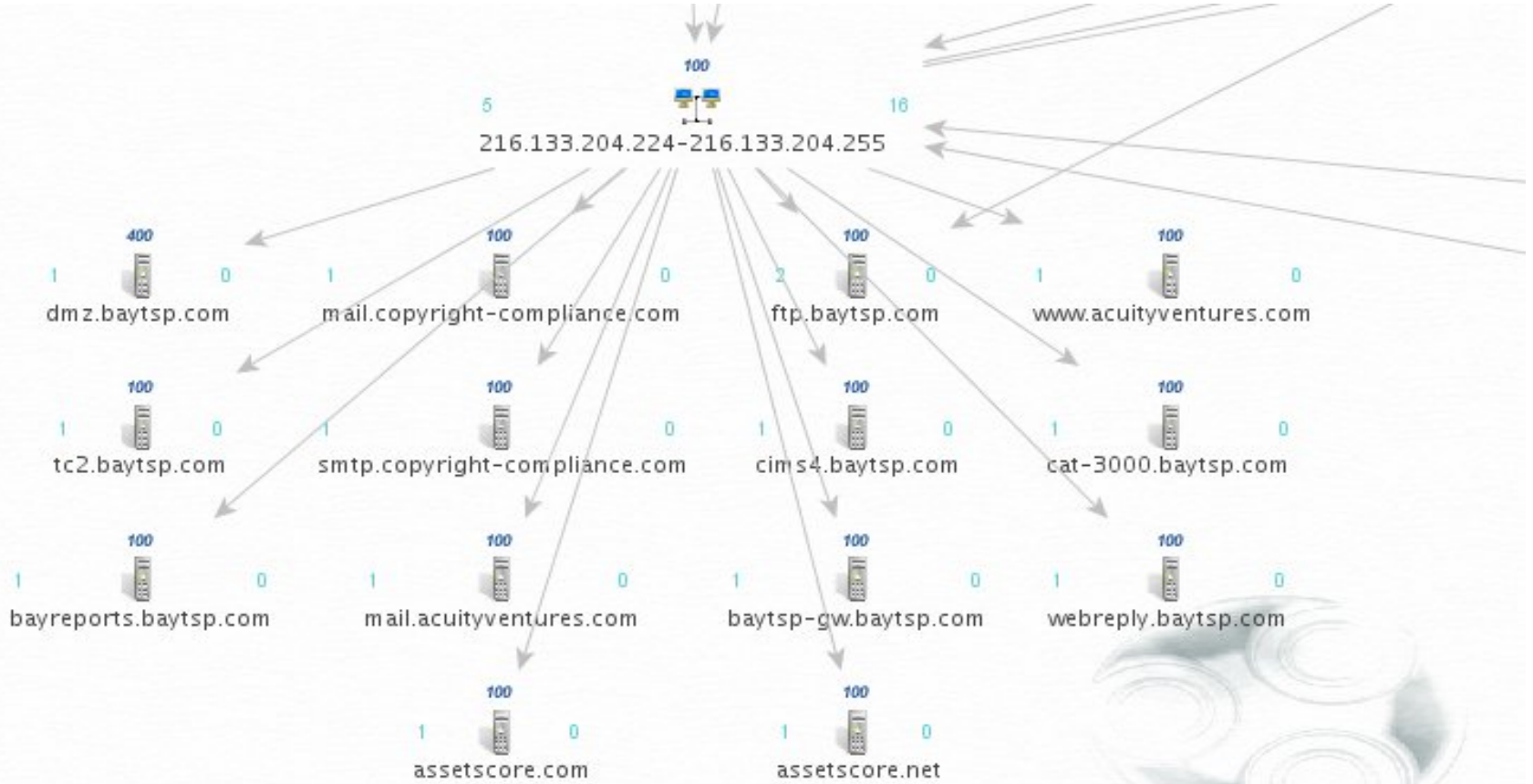


Carnal Ownage

Classified by [redacted] b7c
Declassify on: [redacted]

Maltego

- See shared domains (copyright-compliance, baytsp.net, baytsp.com, assetscore.com, etc)

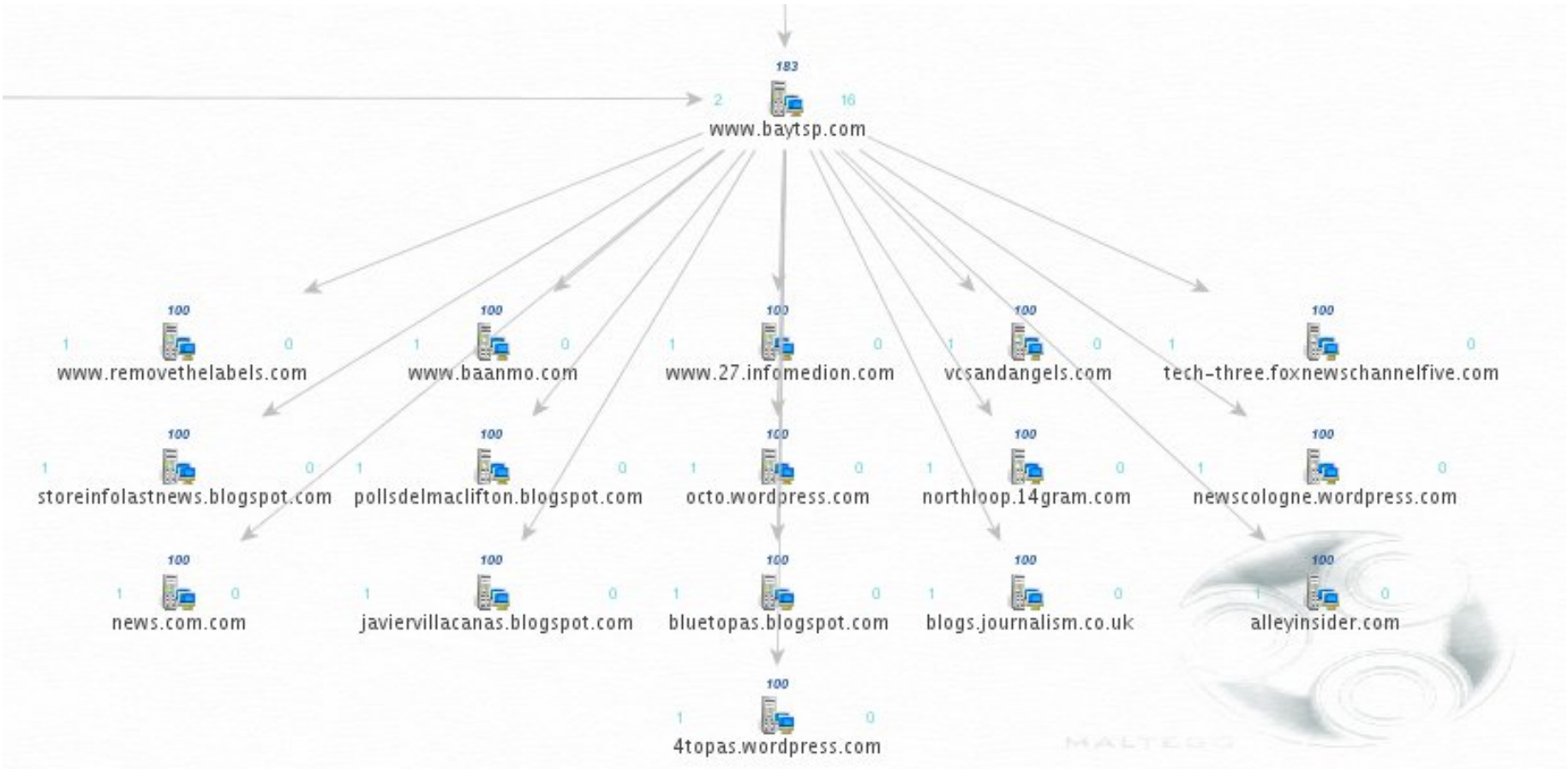


Carnal Ownage

Classified by [redacted] b7c
Reclassify on: OADR

Maltego

- Incoming links

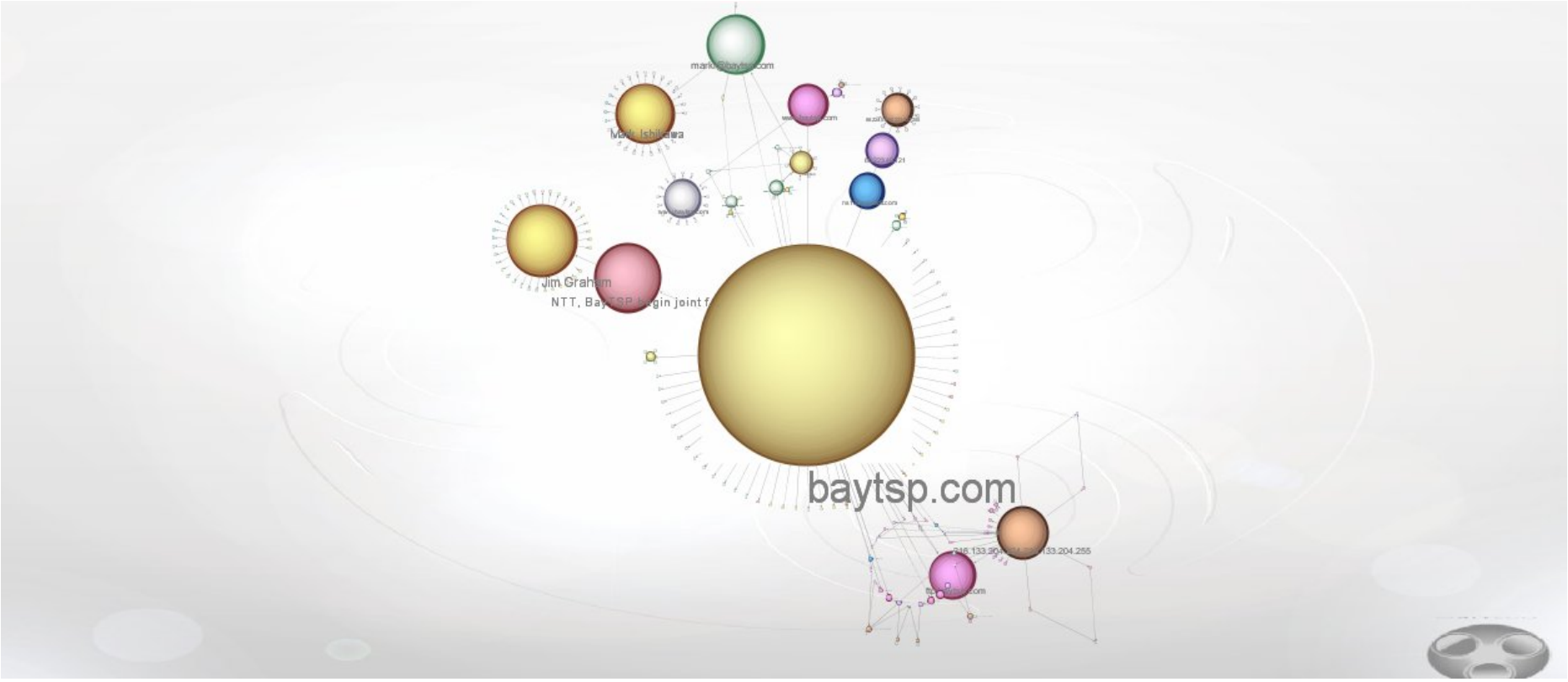


Carnal Ownage

11/10/94
Classified by [redacted] b7c
Declassify on: OADR

Maltego

- Sort your views to see relationships

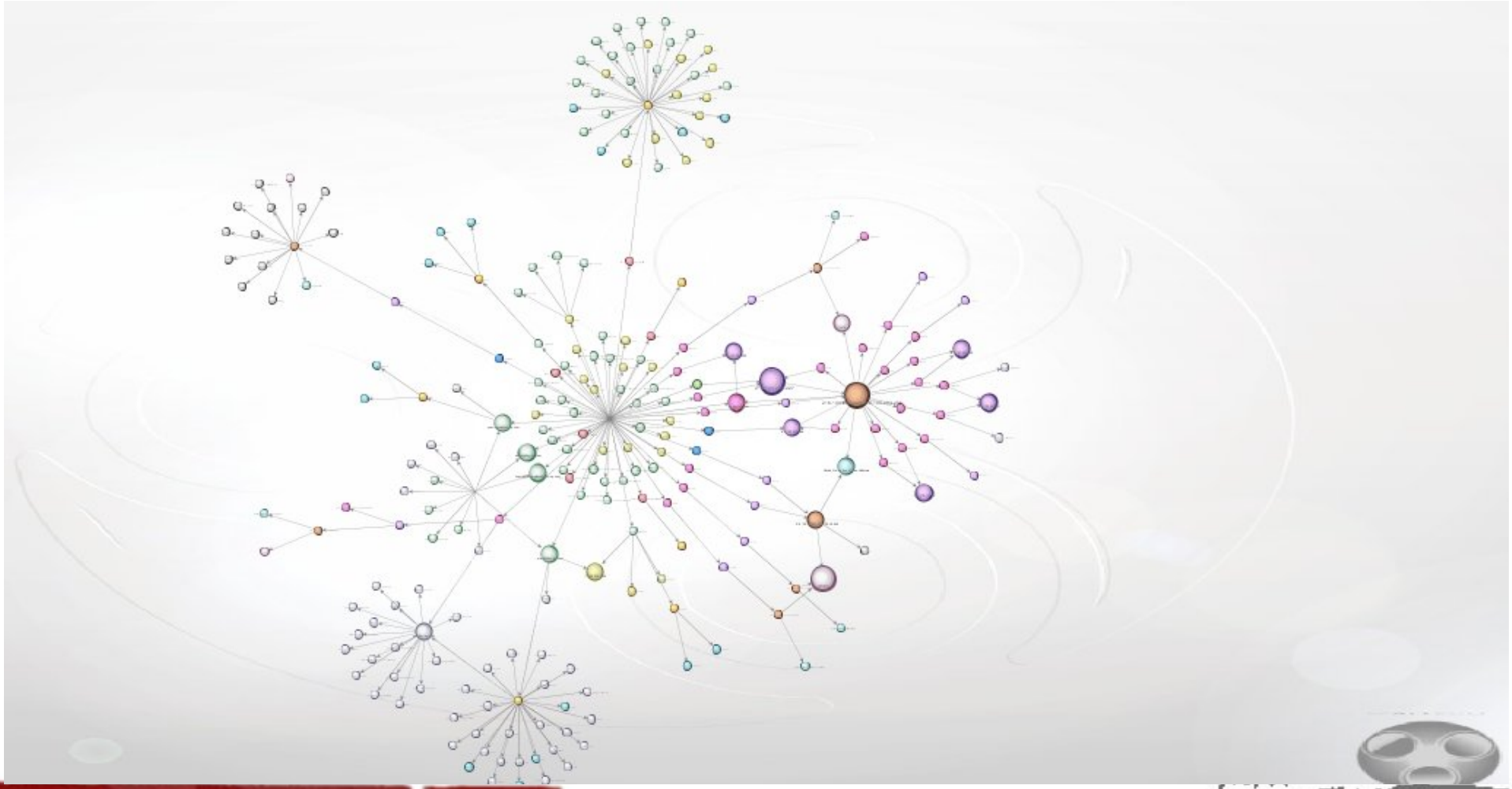


Carnal Ownage

11/10/94
Classified by [redacted] b7c
Declassify on: OADR

Maltego

- Sort your views to see relationships



Carnal Ownage

Classified by [redacted] b7c
Declassify on: 20[illegible]

Maltego

- What else can Maltego do?
  - Technorati transforms, blog tags, search blogs for phrases
  - Incoming links, who links to your domain
  - Social network transforms; find a name, find their email, blog, phone number, etc
  - Print graphs on several pages
  - Can export the data into .csv, can save the maltego file and be opened by any other maltego instance
  - Save pieces of graphs as images
  - Can write your own transforms or stand up your own server.

  - ** version 2 is for pay but cheap $430 USD for first year

Carnal Ownage

11/10/94
Classified by [redacted] b7c
Declassify on: OADR

So What?

- Ok lots of information what did I get from all of it?
  - If you are allowed to send social engineered emails or do client side attacks, you have an initial target list of email addresses. Using email dossier/maltego I can verify working email addresses. I only need one person to open/click that email for my foothold.
  - Naming conventions, users and offices, phone numbers, relationships between organizations
  - Target organization's IP Space and footprint. VPN server's IP, Terminal/Citrix server IPs, firewall's IP, etc.
  - Software versions of software that is typically targeted in client side attacks (MS office)
  - Using Maltego we see the relationships between our site and other sites in addition to the above.
  - All gained without your typical definition of "scanning"

Carnal Ownage

11/10/94
Classified by [redacted] b7c
Declassify on: OADR

Questions?

Chris Gates (CG)

http://carnal0wnage.blogspot.com

http://www.learnsecurityonline.com

Carnal0wnage

11/10/94
Classified by [redacted] b7c
Declassify on: OADR