Data Exfiltration
Not just for Hollywood!

Iftach Ian Amit
VP Consulting

DC9723
CSA-IL Board member
IL-CERT Visionary

http://conference.first.org

12 - 17 June 2011

23rd Vienna

Annual **FIRST** Conference

www.security-art.com

whoami

- Not certified

- Consulting at Security-Art

- Hacker, researcher, developer

- I like crime, and war :-)

- DC9723, IL-CERT

Going above and beyond traditional security

Tuesday, May 31, 2011

Agenda

1. Infiltration

2. Data targeting & acquisition

3. Exfiltration

Going above and beyond traditional security

Tuesday, May 31, 2011

1. Infiltration

- Technical factors

- Human factors

- Command & Control in loosely connected environments

Going above and beyond traditional security

Tuesday, May 31, 2011

Infiltration - Technical

- Exploits!   of what???

  - Web, FTP, mail, SSL-VPN...

    - Will only get you the basic stuff

  - 3rd party tools used (LinkedIn, SalesForce, SaaS applications)...

    - Harder to get
      *although nice to have as reproducible on many targets

Going above and beyond traditional security

Tuesday, May 31, 2011

Infiltration - Technical

The problem:

Small attack surface

Going above and beyond traditional security

Tuesday, May 31, 2011

Infiltration - Technical

- How about them windows?

- Win XP still the dominantly deployed OS on clients (both in corporate and government settings)

- Win 7 is no big deal

- **Attack surface** is much broader (spell Adobe, Symantec, WinZip, AOL, Mozilla, etc...)
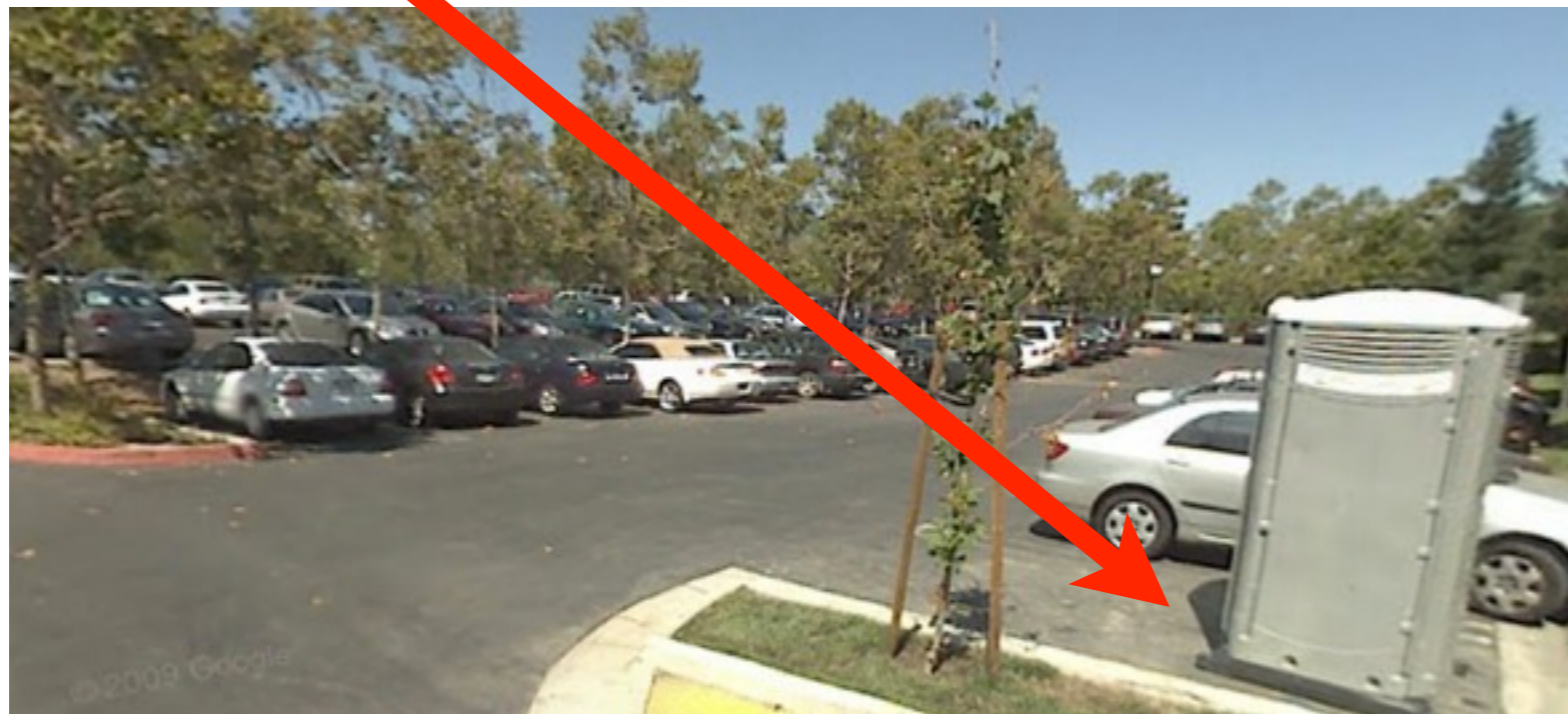
Going above and beyond traditional security

Tuesday, May 31, 2011

Infiltration - Human

- Not as in "I got your guy and I want $1,000,000 to set him free"

- More like "dude, check out the pics from the conference we went to last month. Wicked!"

  - "did you get my memo with the new price-list <link to .xls file>"

  - You get the idea...

Going above and beyond traditional security

Tuesday, May 31, 2011

Infiltration - Human

Going above and beyond traditional security

Tuesday, May 31, 2011

Infiltration - Human

- eMails, web links, phishing...

  - Works like a charm!

- And can be mostly automated

  - SET to the rescue

```
Select from the menu on what you would like to do:

1.   Spear-Phishing Attack Vectors
2.   Website Attack Vectors
3.   Infectious Media Generator
4.   Create a Payload and Listener
5.   Mass Mailer Attack
6.   Teensy USB HID Attack Vector
7    Update the Metasploit Framework
8.   Update the Social-Engineer Toolkit
9.   Help, Credits, and About
10.  Exit the Social-Engineer Toolkit
```

Going above and beyond traditional security

Tuesday, May 31, 2011

Infiltration - Human

And... being nice/nasty/ obnoxious/needy always helps!

11

Going above and beyond traditional security

2. Data Targeting & Acquisition

- Weaponizing commercial tools
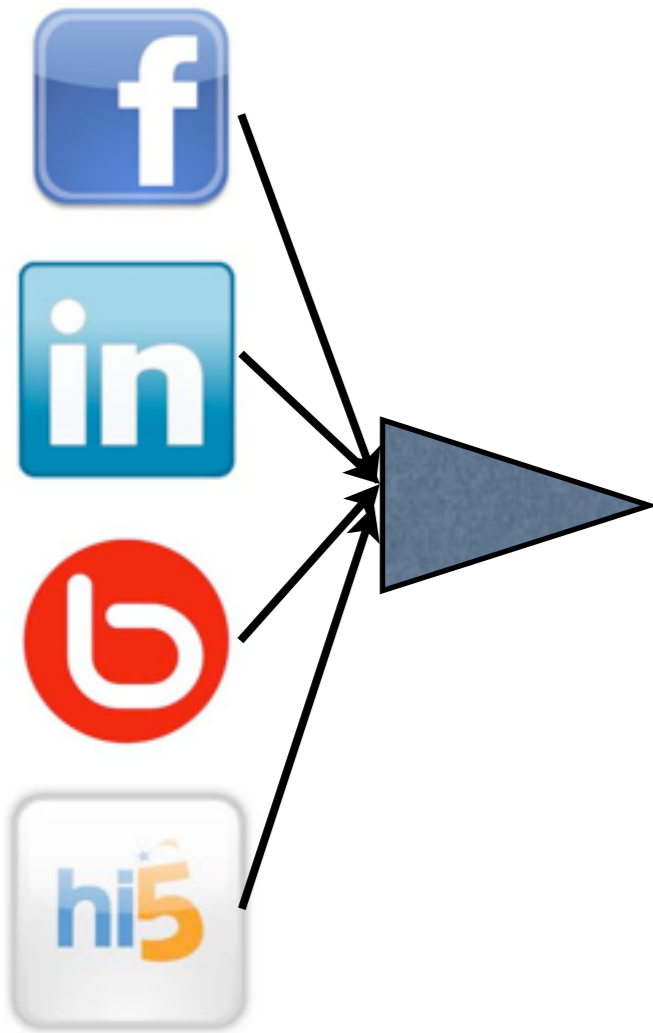
- Creating "APT" capabilities

- But first - targeting...

Going above and beyond traditional security

Tuesday, May 31, 2011

Step 1: Basic Intel

What is the target "willing" to tell about itself?

Going above and beyond traditional security

Tuesday, May 31, 2011
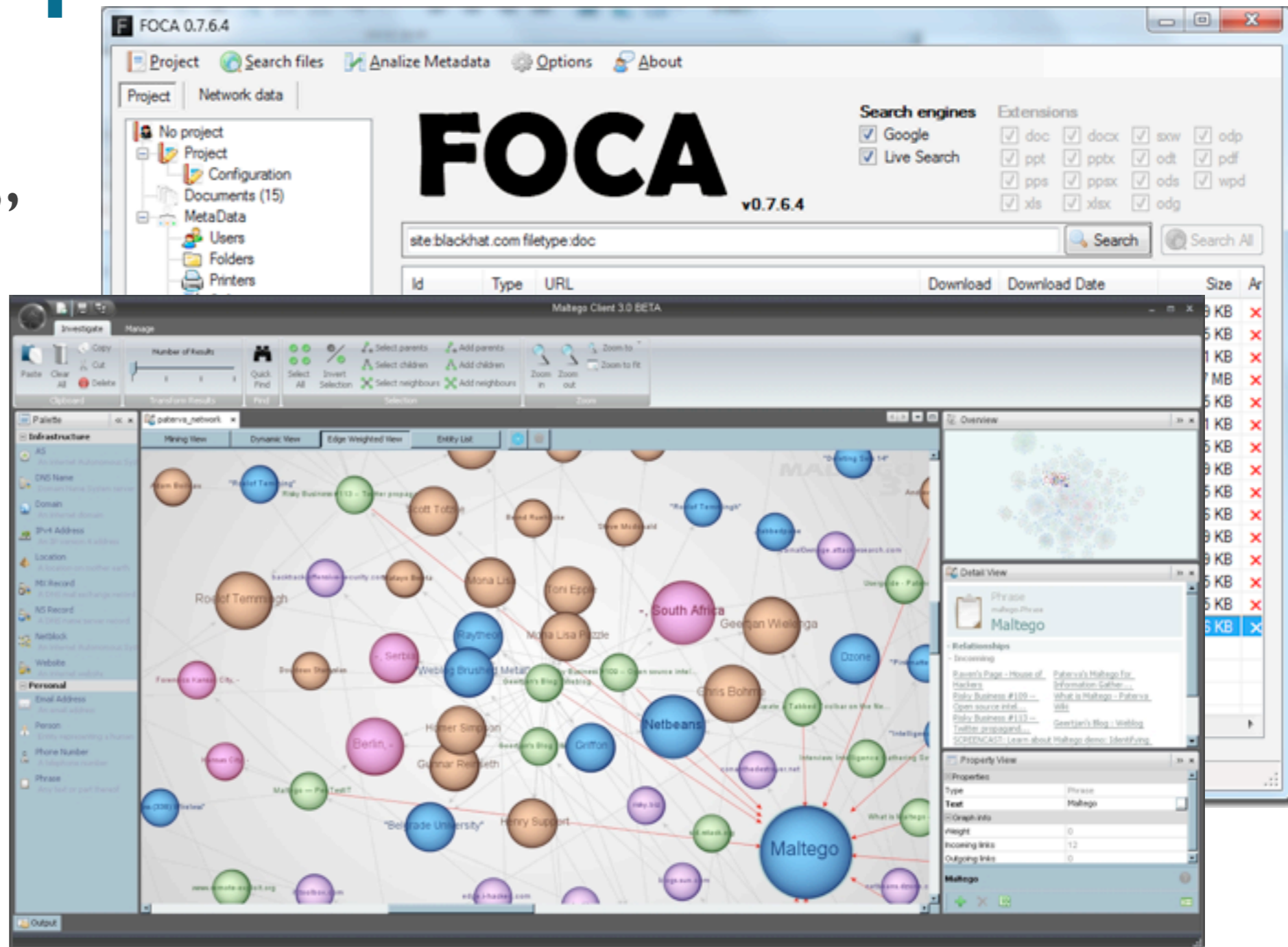
Who's your daddy?

And buddy, and friends, relatives, colleagues...

Going above and beyond traditional security

Tuesday, May 31, 2011
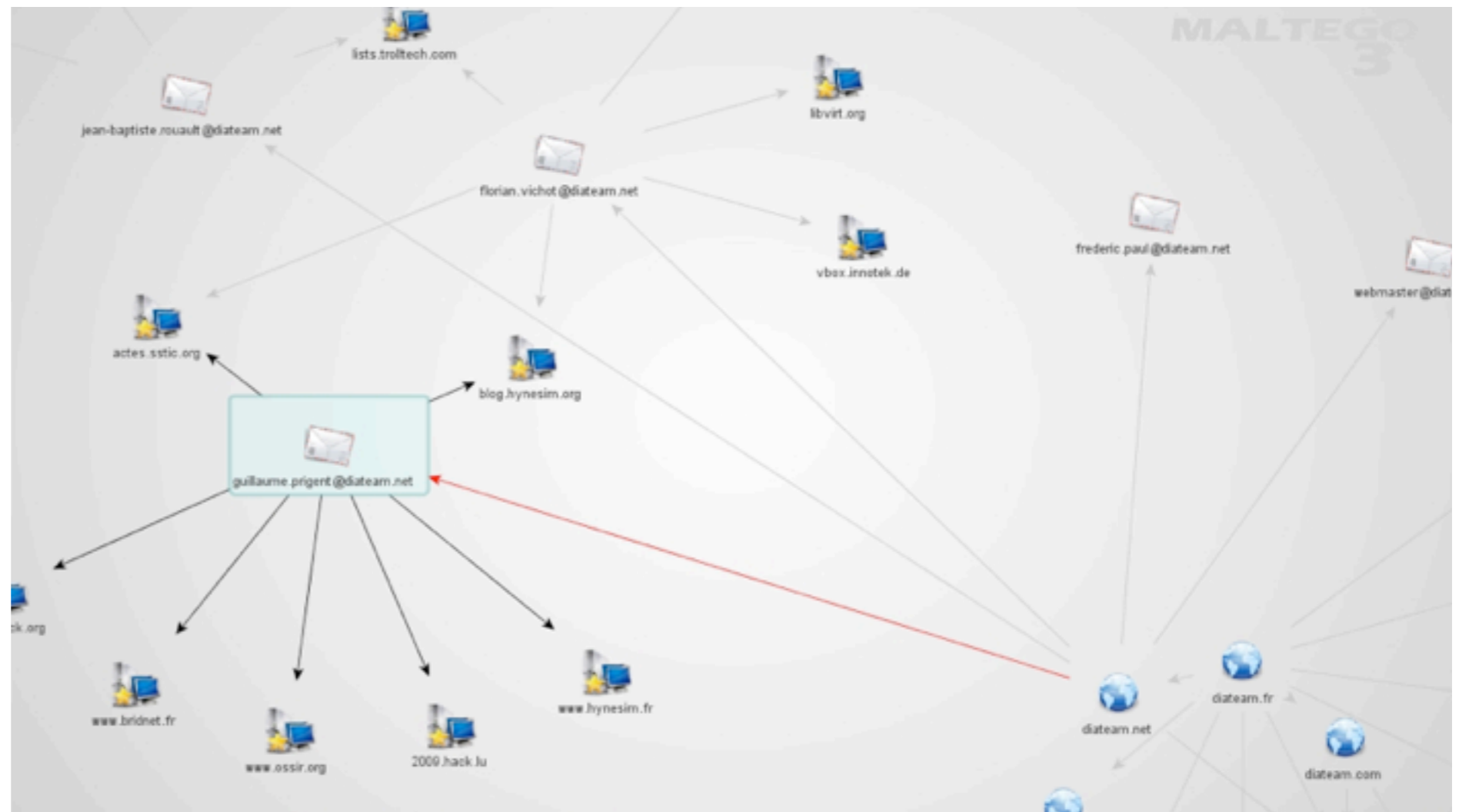
Select your target wisely

And then craft your payload :-)

Going above and beyond traditional security

Tuesday, May 31, 2011

Not as expensive as you think

- ZeuS: $3000-$5000

- SpyEye: $2500-$400

- Limbo: $500-$1500

Going above and beyond traditional security

Tuesday, May 31, 2011
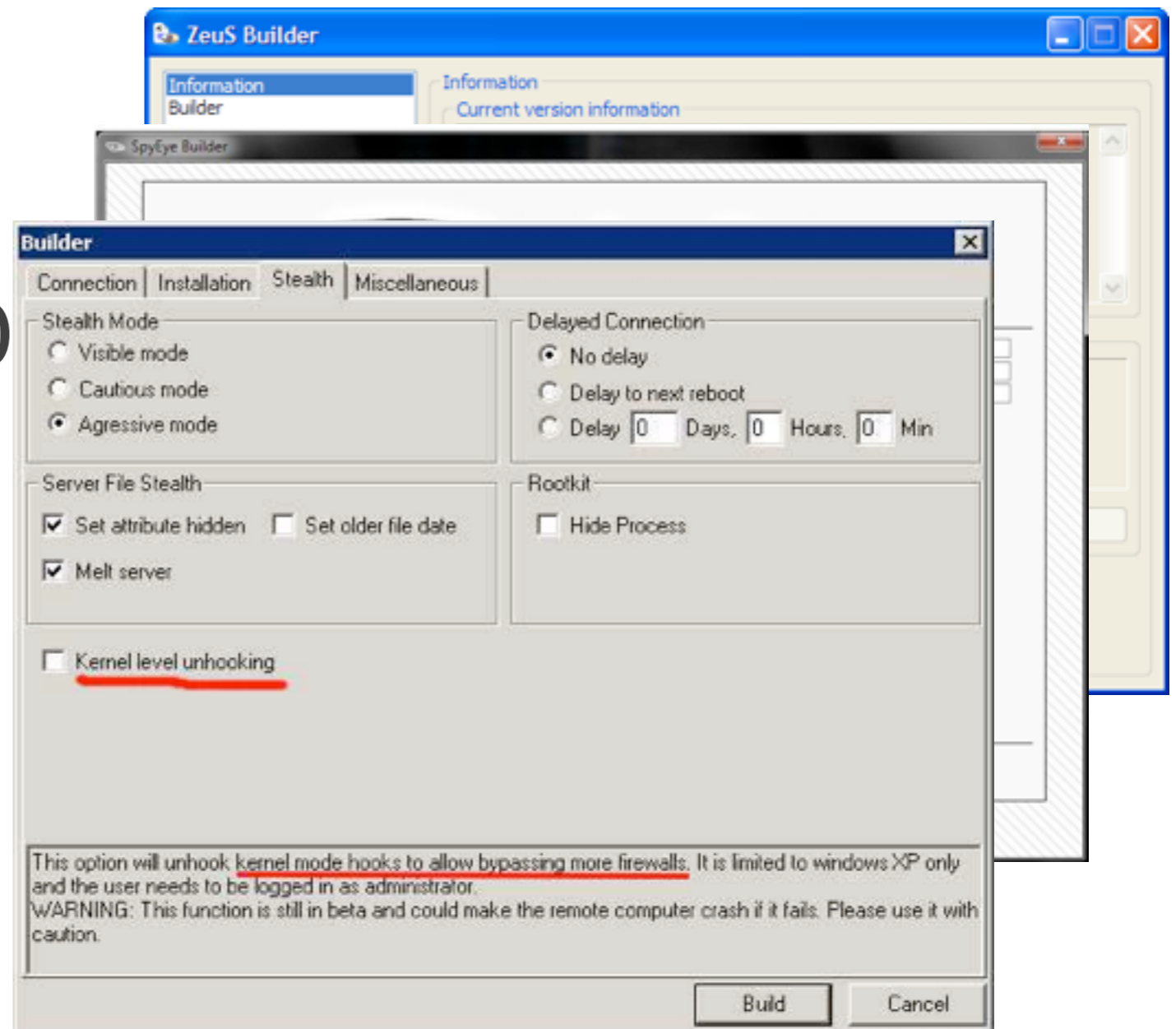
Just make sure to pack

Experienced travelers know the importance of packing properly

Looking for a better option?

Going above and beyond traditional security

Tuesday, May 31, 2011
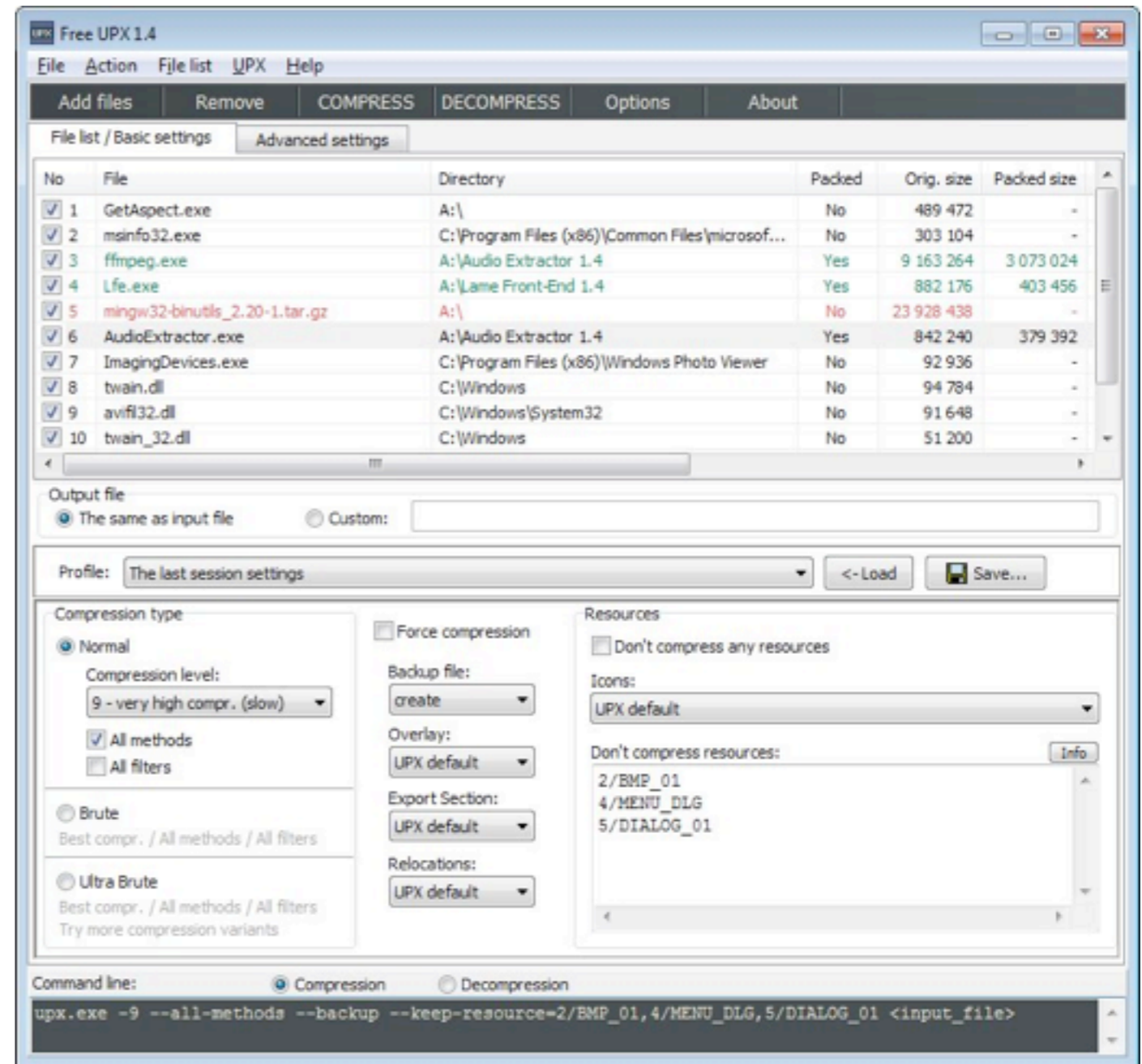
And set measurable goals

- File servers

- Databases

- File types

- Gateways (routes)

- Printers

Going above and beyond traditional security

Tuesday, May 31, 2011

From mass infection to APT

PATIENCE

Mass infection:
5-6 days before
detection

⬇
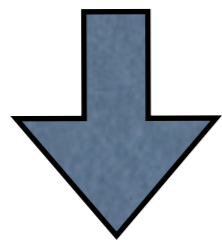
Frequent updates

APT:
5-6 months before
detection

⬇

No* updates

*Almost

19

Going above and beyond traditional security

Tuesday, May 31, 2011
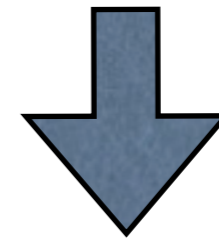
Control?

- What happens when you are so far behind?

- Just use your friends (peers)

  - Expect a one-way command scheme.

  - Exfiltration is a different animal...

Internet

3rd party

You!

Target

Going above and beyond traditional security

Tuesday, May 31, 2011
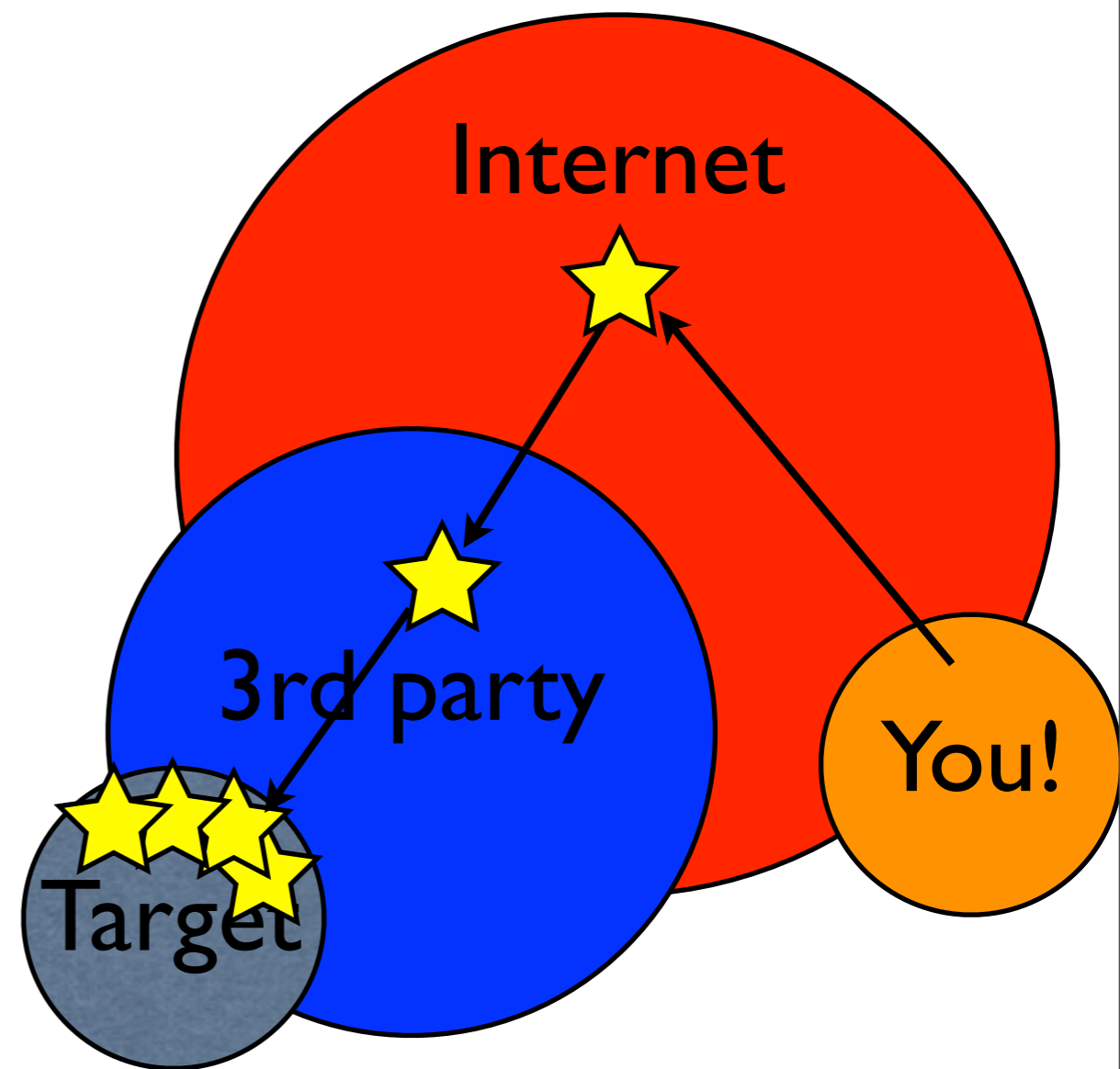
3. Exfiltration

- Avoiding DLP

- Avoiding IPS/IDS egress filters

- Encryption

- Archiving

- Additional techniques

21

Going above and beyond traditional security

Under the radar

- What does the radar look for?

- Text

Going above and beyond traditional security

Tuesday, May 31, 2011

How about them SSLs?

- Cool.

- Although sometimes may be intercepted
  - Pesky content filters...

Going above and beyond traditional security

Tuesday, May 31, 2011

So...

-----BEGIN PGP MESSAGE-----
Version: GnuPG/MacGPG2 v2.0.14 (Darwin)

hQMOA1jQIm6UkL4eEAv/W3r/eYLUmqRNi/Jegt72lK6qdBiBfkg9PZ5YKql9CUZp
FGnVk029K3gEVcrA4k7w2aOtP7tYKRF8v4yrZQ9GZ7eXzR7+Tbf1g+7dveH6U8Bf
BHo8LRovj5OlGghrvpyKYRPlf/NAgzL2G8dyi/FVB0YB4J7/4x0YFEalQHaLiKyt
/gkikyV92njPJ6tPm2sdKUqUHSb20r9AdowZ0VVRrWwdRgUhdNXajjwcbH1BjVuS
Gilw8MnmQkmJAT+TAFkTqC9fjiwtnNMNANJbo2Z36RqsAcKbhVh1eMA7ev0pUakp
Tm4xN64syk/1DEc0VHFbanAreTV3tCbUUIoPQDFGFpiu3oS6/089oUvRtBBbC5p6
leYKEnDllcGWAomRSiYBFWjTca/DIw43QIW/lmdBnwcWLuQmDCmwr3HuhEaOmqfO
hdgaxM4GuVdJCDdwXzwpuaPElCd18weH2XNzudLdeRKN+wjl/4D6bIo+038BcLei
SyhWrMFB7mKSmEzQufQUDACFamtMCn9YOo3mgo+YYk505qhIDLNwZXqyVUqOHvlG
vu7gzuNwUdY5idLqsGEs0K0xVwYntTKUh61tNS/HDfNTVm4Y3p8M88JHhcg7npY5
gJuhWuHkgp2CTsQT+gRjthm3l3AlnIvAfuC5uWLMsjA4sCw2FRDOARxrN9El8maX
/vCxN9aB3dK4S9MSGJ5HhaYpTfpc9CdFkFryzb2sFWfW85nSzNo7dVFCy0jmSr19
o4Jsfj0J0izS3MeGYYz5NSsfBz+6o/IYURL3OXrm4DuJNHY0DvVbYqSQRRx3o2S+
uZekwXwYsqpei/f/sYo875p5NeX3g62zgjy2Vly+n58WaZWoHb5Y0QCxNfpjdcAQ
3tuZQaUvlqrkQeSRxKXD7pxlHdwHDgfvw01RU8NsMkfsBoTZY27BjFvlg5S/pv9O
6IznXaJu9jRWDj6tvSypx8X2iiVgtSHYahlqEUH1RusAMCILkx0DydCvUud/qRbT
YcnkVVgA8ojeDoVpp3AabRrSmgEAOwW6M0KvnSuMKniLIKe7kolqGjEuLAx7s5Kg
mMHfNki5dYWvQzHv03ID9UG+uW6o54BnsajEVe2EcYTPT+8pg2bCxnMElK0ds9ls
qvf2Kx4kqO0qMeJG1II2zfAFqmMiTMtgA2CZ0Y42hA/bQK/CCM8QVo9JcGn3Jf6N
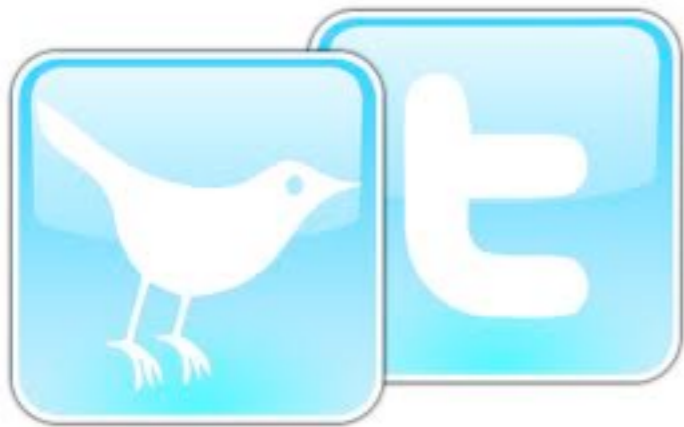0X1TVob7xDo/fkRROHv74dlh2Kxa0SH8iGdb4kI=
=jN3t
-----END PGP MESSAGE-----

Going above and beyond traditional security

Tuesday, May 31, 2011

Still "too detectable"

hQMOA1jQIm6UkL4eEAv/W3r/eYLUmqRNi/Jegt72lK6qdBiBfkg9PZ5YKql9CUZp
FGnVk029K3gEVcrA4k7w2aOtP7tYKRF8v4yrZQ9GZ7eXzR7+Tbf1g+7dveH6U8Bf
BHo8LRovj5OlGghrvpyKYRPlf/NAgzL2G8dyi/FVB0YB4J7/4x0YFEalQHaLiKyt
/gkikyV92njPJ6tPm2sdKUqUHSb20r9AdowZ0VVRrWwdRgUhdNXajjwcbH1BjVuS
Gilw8MnmQkmJAT+TAFkTqC9fjiwtnNMNANJbo2Z36RqsAcKbhVh1eMA7ev0pUakp
Tm4xN64syk/1DEc0VHFbanAreTV3tCbUUIoPQDFGFpiu3oS6/089oUvRtBBbC5p6
leYKEnDllcGWAomRSiYBFWjTca/DIw43QIW/lmdBnwcWLuQmDCmwr3HuhEaOmqfO
hdgaxM4GuVdJCDdwXzwpuaPElCd18weH2XNzudLdeRKN+wjl/4D6bIo+038BcLei
SyhWrMFB7mKSmEzQufQUDACFamtMCn9YOo3mgo+YYk505qhIDLNwZXqyVUqOHvlG
vu7gzuNwUdY5idLqsGEs0K0xVwYntTKUh61tNS/HDfNTVm4Y3p8M88JHhcg7npY5
gJuhWuHkgp2CTsQT+gRjthm3l3AlnIvAfuC5uWLMsjA4sCw2FRDOARxrN9El8maX
/vCxN9aB3dK4S9MSGJ5HhaYpTfpc9CdFkFryzb2sFWfW85nSzNo7dVFCy0jmSr19
o4Jsfj0J0izS3MeGYYz5NSsfBz+6o/IYURL3OXrm4DuJNHY0DvVbYqSQRRx3o2S+
uZekwXwYsqpei/f/sYo875p5NeX3g62zgjy2Vly+n58WaZWoHb5Y0QCxNfpjdcAQ
3tuZQaUvlqrkQeSRxKXD7pxlHdwHDgfvw01RU8NsMkfsBoTZY27BjFvlg5S/pv9O
6IznXaJu9jRWDj6tvSypx8X2iiVgtSHYahlqEUH1RusAMCILkx0DydCvUud/qRbT
YcnkVVgA8ojeDoVpp3AabRrSmgEAOwW6M0KvnSuMKniLIKe7kolqGjEuLAx7s5Kg
mMHfNki5dYWvQzHv03ID9UG+uW6o54BnsajEVe2EcYTPT+8pg2bCxnMElK0ds9Is
qvf2Kx4kqO0qMeJG1II2zfAFqmMiTMtgA2CZ0Y42hA/bQK/CCM8QVo9JcGn3Jf6N
0X1TVob7xDo/fkRROHv74dIh2Kxa0SH8iGdb4kI=
=jN3t

Going above and beyond traditional security

Tuesday, May 31, 2011

Much better

- Throws in some additional encodings

- And an XOR for old time's sake

- And we are good to go...

  - 0% detection rate

Going above and beyond traditional security

Tuesday, May 31, 2011

Resistance is futile

Going above and beyond traditional security

Tuesday, May 31, 2011

But you have no network

- They killed 80, 443, 53 and cut the cable to the interwebs!

- Go old-school!

Going above and beyond traditional security

Tuesday, May 31, 2011

Kill some trees

29

Going above and beyond traditional security

To shred or not to shred?

Going above and beyond traditional security

Tuesday, May 31, 2011

Yeah, good ol'e DD...

31

Going above and beyond traditional security

Tuesday, May 31, 2011

Back to hi-tech (?)
ET Phone Home

Got VOIP?   Excellent!

Target a handset/switch

Set up a public PBX
OR a conference call
OR a voicemail box
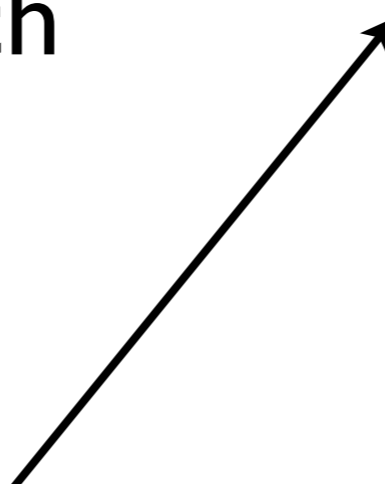
Collect your data

Encode

Call, leave a message, don't expect to be called back...

Going above and beyond traditional security

Tuesday, May 31, 2011

Voice exfiltration demo

33

Going above and beyond traditional security

Tuesday, May 31, 2011

Killing paper isn't nice

- Fax it!

- Most corporations have email-to-fax services

  - heard of the address 555-7963@fax.corp.com ?

- Just send any document (text, doc, pdf) to it and off you go with the data...

Going above and beyond traditional security

Tuesday, May 31, 2011

Conclusions

- Available controls

- Information flow path mapping

- Asset mapping and monitoring

Going above and beyond traditional security

Tuesday, May 31, 2011

Controls

- Start with the human factor

- **Then** add technology

Going above and beyond traditional security

Tuesday, May 31, 2011

Know yourself, know your enemy

- Where do people leave data

  - **Hint** - spend time with developers.

- "Hack" the business process

- Test, test again, and then test. Follow with a surprise test!

Going above and beyond traditional security

Tuesday, May 31, 2011

Map your assets

"be true to yourself, not to what you believe things should look like"

Old chinese proverb

Going above and beyond traditional security

Tuesday, May 31, 2011

And monitor them!

They are YOUR assets
after all

No reason to be
shy about it...

And remember to add
honey...

Going above and beyond traditional security

Tuesday, May 31, 2011

Then...

TEST SOME MORE

For hints/guides see: www.pentest-standard.org

Shameless Plug!

Going above and beyond traditional security

Tuesday, May 31, 2011

Questions?

Go get your fix here:
www.security-art.com

Thank **you**!

Too shy to ask now?
iamit@security-art.com

Need your daily chatter?
twitter.com/iiamit

Going above and beyond traditional security

Tuesday, May 31, 2011