Iftach Ian Amit | September 2011

Pushing in, leaving a present and pulling out without anybody noticing

Iftach Ian Amit
VP Consulting

DC9723
CSA-IL Board member
IL-CERT Visionary

www.security-art.com

whoami

- Not certified
- VP Consulting at Security-Art
- Hacker, researcher, developer
- I like crime, and war :-)
- DC9723, PTES, IL-CERT, IAF

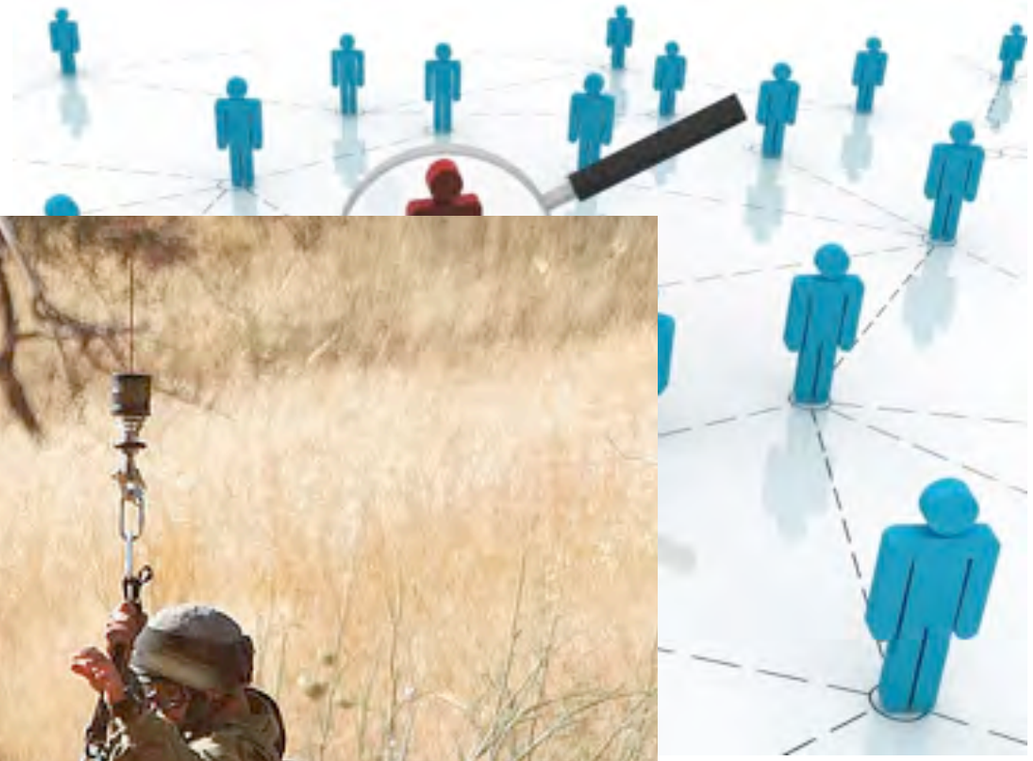
Agenda

Agenda

Agenda

Going above and beyond traditional security

Agenda



I. Infiltration

- Technical factors
- Human factors
- Command & Control in loosely connected environments

Infiltration - Technical

Infiltration - Technical

- Exploits! of what???

Infiltration - Technical

- Exploits! of what???
  - Web, FTP, mail, SSL-VPN...

Infiltration - Technical

- Exploits! of what???
  - Web, FTP, mail, SSL-VPN...
    - Will only get you the basic stuff

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)...

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

Iftach Ian Amit | September 2011

Infiltration - Technical

The problem:

Small attack surface

Infiltration - Technical

Infiltration - Technical

- How about them windows?

Infiltration - Technical

- How about them windows?
- Win XP still the dominantly deployed OS on clients (both in corporate and government settings)

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

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

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...)

Infiltration - Human

Infiltration - Human

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

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!"

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>"

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...

Infiltration - Human

Infiltration - Human

Infiltration - Human

Infiltration - Human

Infiltration - Human

- eMails, web links, phishing...

Infiltration - Human

- eMails, web links, phishing...
  - Works like a charm!

Infiltration - Human

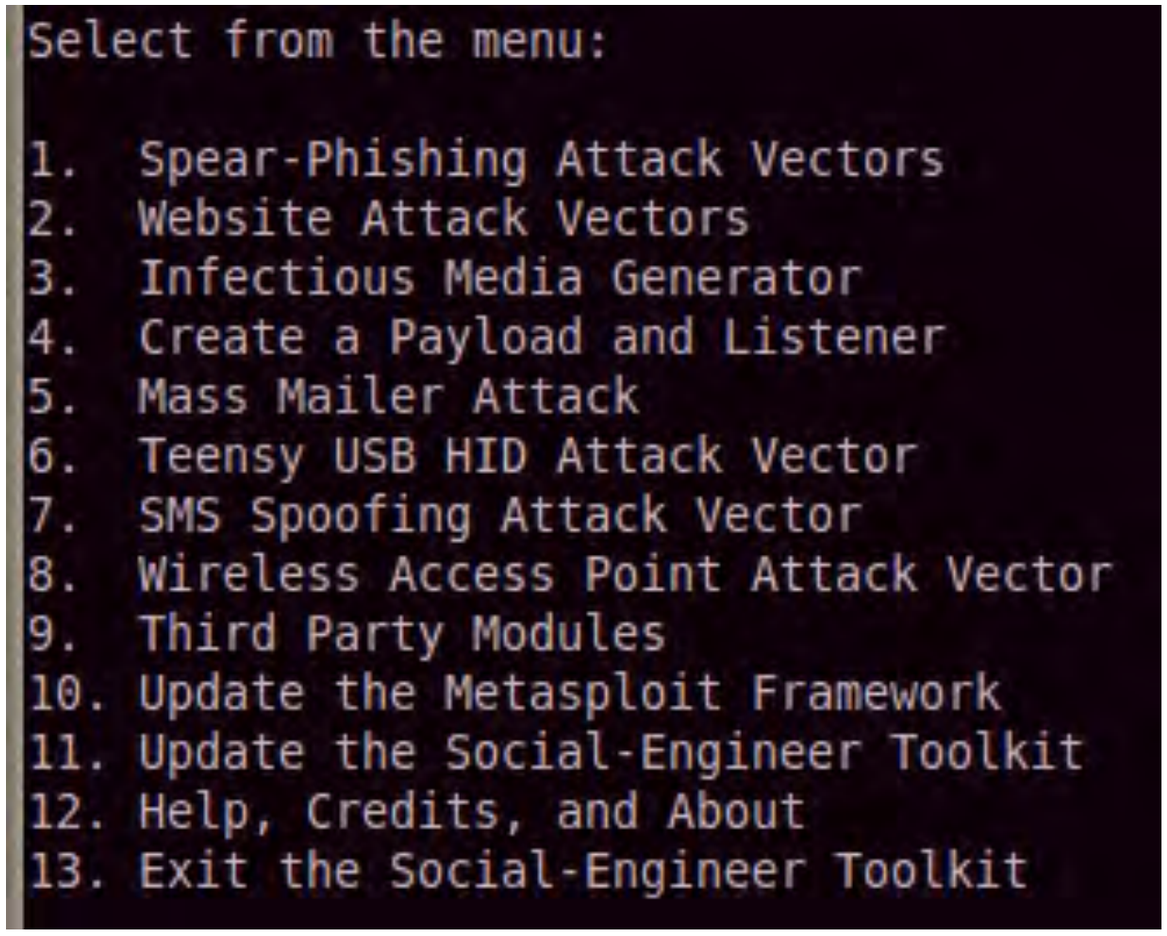
- eMails, web links, phishing...
  - Works like a charm!
- And can be mostly automated

Infiltration - Human

- eMails, web links, phishing...
  - Works like a charm!
- And can be mostly automated
  - SET to the rescue

Infiltration - Human

- eMails, web links, phishing...
  - Works like a charm!
- And can be mostly automated
  - SET to the rescue



Infiltration - Human

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

Infiltration - Human

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

Infiltration - Human

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

Infiltration - Human

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

Infiltration - Human

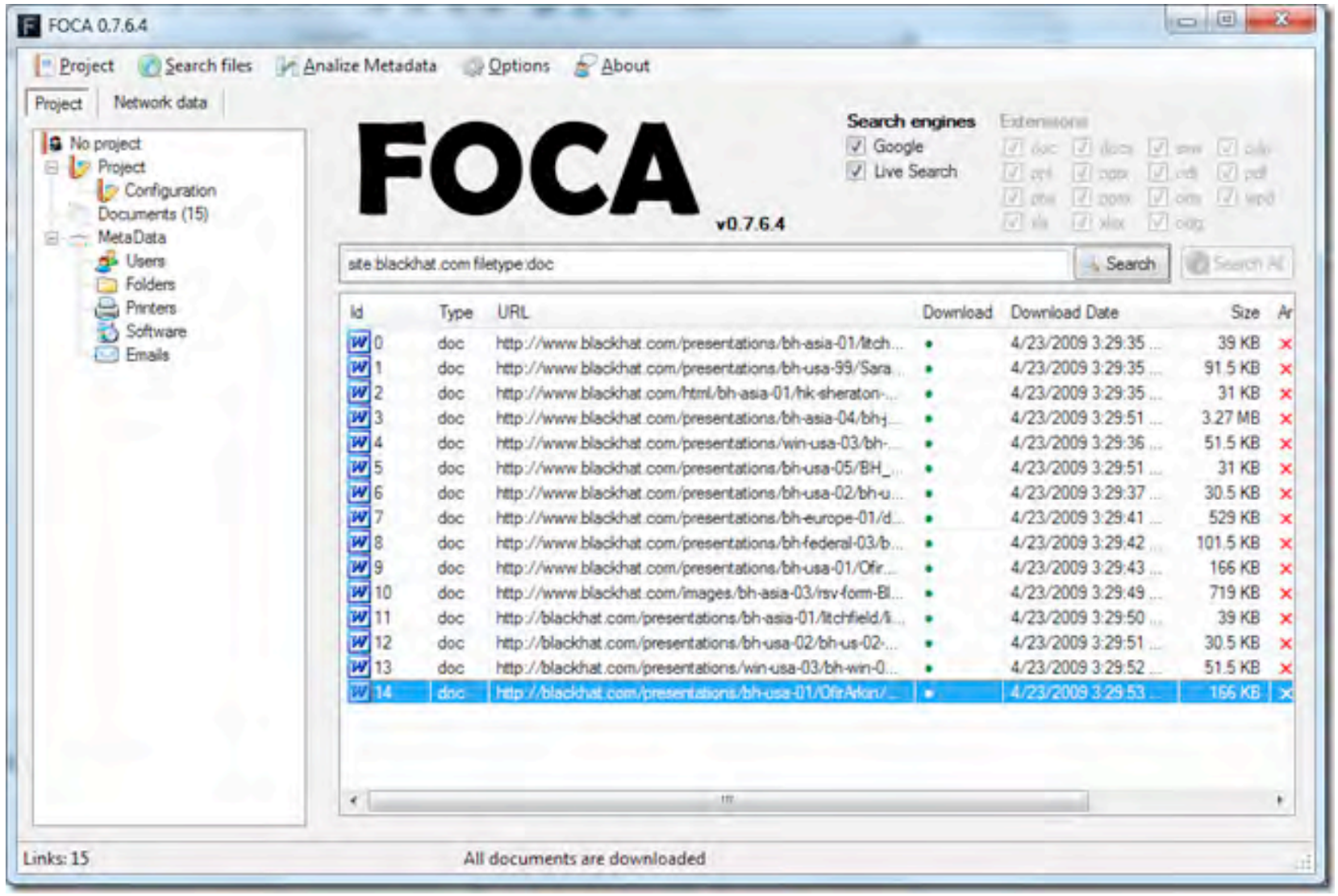
And... being nice/nasty/ obnoxious/needy always helps!

2. Data Targeting & Acquisition

- Weaponizing commercial tools
- Creating "APT" capabilities
- But first - targeting...

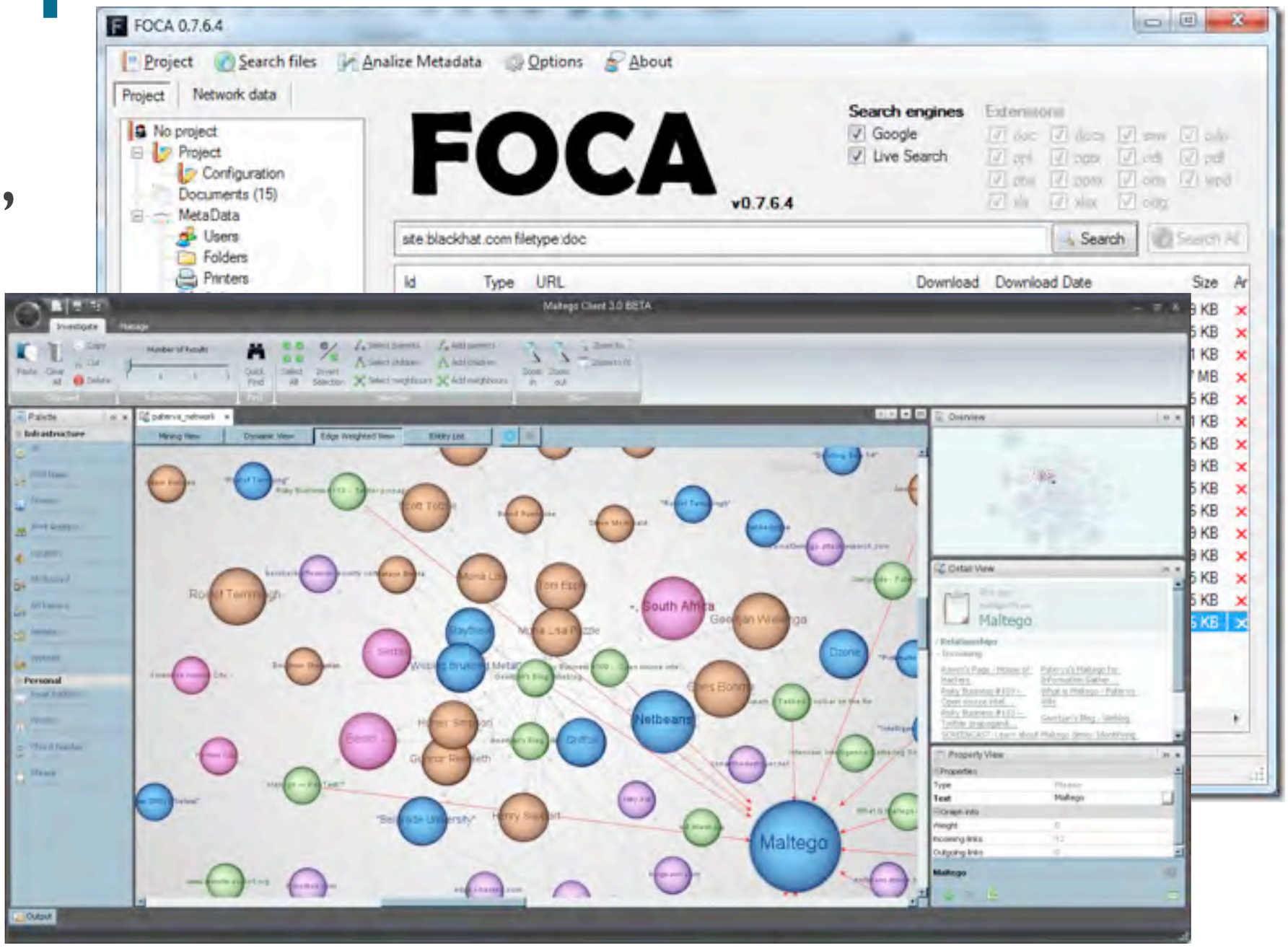
Step 1: Basic Intel

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



Step 1: Basic Intel

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



Who's your daddy?

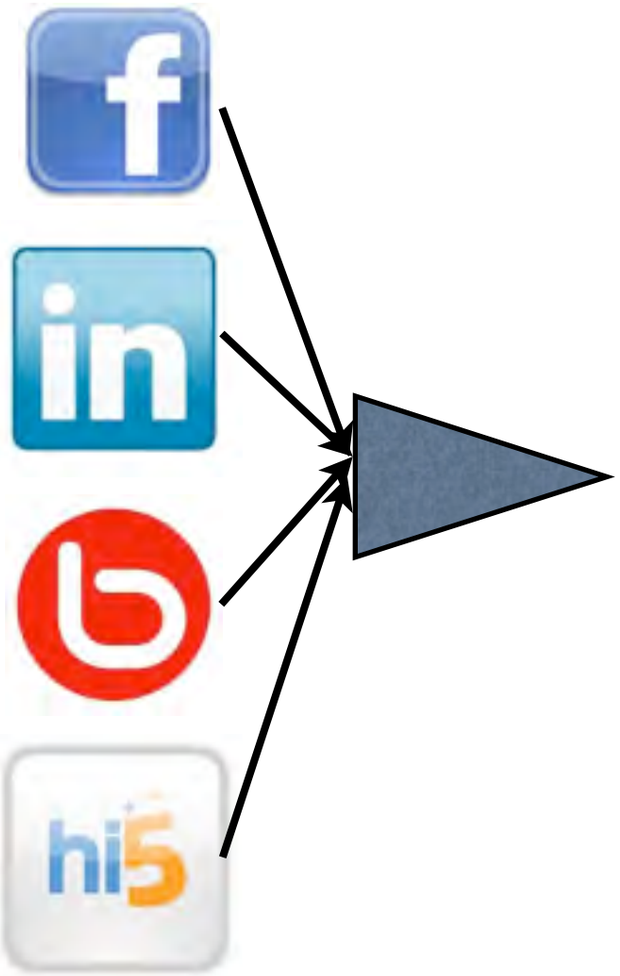
And buddy, and friends, relatives, colleagues...

Who's your daddy?

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

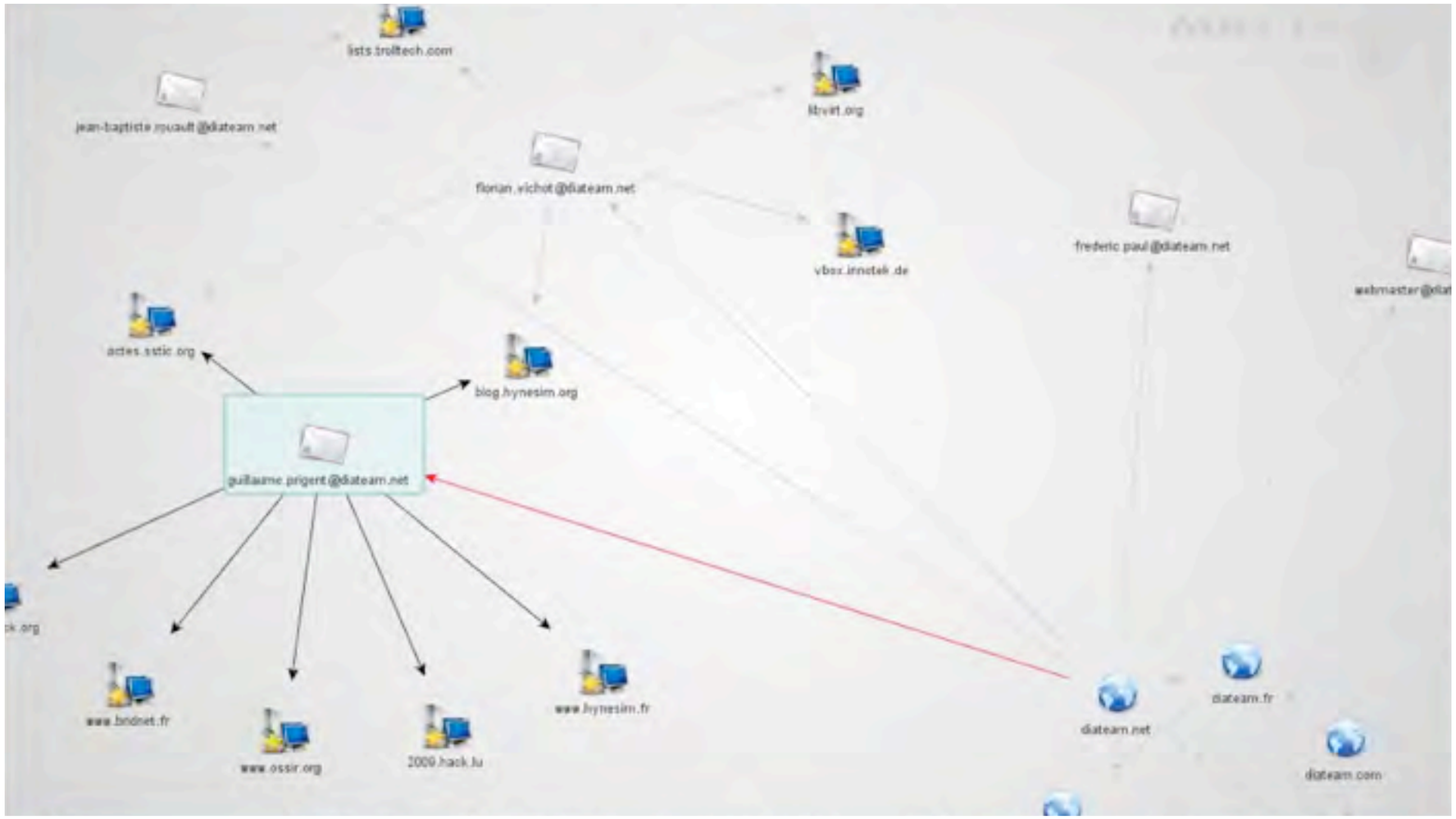
Who's your daddy?

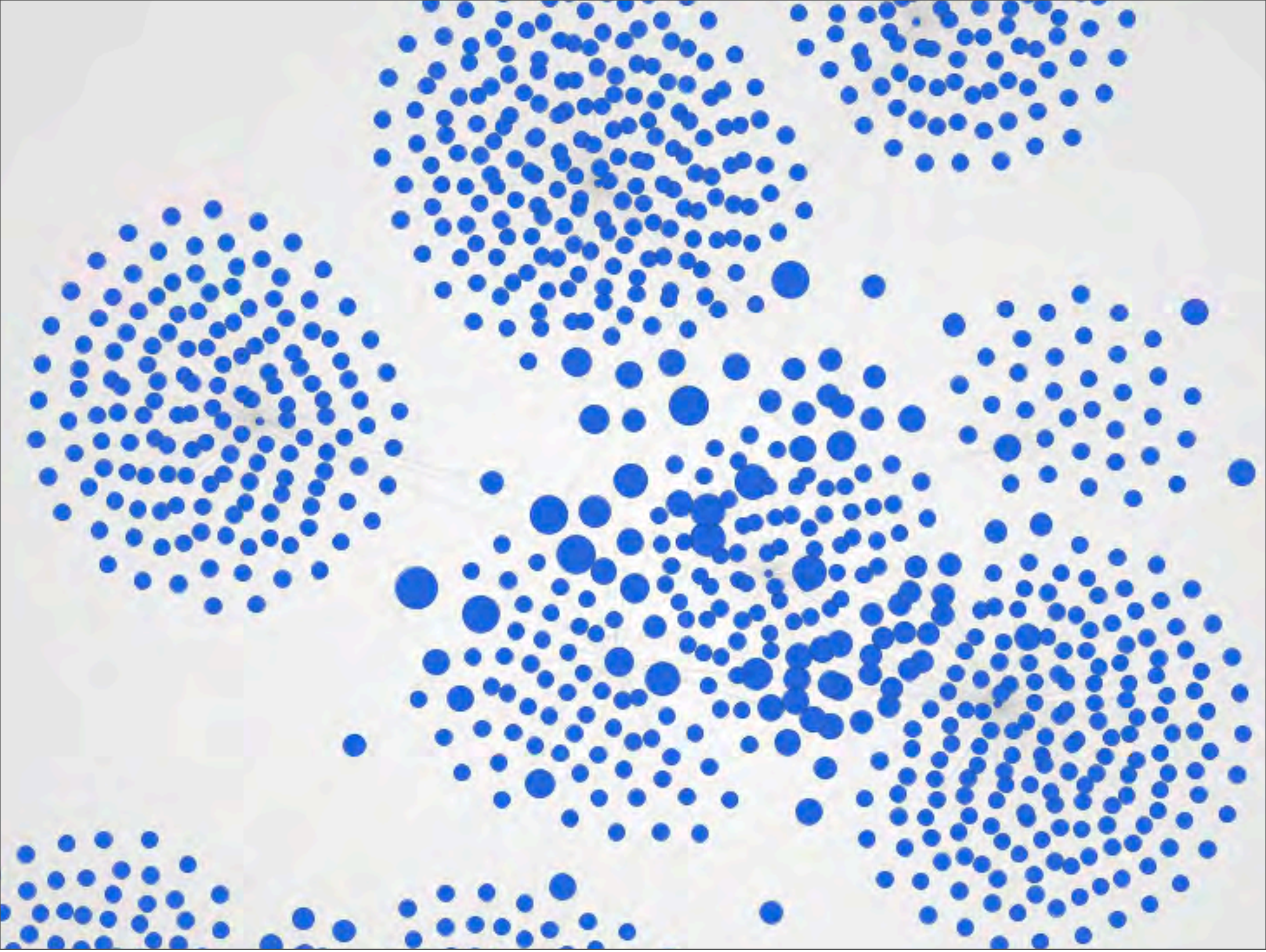
And buddy, and friends, relatives, colleagues...

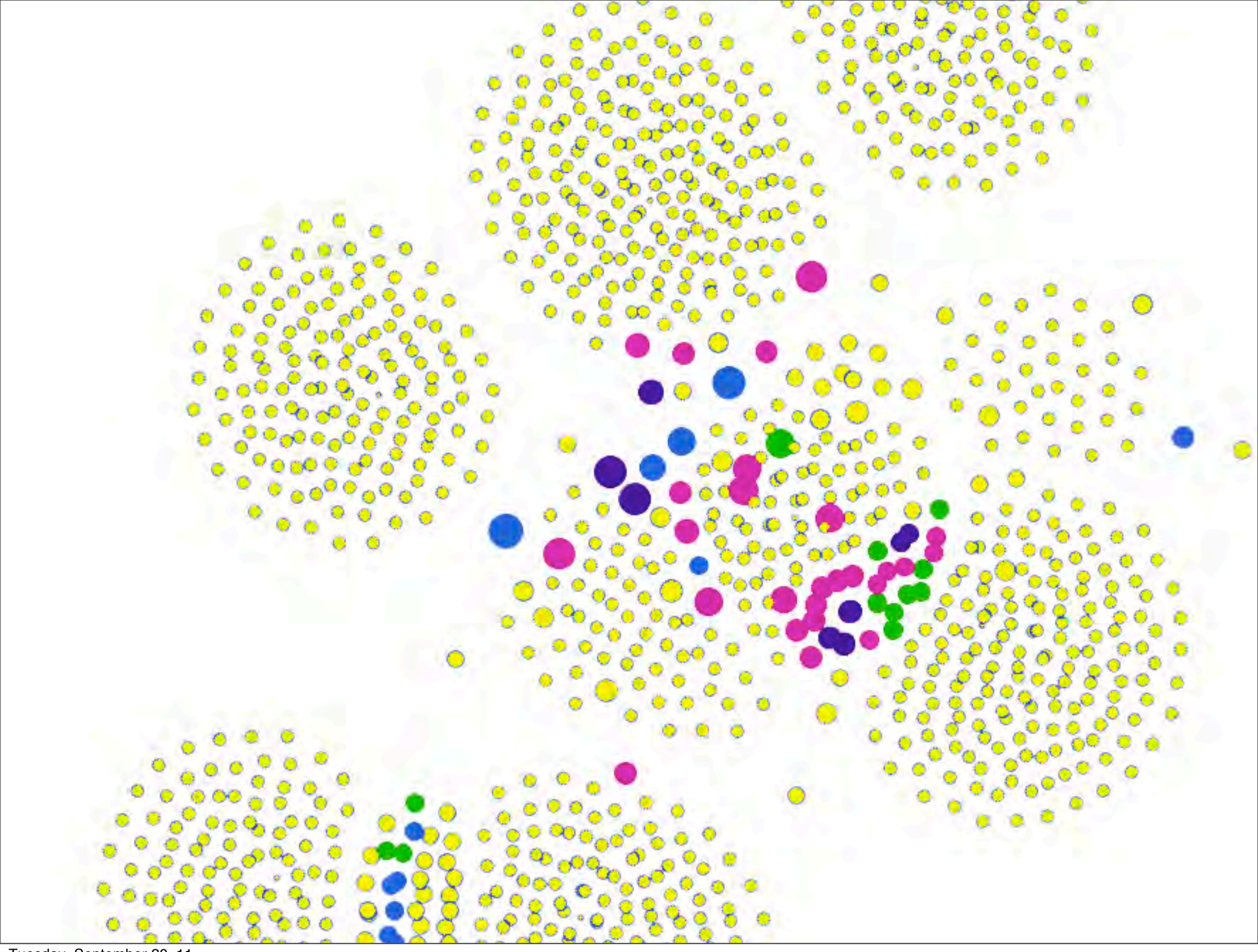


Who's your daddy?

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





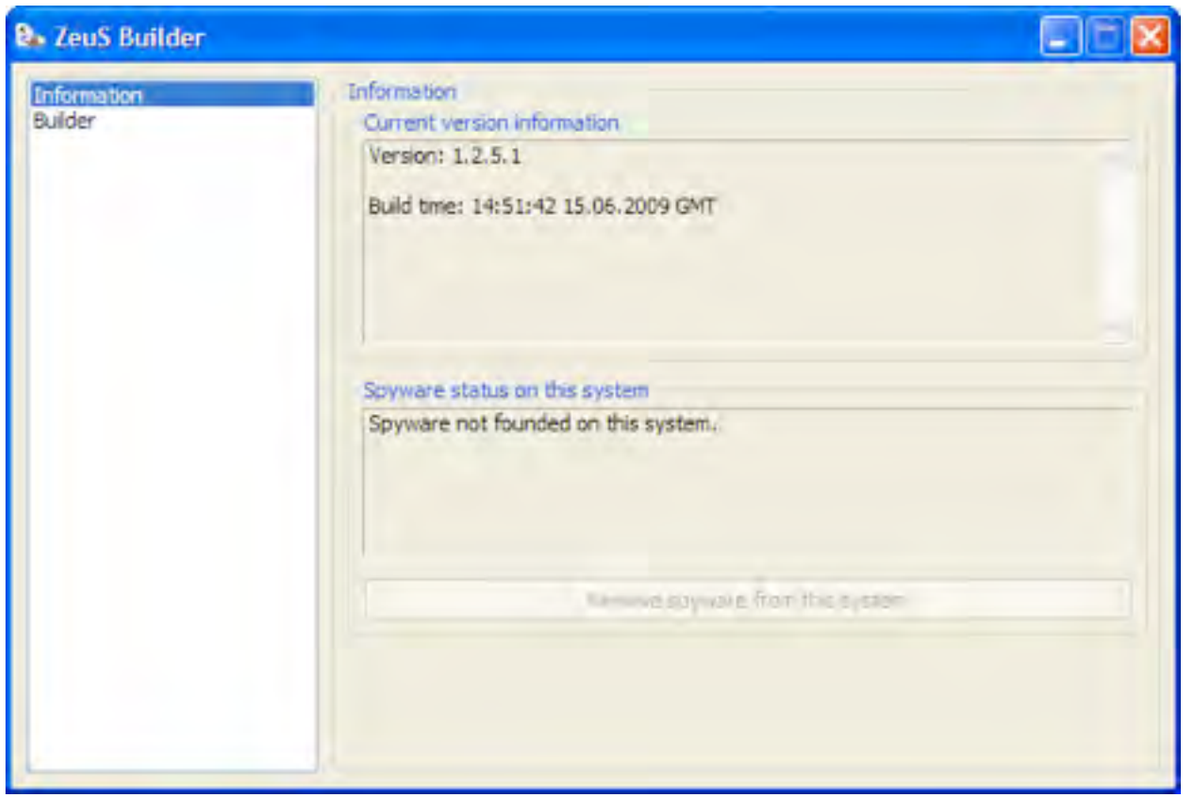


Select your target wisely

And then craft your payload :-)

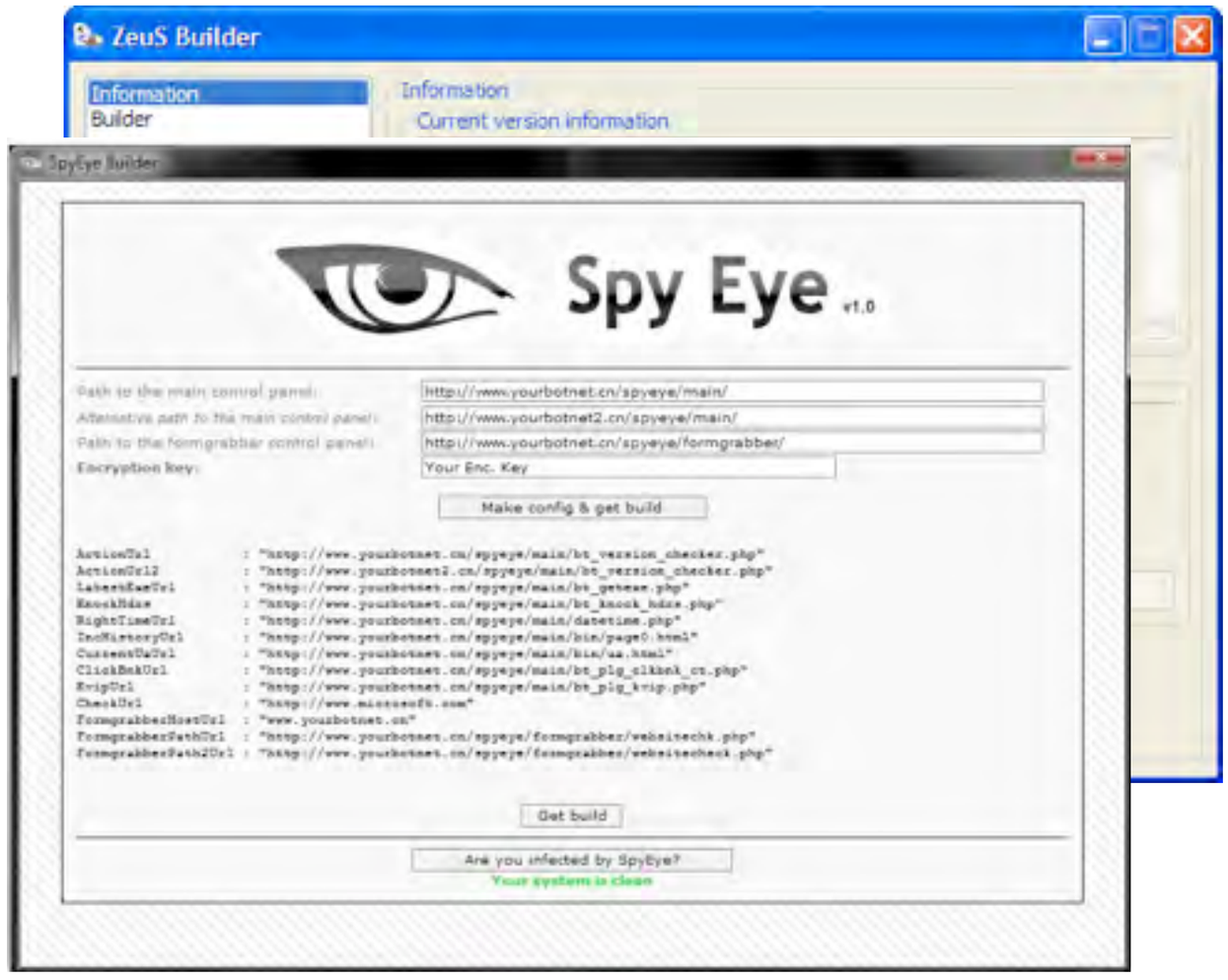
Not as expensive as you think

- ZeuS: $3000-$5000
- SpyEye: $2500-$4000
- Limbo: $500-$1500



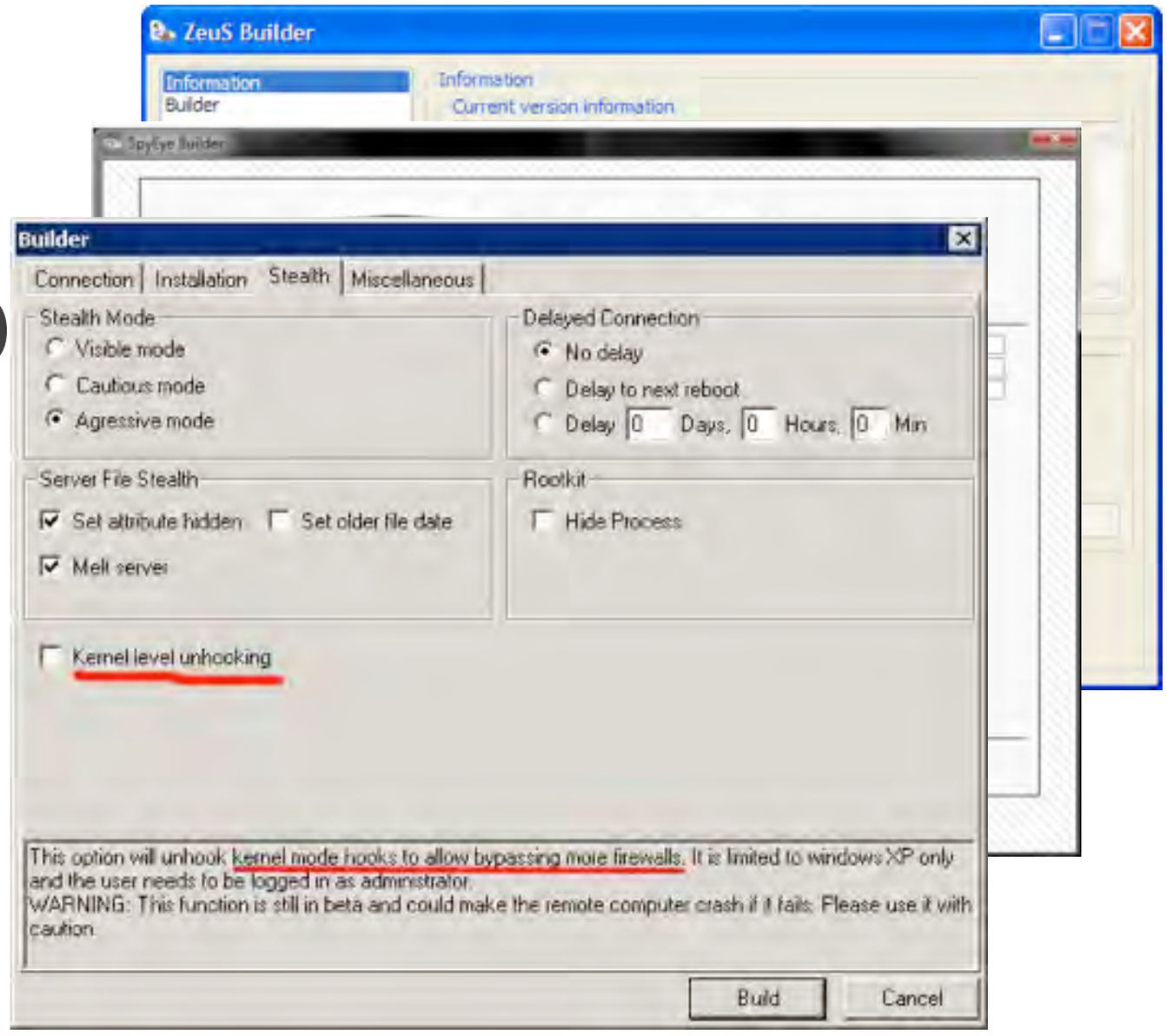
Not as expensive as you think

- ZeuS: $3000-$5000
- SpyEye: $2500-$4000
- Limbo: $500-$1500



Not as expensive as you think

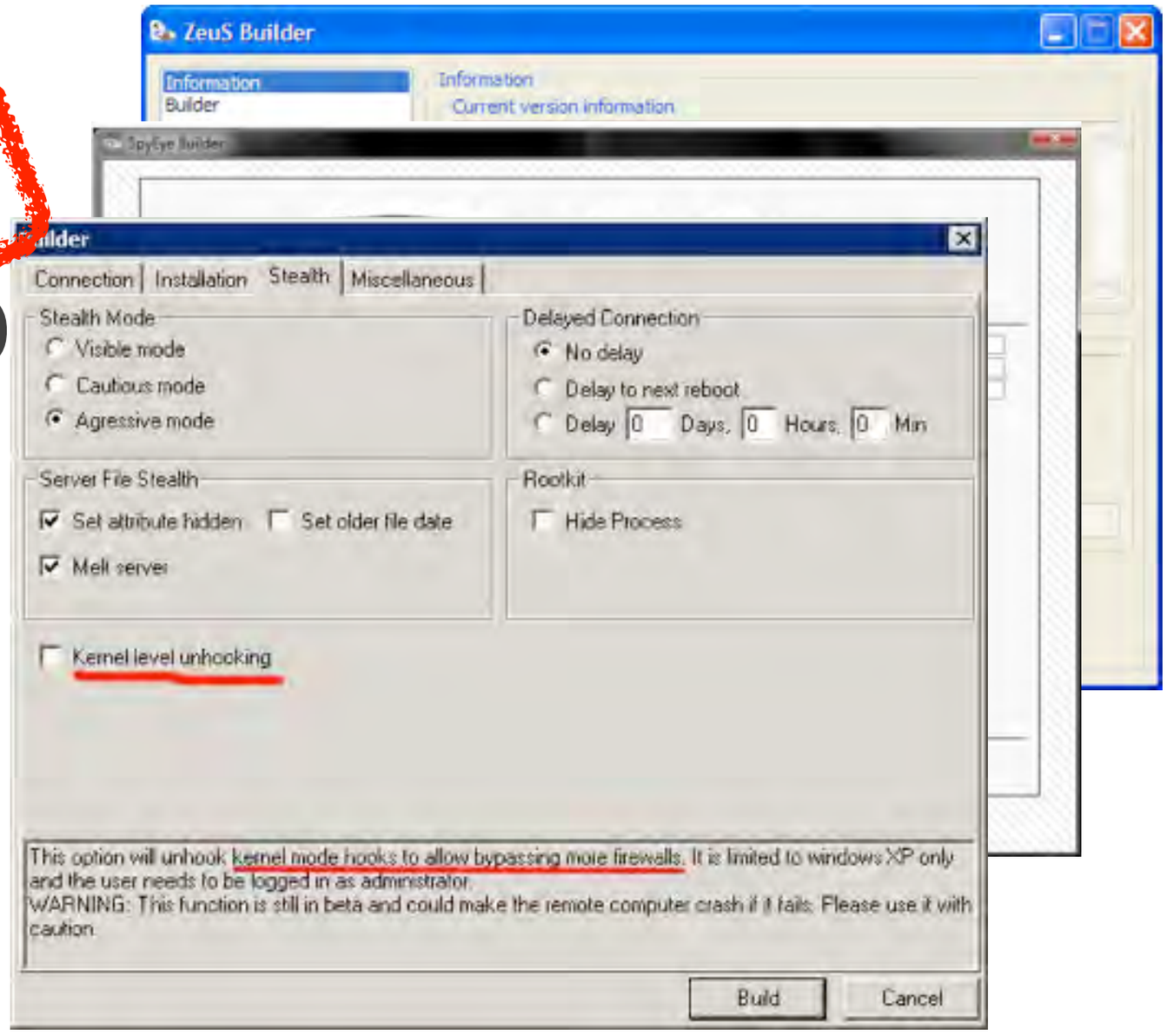
- ZeuS: $3000-$5000
- SpyEye: $2500-$400
- Limbo: $500-$1500



Not as expensive as you think

- ZeuS: $3000-$5000
- SpyEye: $2500-$400
- Limbo: $500-$1500

FREE!

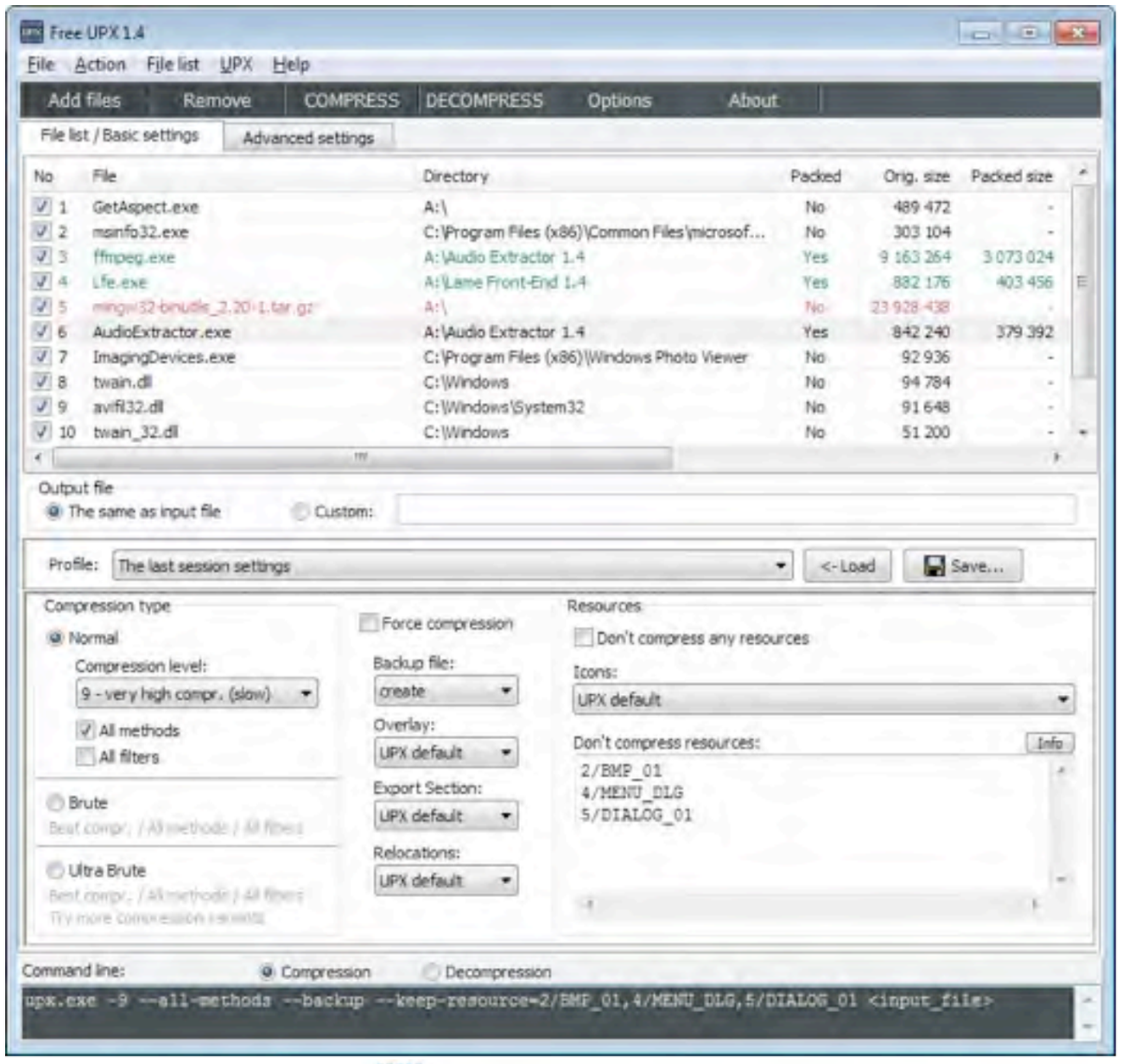


Just make sure to pack

Experienced travelers
know the importance
of packing properly

Just make sure to pack

Experienced travelers know the importance of packing properly



And set measurable goals

- File servers
- Databases
- File types
- Gateways (routes)
- Printers

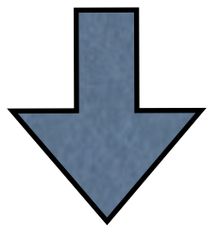
From mass infection to APT

Mass infection:
5-6 days before
detection

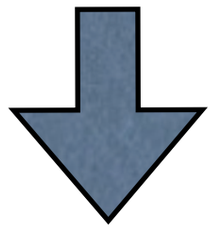
APT:
5-6 months before
detection

From mass infection to APT

Mass infection:
5-6 days before
detection



APT:
5-6 months before
detection



From mass infection to APT

Mass infection:
5-6 days before detection

Frequent updates

APT:
5-6 months before detection

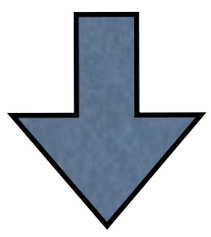
No* updates

* Almost

From mass infection to APT

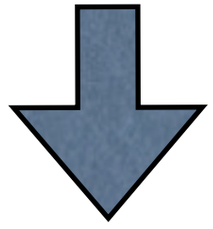
PATIENCE

Mass infection:
5-6 days before detection



Frequent updates

APT:
5-6 months before detection

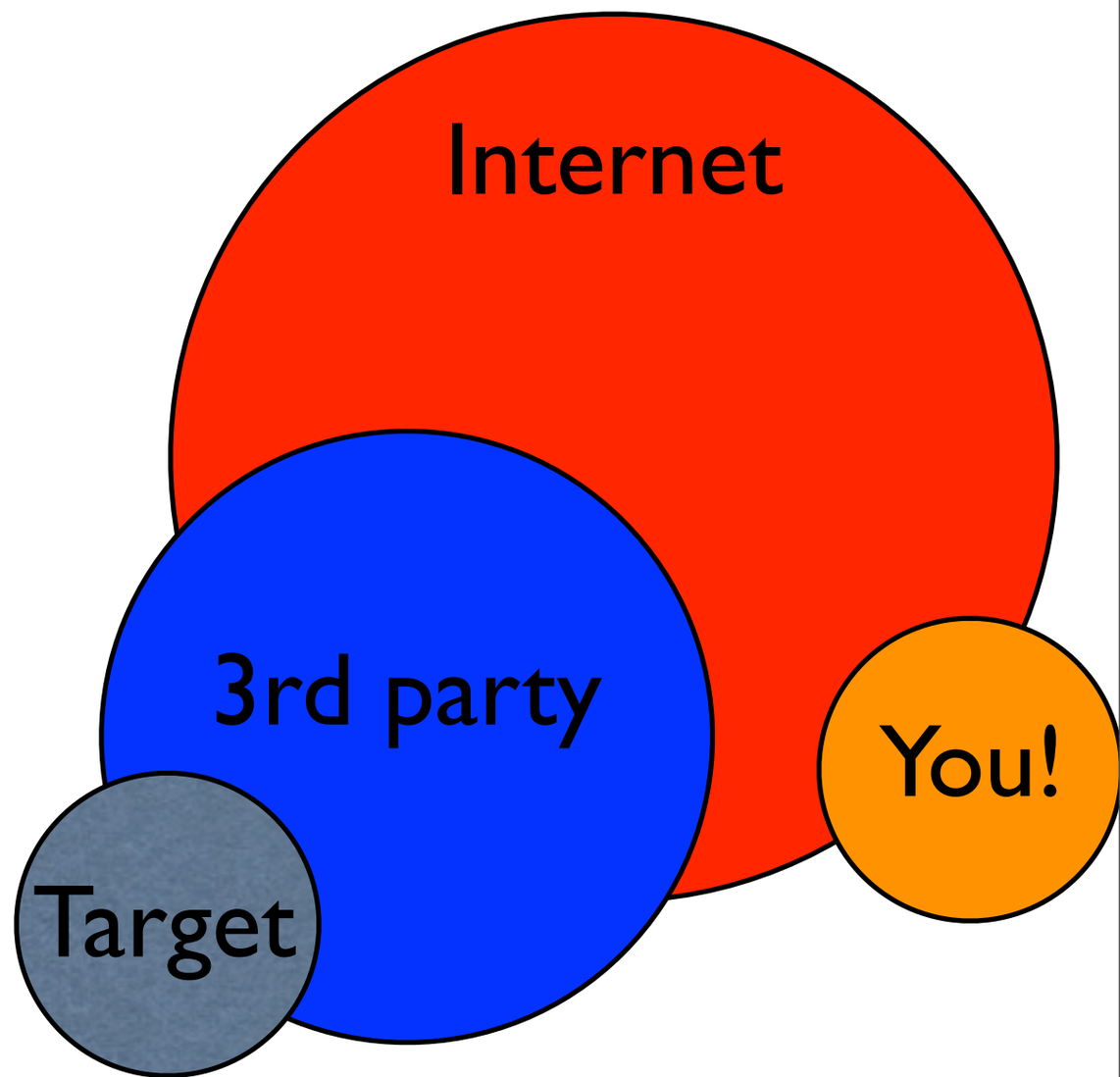


No* updates

* Almost

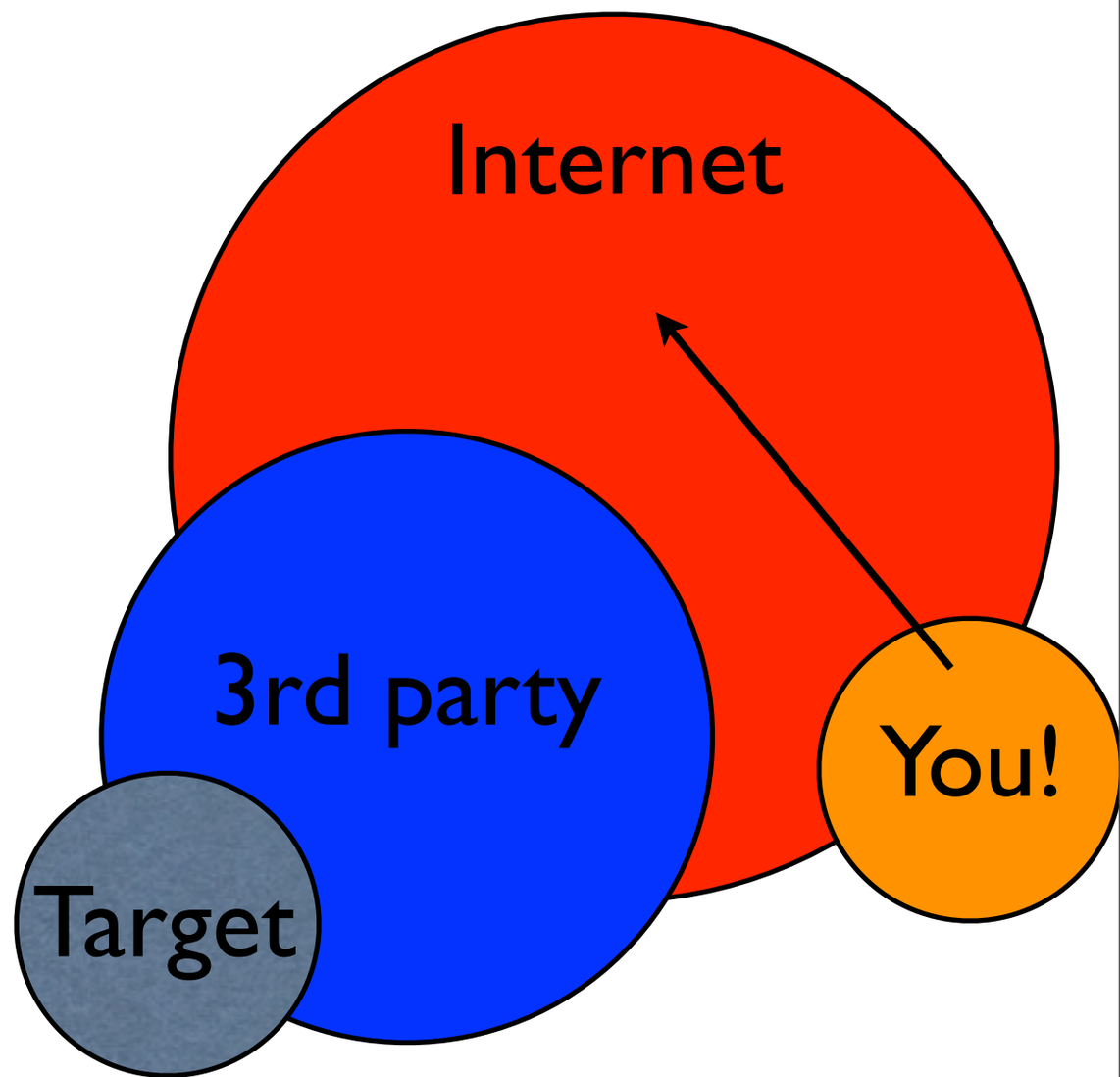
Control?

- What happens when you are so far behind?
- Just use your friends (peers)
  - Expect a one-way command scheme.
  - Exfiltration is a different animal...



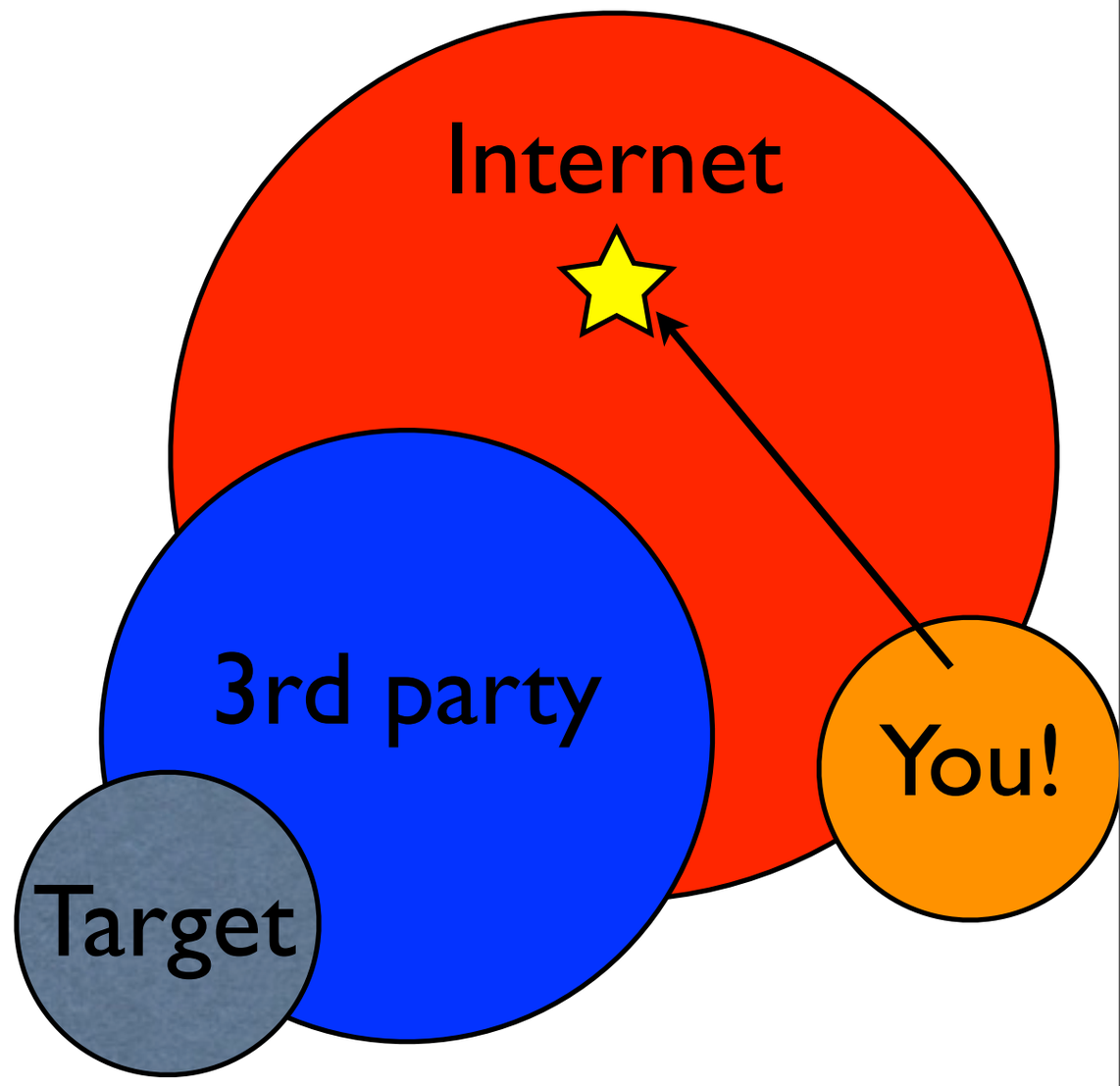
Control?

- What happens when you are so far behind?
- Just use your friends (peers)
  - Expect a one-way command scheme.
  - Exfiltration is a different animal...



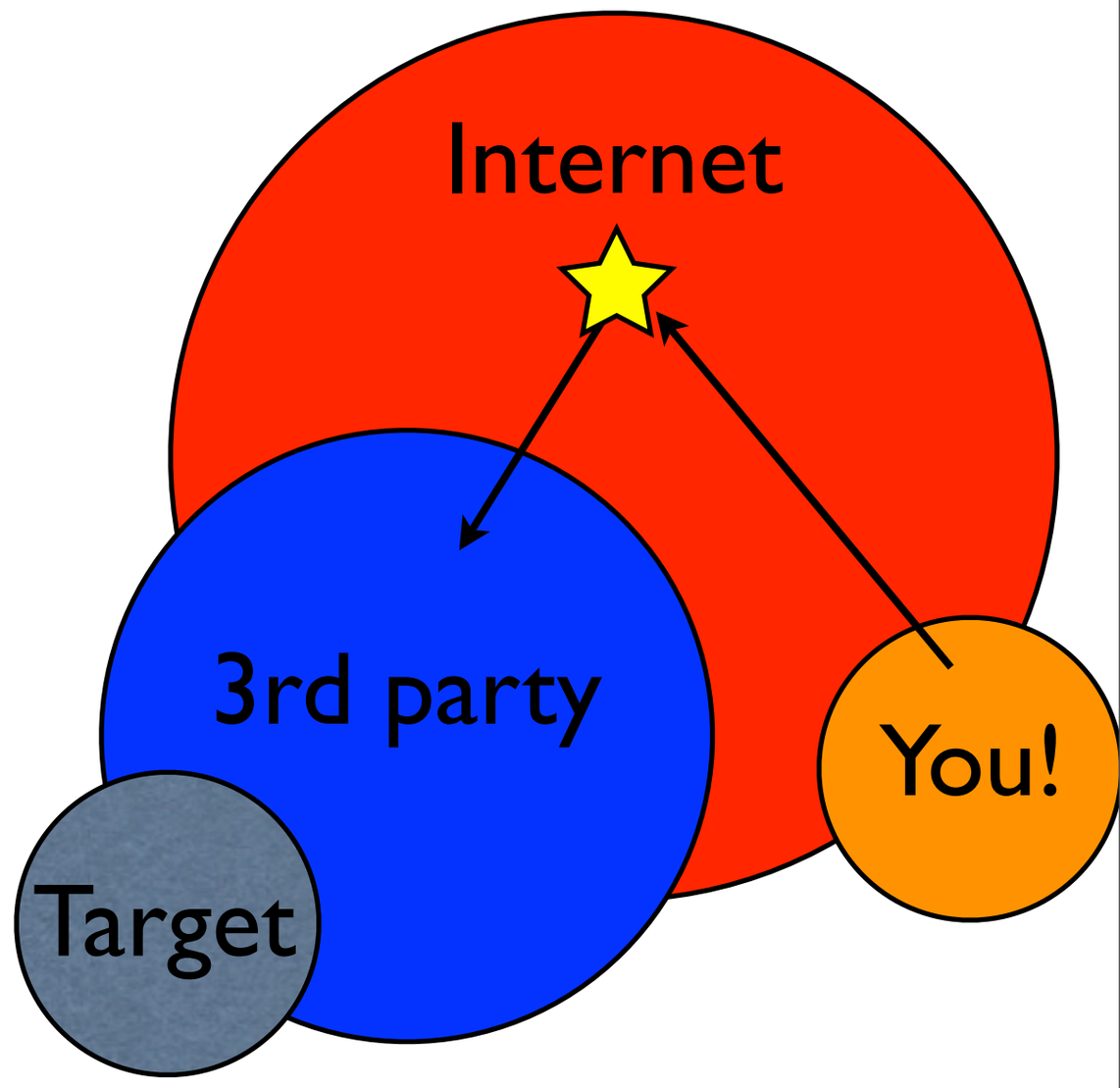
Control?

- What happens when you are so far behind?
- Just use your friends (peers)
  - Expect a one-way command scheme.
  - Exfiltration is a different animal...



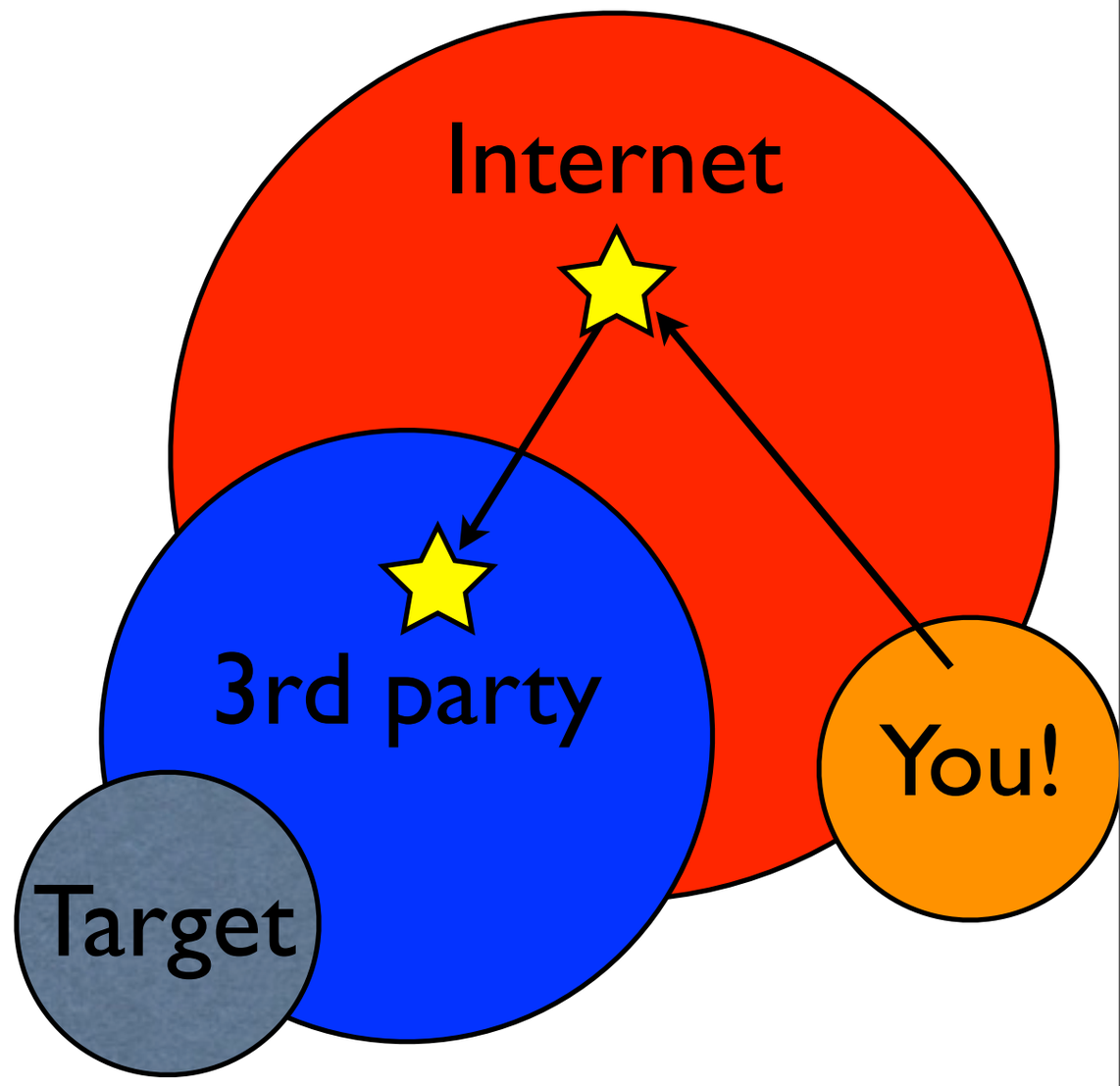
Control?

- What happens when you are so far behind?
- Just use your friends (peers)
  - Expect a one-way command scheme.
  - Exfiltration is a different animal...



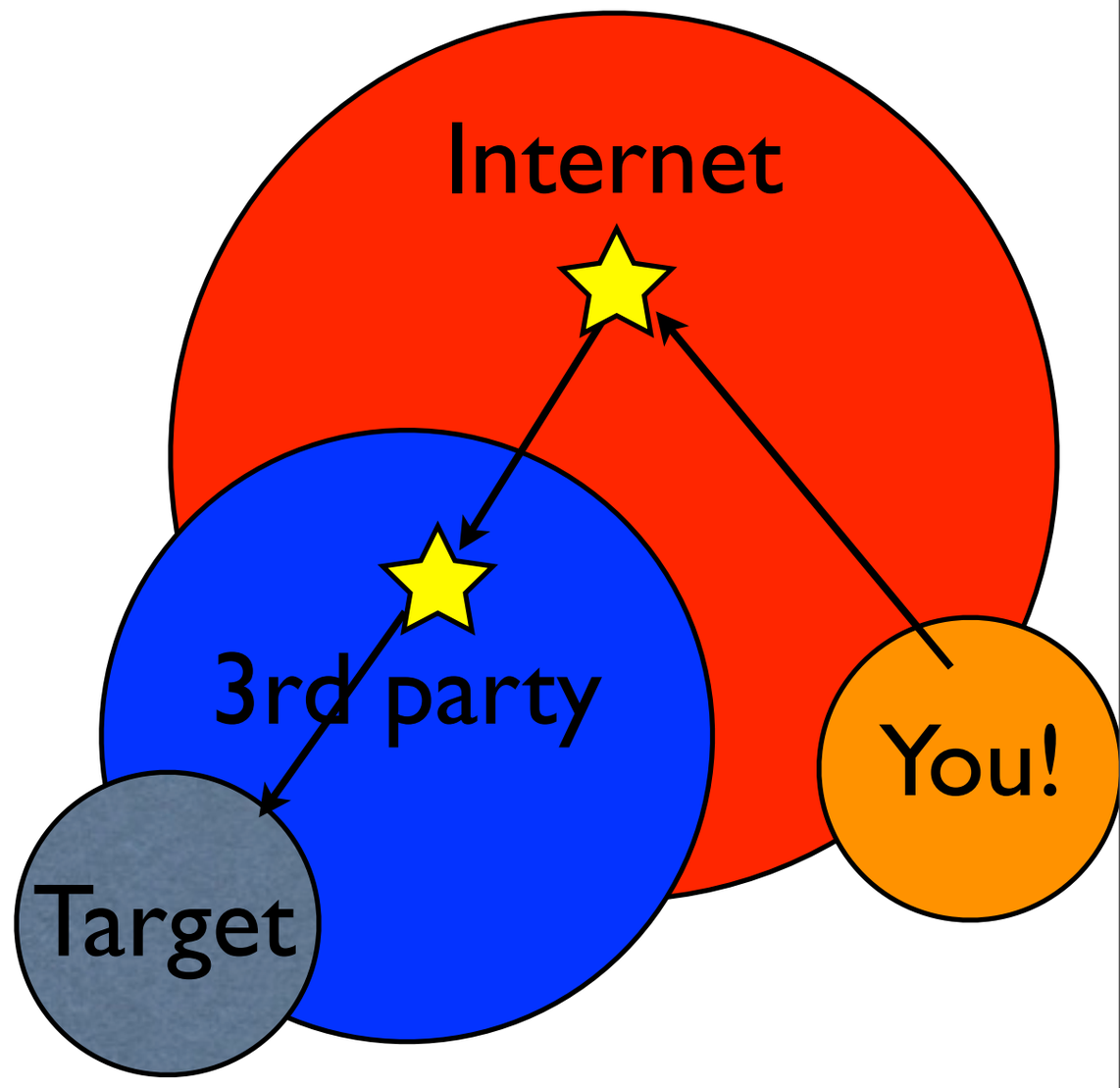
Control?

- What happens when you are so far behind?
- Just use your friends (peers)
  - Expect a one-way command scheme.
  - Exfiltration is a different animal...



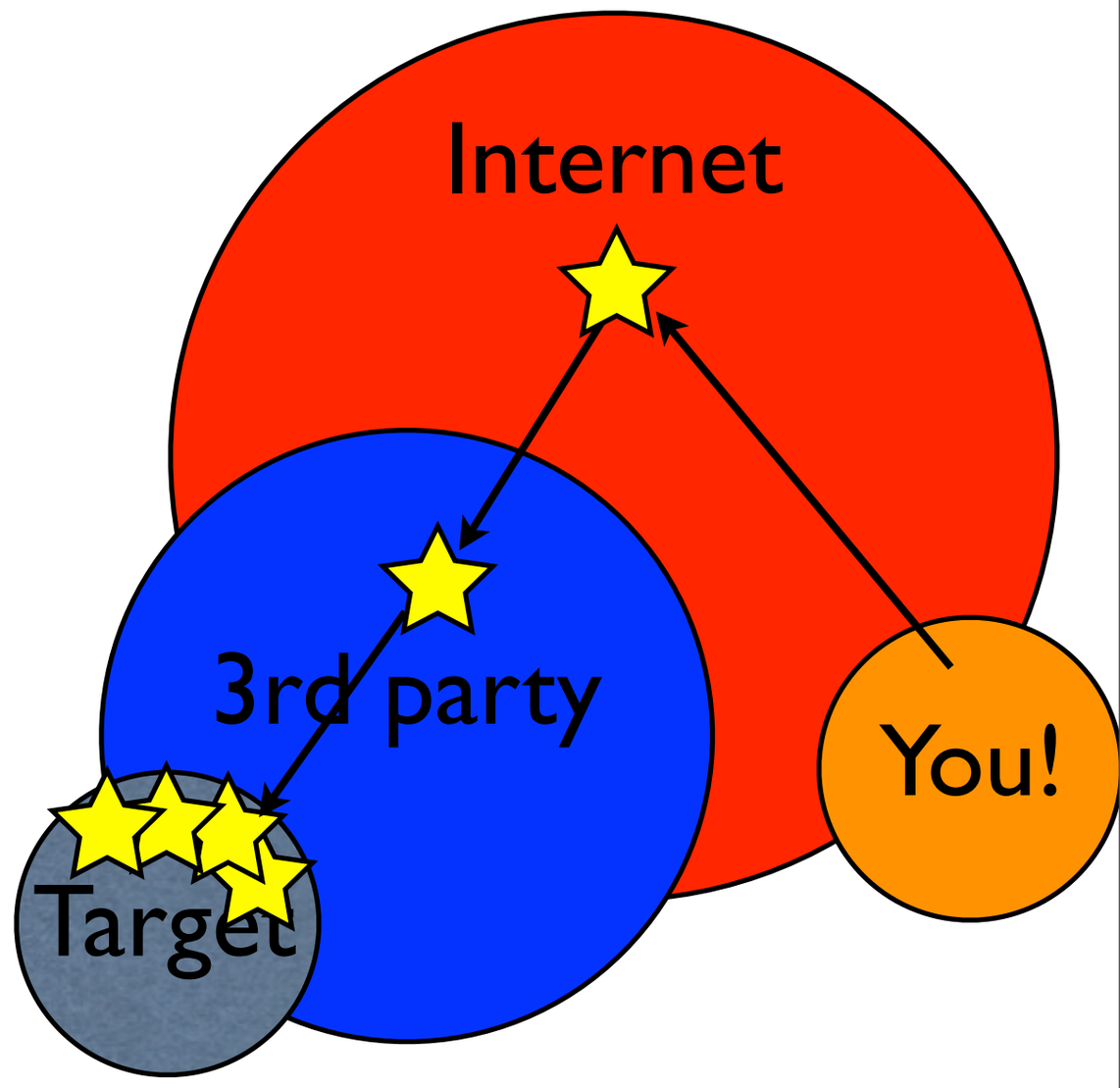
Control?

- What happens when you are so far behind?
- Just use your friends (peers)
  - Expect a one-way command scheme.
  - Exfiltration is a different animal...



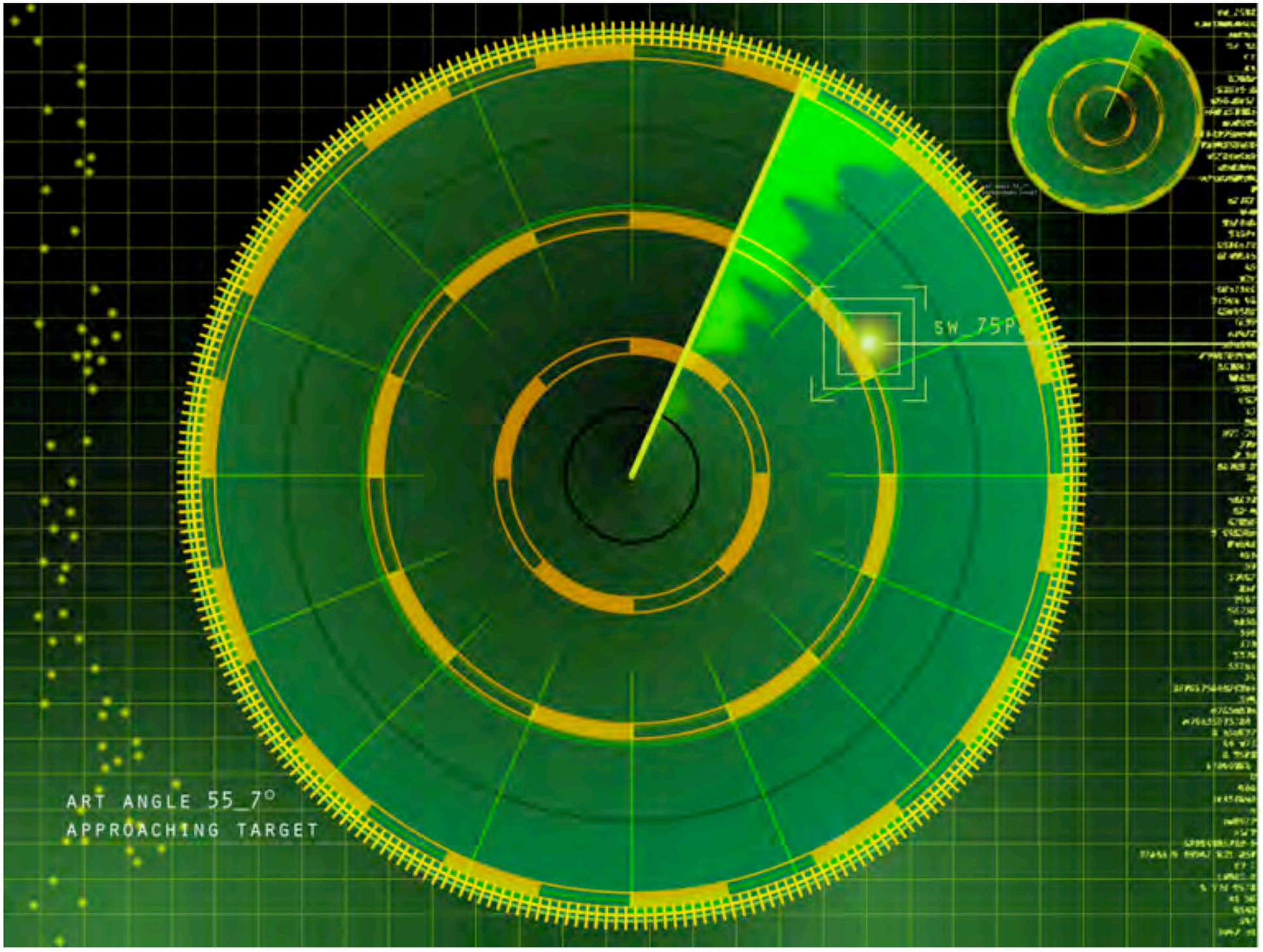
Control?

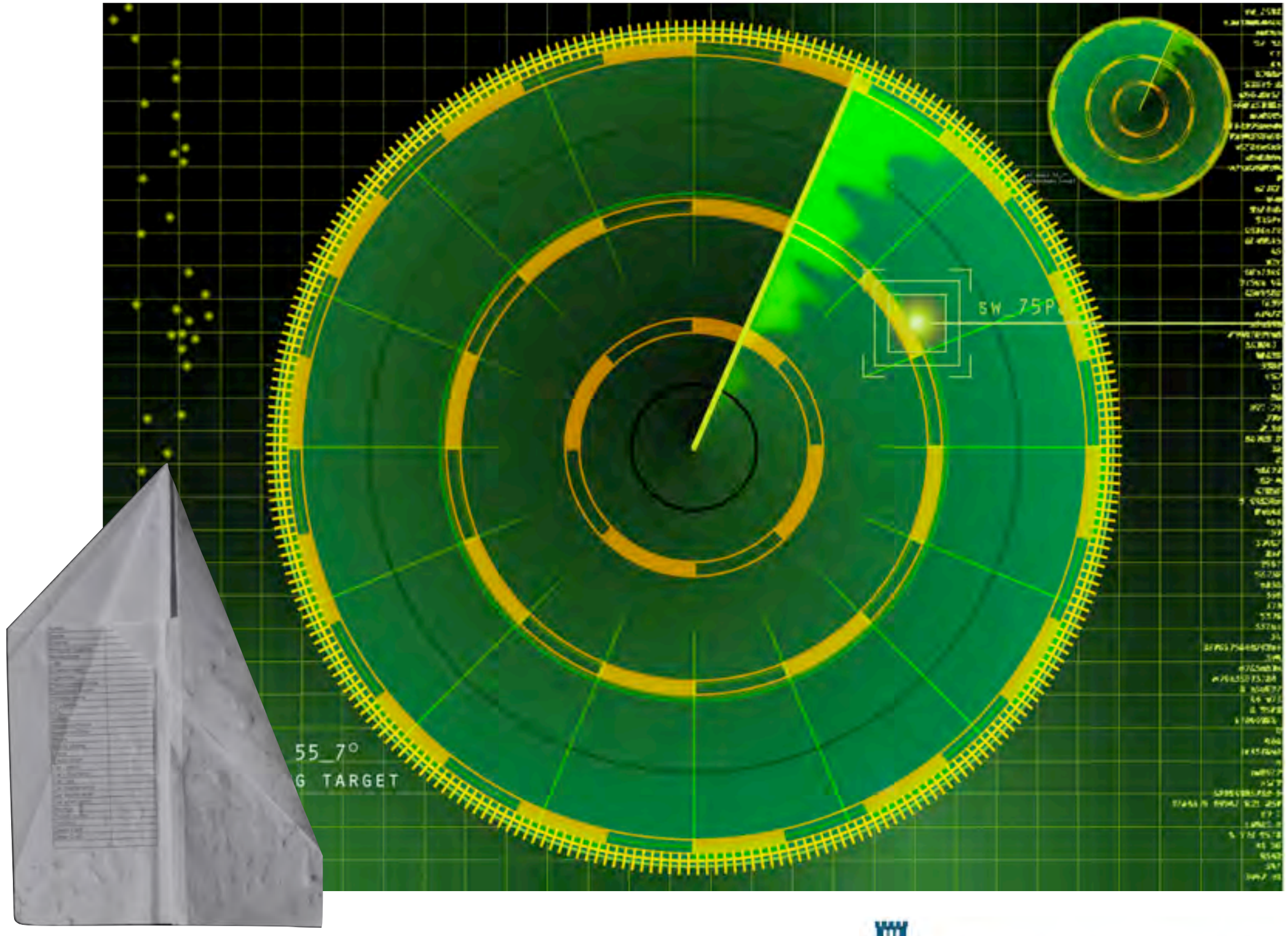
- What happens when you are so far behind?
- Just use your friends (peers)
  - Expect a one-way command scheme.
  - Exfiltration is a different animal...



3. Exfiltration

- Avoiding DLP
- Avoiding IPS/IDS egress filters
- Encryption
- Archiving
- Additional techniques





How about them SSLs?

- Cool.

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

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/Dlw43QlW/lmdBnwcWLuQmDCmwr3HuhEaOmqfO
hdgaxM4GuVdJCDdwXzwpuaPElCd18weH2XNzudLdeRKN+wjl/4D6blo+038BcLei
SyhWrMFB7mKSmEzQufQUDACFamtMCn9YOo3mgo+YYk505qhIDLNwZXqyVUqOHvIG
vu7gzuNwUdY5idLqsGEs0K0xVwYntTKUh61tNS/HDfNTVm4Y3p8M88JHhcg7npY5
gJuhWuHkgp2CTsQT+gRjthm3l3AlnIvAfuC5uWLMsjA4sCw2FRDOARxrN9El8maX
/vCxN9aB3dK4S9MSGJ5HhaYpTfpc9CdFkFryzb2sFWfW85nSzNo7dVFCy0jmSr19
o4Jsfj0J0izS3MeGYYz5NSsfBz+6o/IYURL3OXrm4DuJNHY0DvVbYqSQRRx3o2S+
uZekwXwYsqpei/f/sYo875p5NeX3g62zgjy2Vly+n58WaZWoHb5Y0QCxNfpjdcAQ
3tuZQaUvlqrkQeSRxKXD7pxlHdwHDgfvw01RU8NsMkfsBoTZY27BjFvIg5S/pv9O
6IznXaJu9jRWDj6tvSypx8X2iiVgtSHYahlqEUH1RusAMCILkx0DydCvUud/qRbT
YcnkVVgA8ojeDoVpp3AabRrSmgEAOwW6M0KvnSuMKniLIKe7koIqGjEuLAx7s5Kg
mMHfNki5dYWvQzHv03ID9UG+uW6o54BnsajEVe2EcYTPT+8pg2bCxnMEIK0ds9Is
qvf2Kx4kqO0qMeJG1Il2zfAFqmMiTMtgA2CZ0Y42hA/bQK/CCM8QVo9JcGn3Jf6N
0X1TVob7xDo/fkRROHv74dIh2Kxa0SH8iGdb4kI=
=jN3t
-----END PGP MESSAGE-----

Still "too detectable"

Still "too detectable"

hQMOA1jQIm6UkL4eEAv/W3r/eYLUmqRNi/Jegt72lK6qdBiBfkg9PZ5YKqI9CUZp
FGnVk029K3gEVcrA4k7w2aOtP7tYKRF8v4yrZQ9GZ7eXzR7+Tbf1g+7dveH6U8Bf
BHo8LRovj5OlGghrvpyKYRPlf/NAgzL2G8dyi/FVB0YB4J7/4x0YFEalQHaLiKyt
/gkikyV92njPJ6tPm2sdKUqUHSb20r9AdowZ0VVRrWwdRgUhdNXajjwcbH1BjVuS
Gilw8MnmQkmJAT+TAFkTqC9fjiwtnNMNANJbo2Z36RqsAcKbhVh1eMA7ev0pUakp
Tm4xN64syk/1DEc0VHFbanAreTV3tCbUUloPQDFGFpiu3oS6/089oUvRtBBbC5p6
leYKEnDIlcGWAomRSiYBFWjTca/DIw43QIW/ImdBnwcWLuQmDCmwr3HuhEaOmqfO
hdgaxM4GuVdJCDdwXzwpuaPElCd18weH2XNzudLdeRKN+wjl/4D6bIo+038BcLei
SyhWrMFB7mKSmEzQufQUDACFamtMCn9YOo3mgo+YYk505qhIDLNwZXqyVUqOHvIG
vu7gzuNwUdY5idLqsGEs0K0xVwYntTKUh61tNS/HDfNTVm4Y3p8M88JHhcg7npY5
gJuhWuHkgp2CTsQT+gRjthm3l3AlnIvAfuC5uWLMsjA4sCw2FRDOARxrN9El8maX
/vCxN9aB3dK4S9MSGJ5HhaYpTfpc9CdFkFryzb2sFWfW85nSzNo7dVFCy0jmSr19
o4Jsfj0J0izS3MeGYYz5NSsfBz+6o/IYURL3OXrm4DuJNHY0DvVbYqSQRRx3o2S+
uZekwXwYsqpei/f/sYo875p5NeX3g62zgjy2Vly+n58WaZWoHb5Y0QCxNfpjdcAQ
3tuZQaUvlqrkQeSRxKXD7pxlHdwHDgfvw01RU8NsMkfsBoTZY27BjFvIg5S/pv9O
6IznXaJu9jRWDj6tvSypx8X2iiVgtSHYahlqEUH1RusAMCILkx0DydCvUud/qRbT
YcnkVVgA8ojeDoVpp3AabRrSmgEAOwW6M0KvnSuMKniLIKe7kolqGjEuLAx7s5Kg
mMHfNki5dYWvQzHv03ID9UG+uW6o54BnsajEVe2EcYTPT+8pg2bCxnMEIK0ds9Is
qvf2Kx4kqO0qMeJG1Il2zfAFqmMiTMtgA2CZ0Y42hA/bQK/CCM8QVo9JcGn3Jf6N
0X1TVob7xDo/fkRROHv74dIh2Kxa0SH8iGdb4kI=
=jN3t

Much better

- Throws in some additional encodings
- And an XOR for old time's sake

- And we are good to go...
  - 0% detection rate

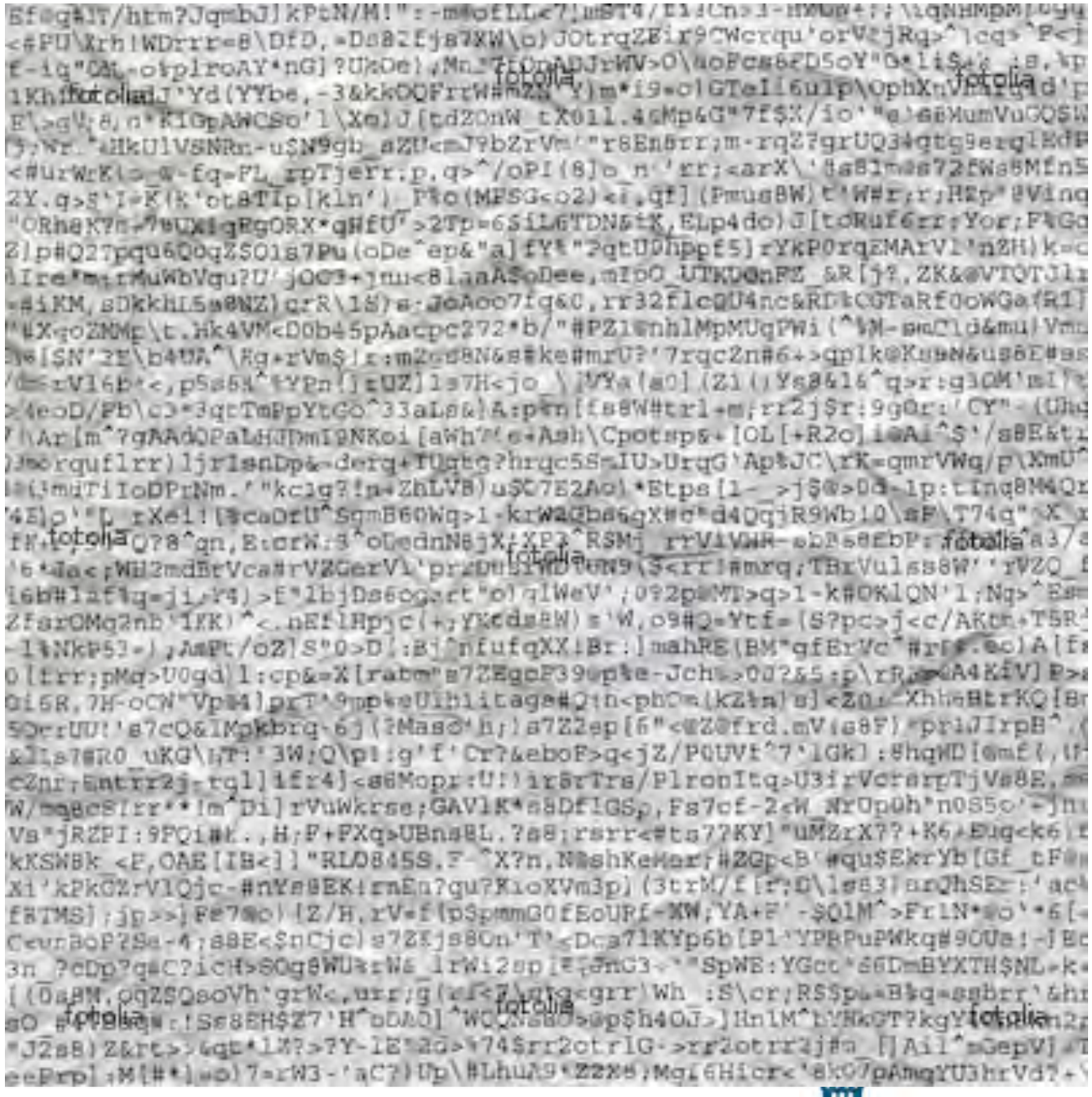
Resistance is futile

But you have no network

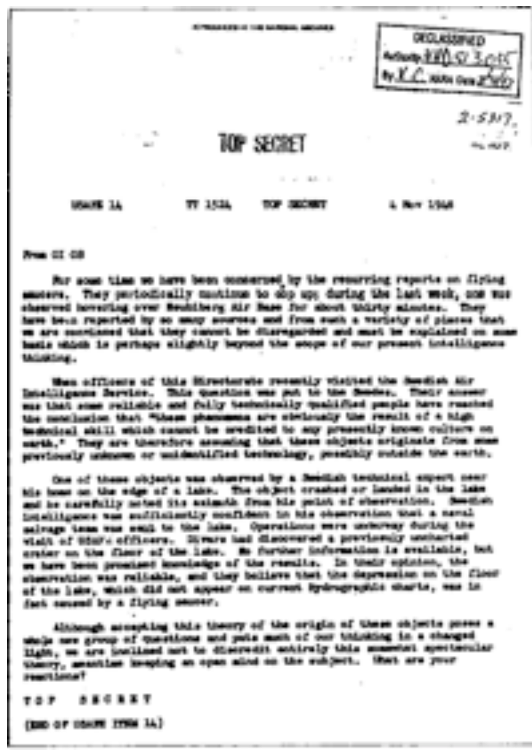
- They killed 80, 443, 53 and cut the cable to the interwebs!

- Go old-school!

Kill some trees

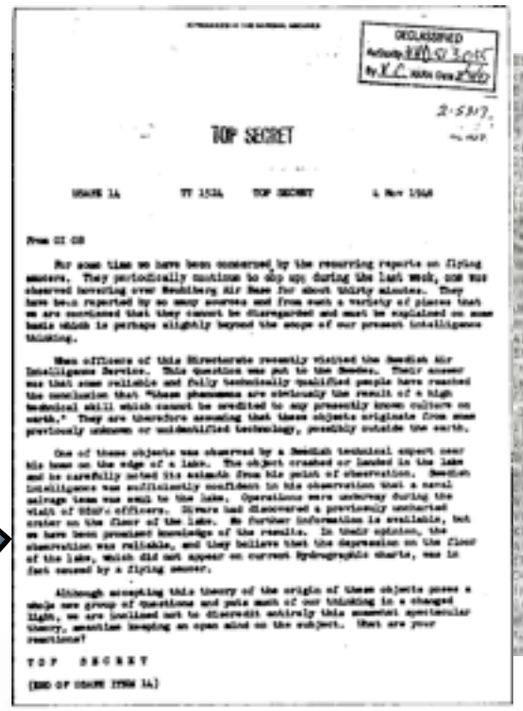


To shred or not to shred?



Going above and beyond traditional security

To shred or not to shred?


TOP SECRET

USAFE 14 TT 1534 TOP SECRET 4 Nov 1968

From CC CB

For some time we have been concerned by the recurring reports on flying saucers. They periodically continue to pop up; during the last week, one was observed hovering over Sondrberg Air Base for about thirty minutes. They have been reported by so many sources and from such a variety of places that we are convinced that they cannot be disregarded and must be explained on some basis which is perhaps slightly beyond the scope of our present intelligence thinking.

When officers of this Directorate recently visited the Swedish Air Intelligence Service, this question was put to the Swedes. Their answer was that some reliable and fully technically qualified people have reached the conclusion that "these phenomena are obviously the result of a high technical skill which cannot be credited to any presently known culture on earth." They are therefore assuming that these objects originate from some previously unknown or unidentified technology, possibly outside the earth.

One of these objects was observed by a Swedish technical expert near his home on the edge of a lake. The object crashed or landed in the lake and he carefully noted its azimuth from his point of observation. Swedish intelligence was sufficiently confident in his observation that a naval salvage team was sent to the lake. Operations were underway during the visit of USAF officers. Divers had discovered a previously uncharted crater on the floor of the lake. No further information is available, but we have been promised knowledge of the results. In their opinion, the observation was reliable, and they believe that the depression on the floor of the lake, which did not appear on current hydrographic charts, was in fact caused by a flying saucer.

Although accepting this theory of the origin of these objects poses a whole new group of questions and puts much of our thinking in a changed light, we are inclined not to discredit entirely this somewhat spectacular theory, meantime keeping an open mind on the subject. What are your reactions?

TOP SECRET

(END OF USAFE 17986 14)

Yeah, good ol'e DD...

Back to hi-tech (?)

ET Phone Home

Back to hi-tech (?)

ET Phone Home

Got VOIP?

Back to hi-tech (?)

ET Phone Home

Got VOIP? Excellent!

Back to hi-tech (?)
ET Phone Home

Got VOIP? Excellent!

Target a handset/switch

Back to hi-tech (?)

ET Phone Home

Got VOIP? Excellent!

Target a handset/switch

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

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

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

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

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

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

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

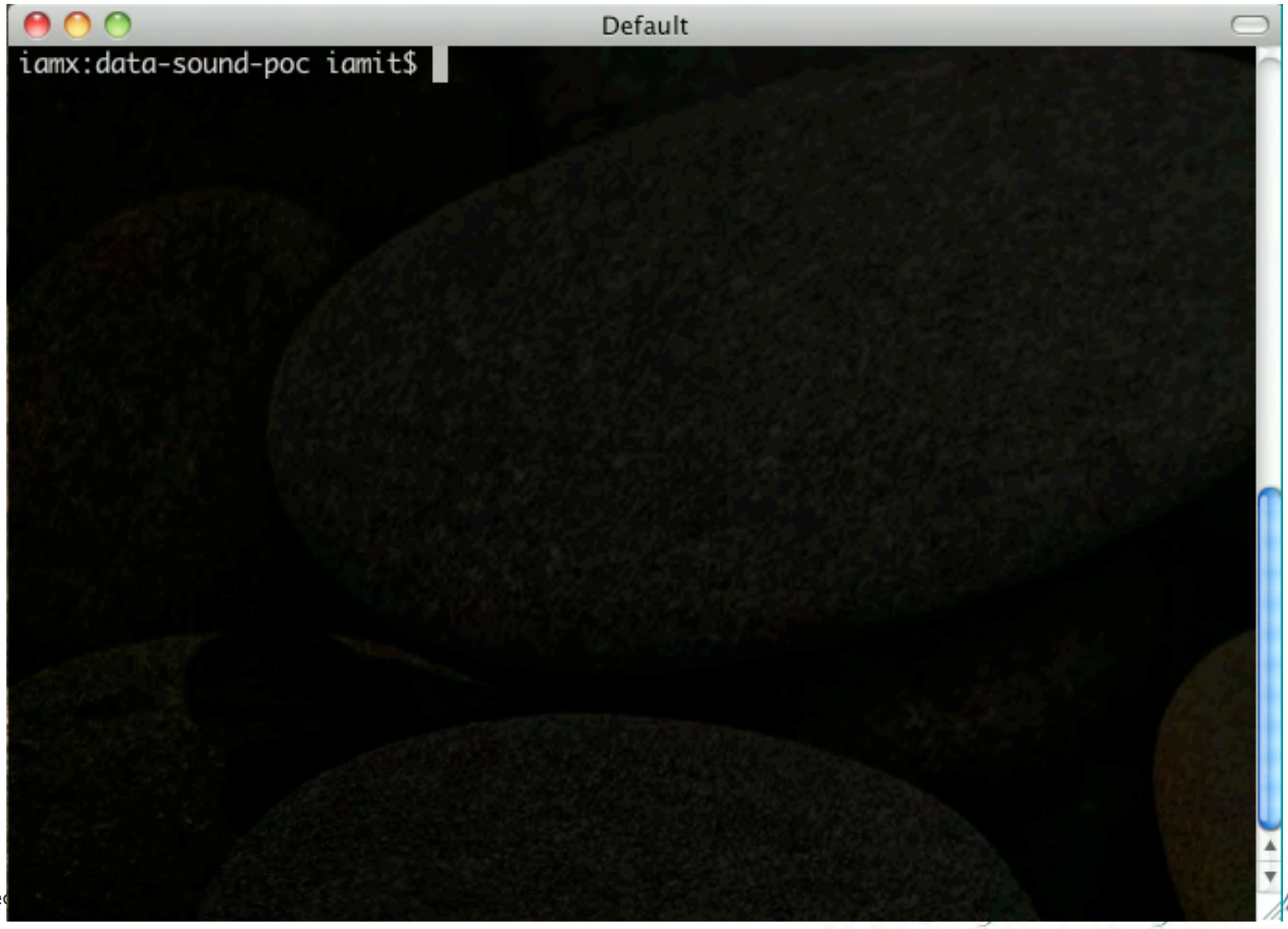
Collect your data

Encode

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

Voice exfiltration demo

Voice exfiltration demo



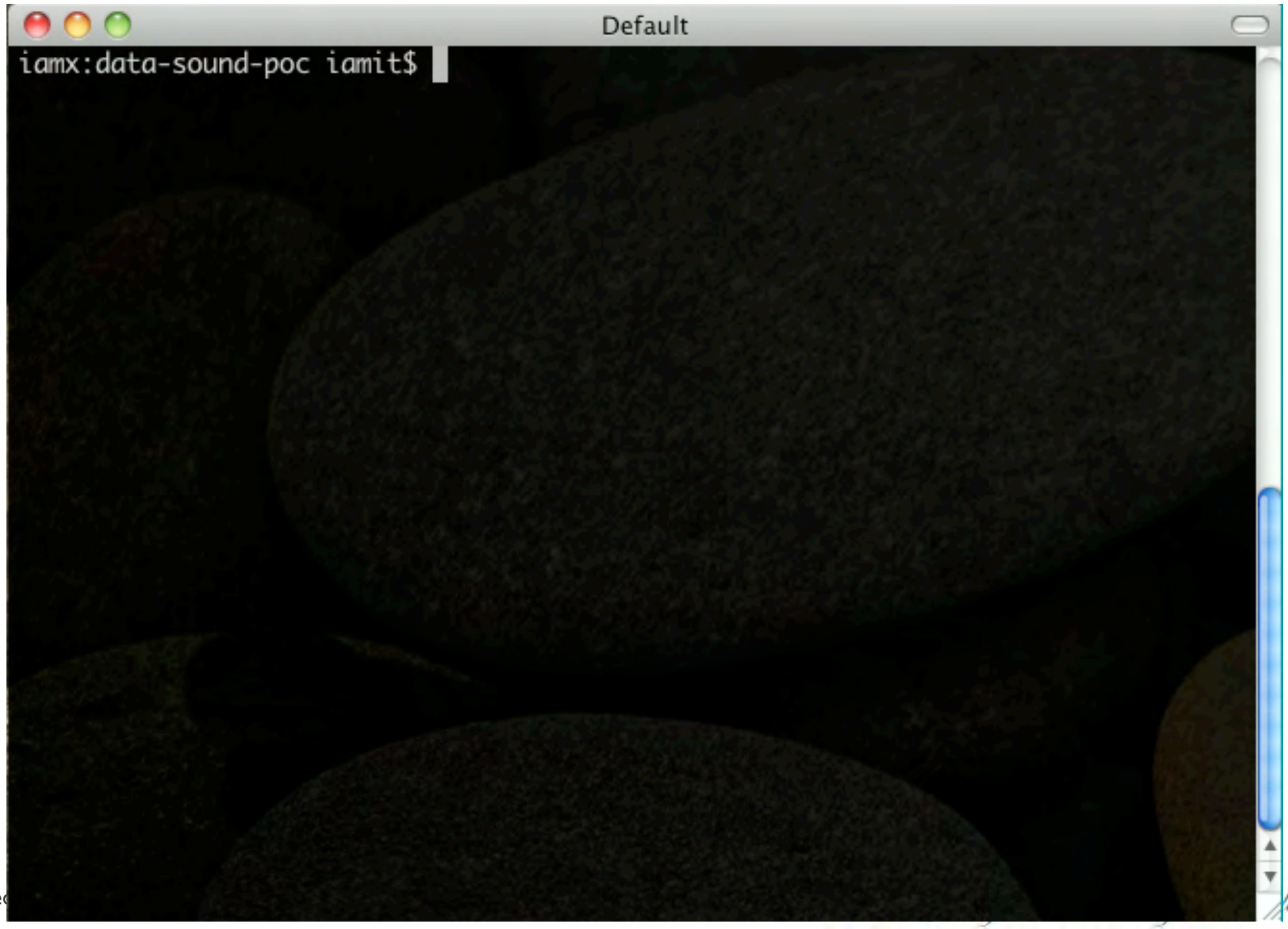
Voice exfiltration demo

Iftach Ian Amit | September 2011

Voice exfiltration demo

Voice exfiltration demo

Voice exfiltration demo



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...

Conclusions

- Available controls
- Information flow path mapping
- Asset mapping and monitoring

Controls

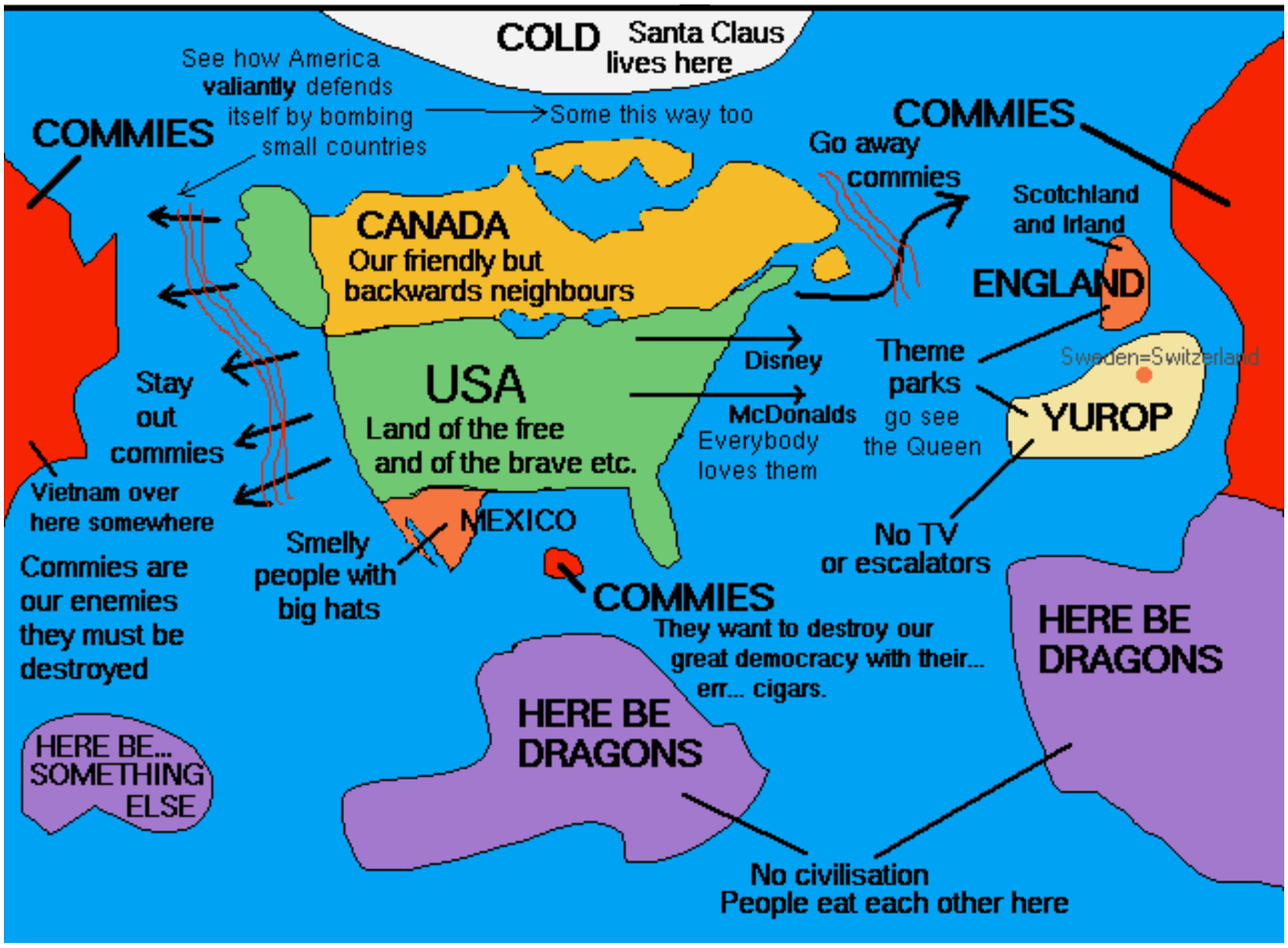
- Start with the human factor
- **Then** add technology

Controls

- Start with the human factor
- **Then** add technology

- Where people leave data
  - **Hint** - spend time with developers.
- "Hack" the **business** process
- Test, test again, and then test. Follow with a surprise test!

Map your assets



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

Old chinese proverb

And monitor them!

They are YOUR assets
after all

No reason to be
shy about it...

And remember to add
honey...

2 tips for monitoring

- Pre-infiltration - social media
  - Check out SocialNet for Maltego from packetninjas.net... :-)

- Post-infoltration - ALL your channels
  - Yes - VoIP is one of them. Record, transcribe, feed to DLP. Simple as that.

Then...

TEST SOME MORE

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

Questions?

Thank **you**!

Whitepapers:
www.security-art.com

Data modulation Exfil POC:
http://code.google.com/p/data-sound-poc/

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

Need your daily chatter?
twitter.com/iiamit