

Iftach Ian Amit | June 2011



Data Exfiltration Not just for Hollywood!

Iftach Ian Amit
VP Consulting

DC9723
CSA-IL Board member
IL-CERT Visionary



whoami

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



Agenda

1. Infiltration
2. Data targeting & acquisition
3. Exfiltration



I. Infiltration

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



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



Infiltration - Technical

The problem:

Small attack surface



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...)

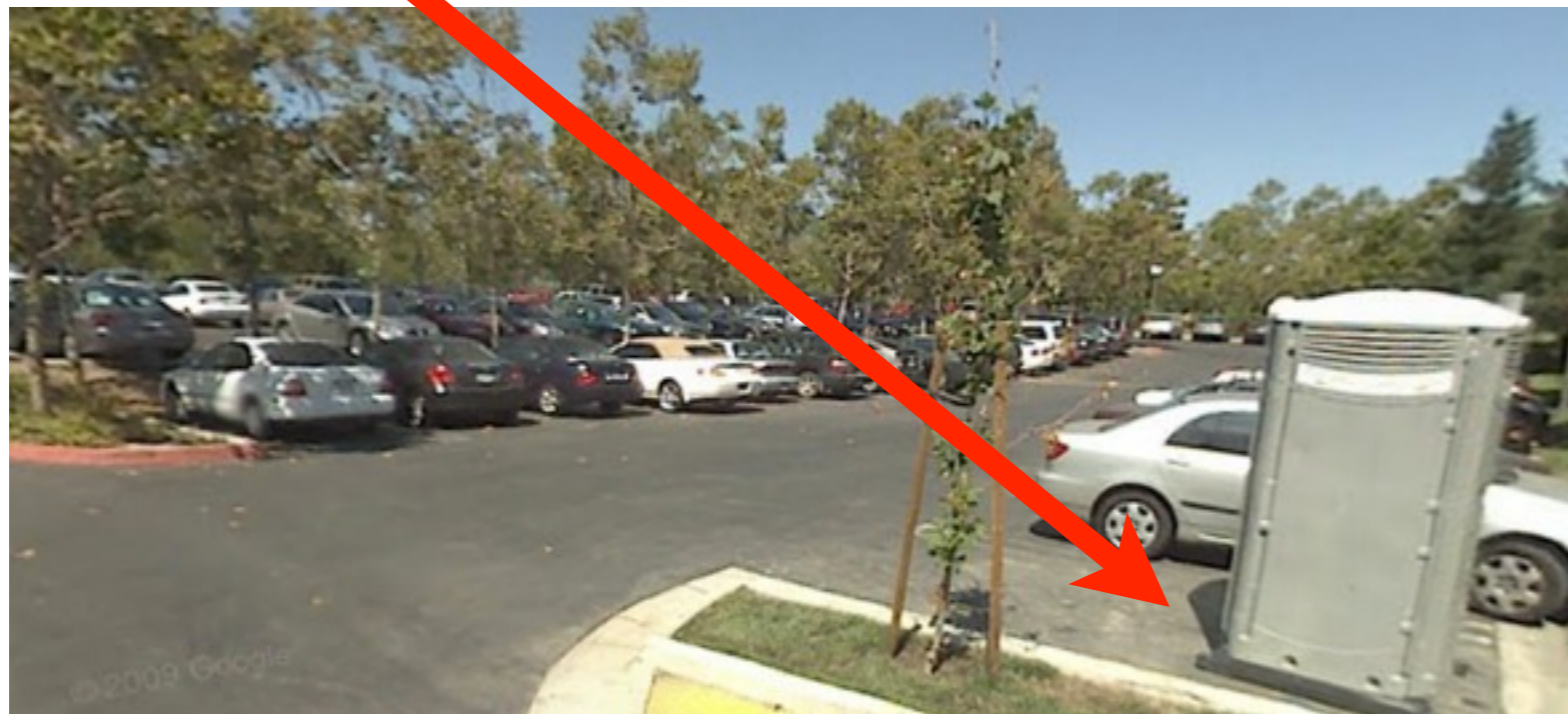


Infiltration - Human

- 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

- 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



Infiltration - Human

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



2. Data Targeting & Acquisition

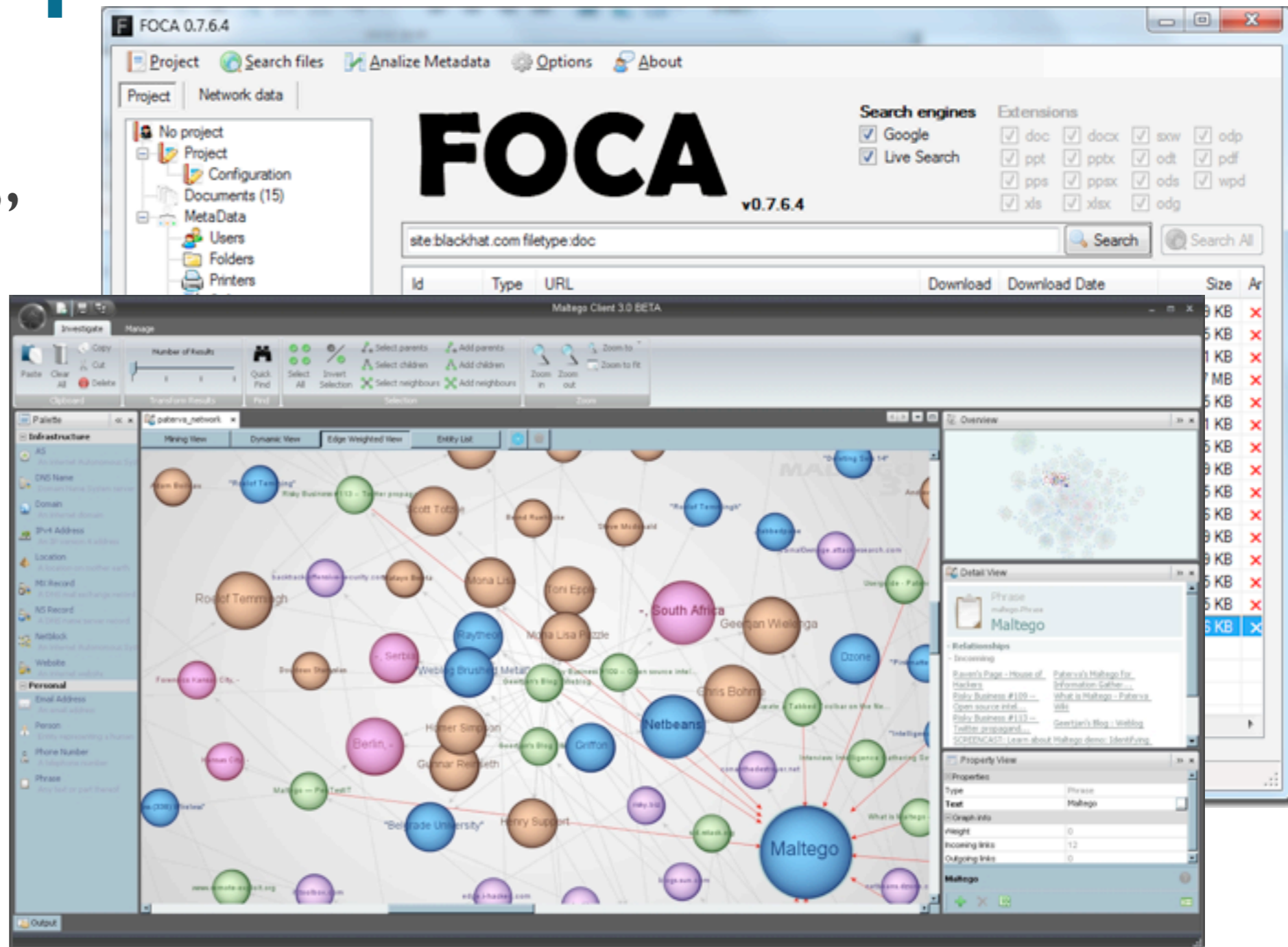
- Weaponizing commercial tools
- Creating “APT” capabilities

- But first - targeting...



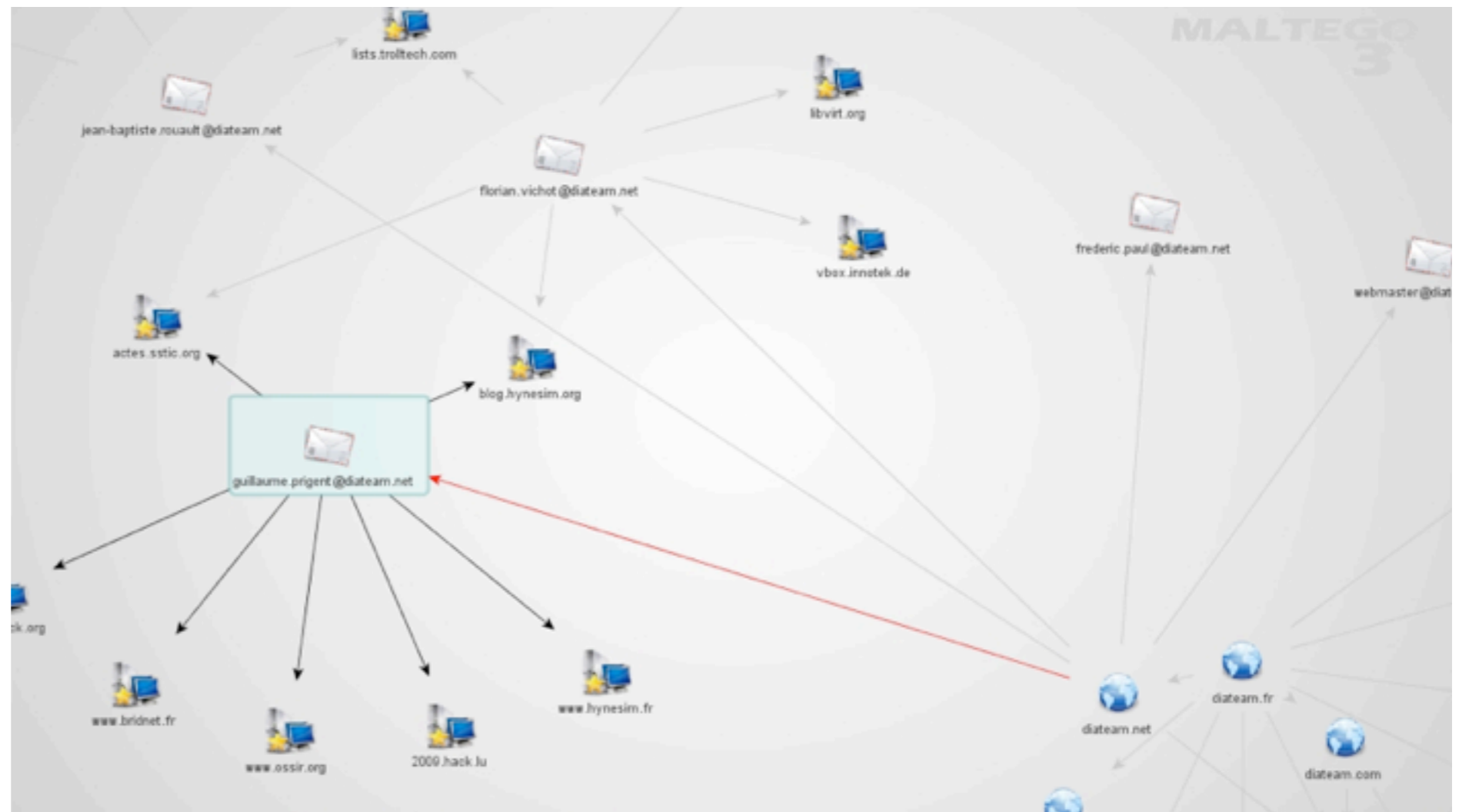
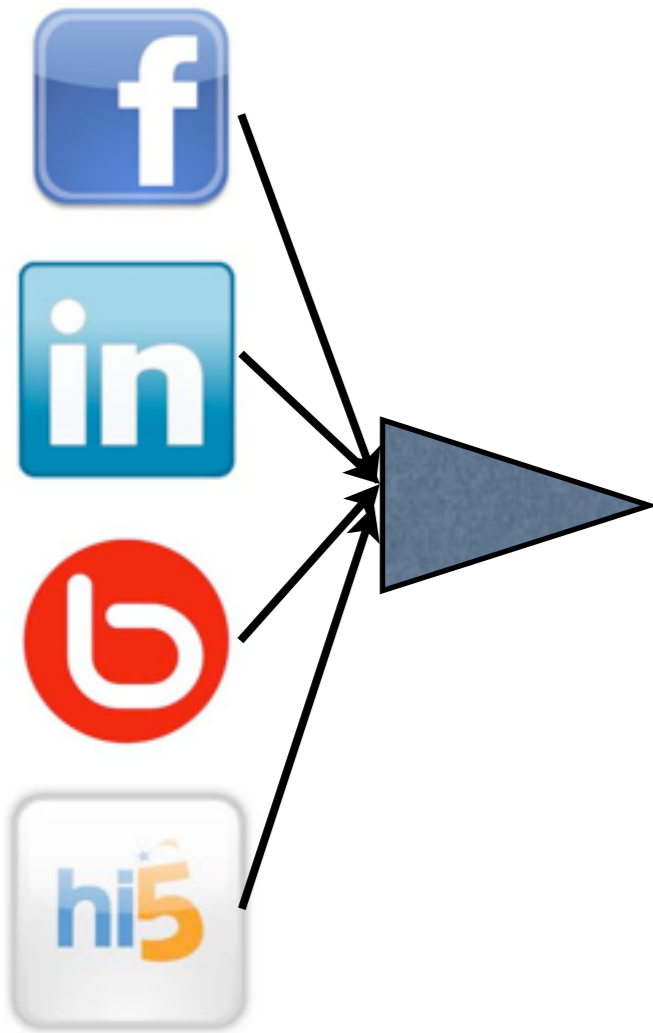
Step 1: Basic Intel

What is the target “willing” to tell about itself?



Who's your daddy?

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



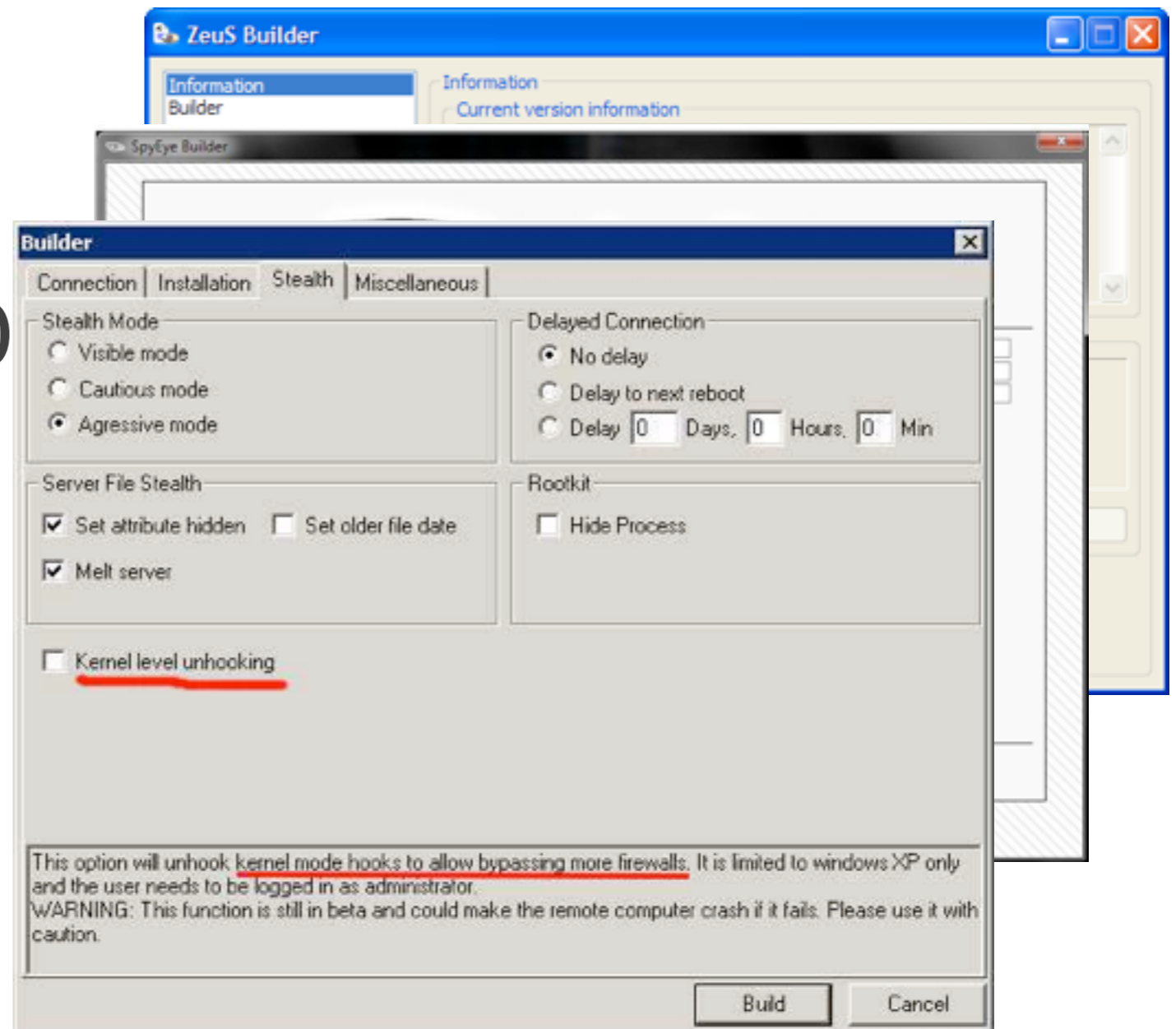
Select your target wisely

And then craft your payload :-)



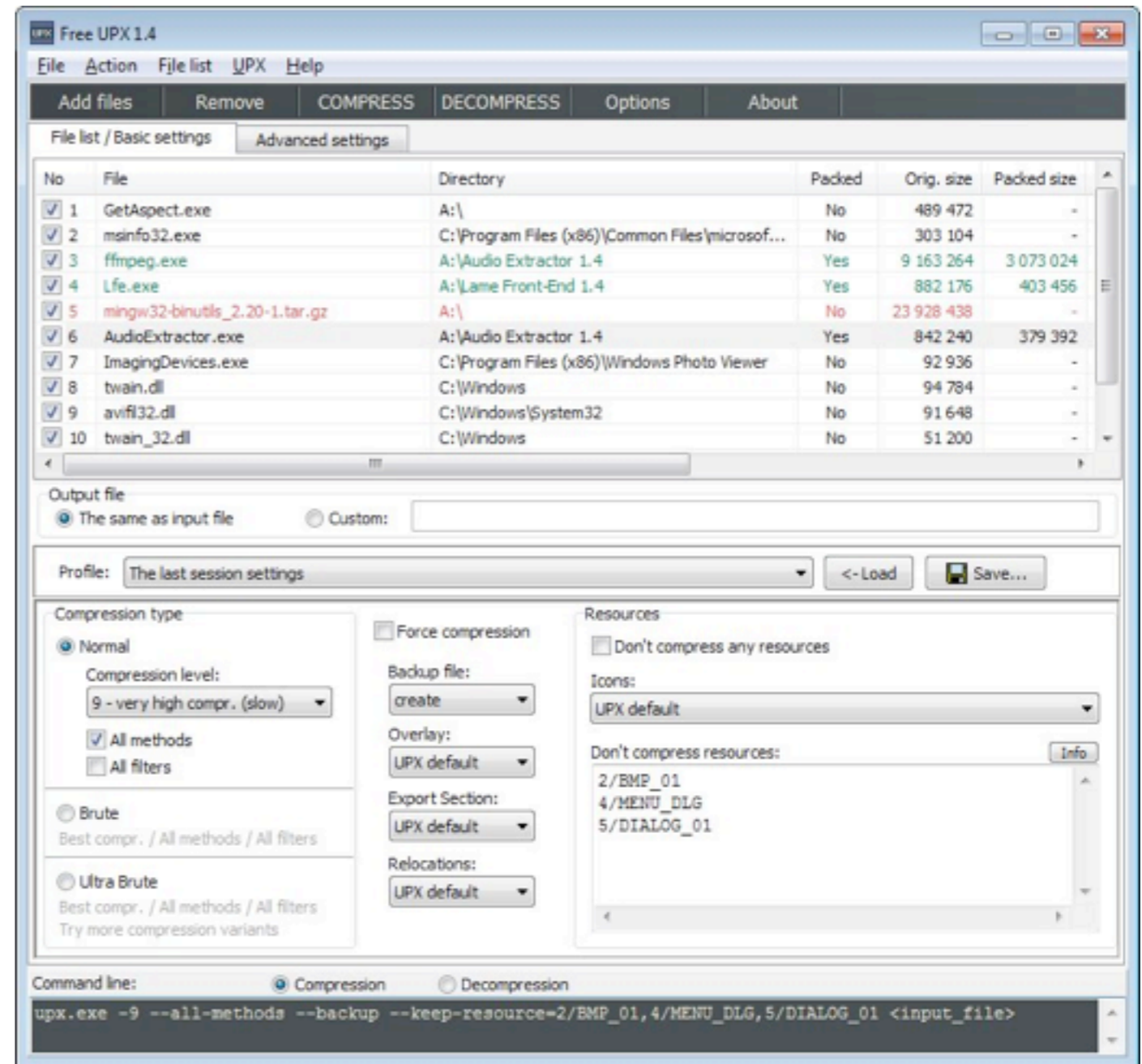
Not as expensive as you think

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



Just make sure to pack

Experienced travelers know the importance of packing properly



And set measurable goals

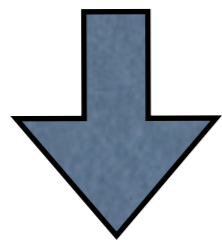
- File servers
- Databases
- File types
- Gateways (routes)
- Printers



From mass infection to APT

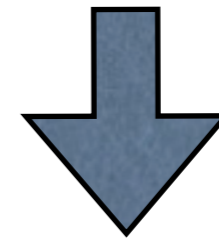
PATIENCE

Mass infection:
5-6 days before
detection



Frequent updates

APT:
5-6 months before
detection



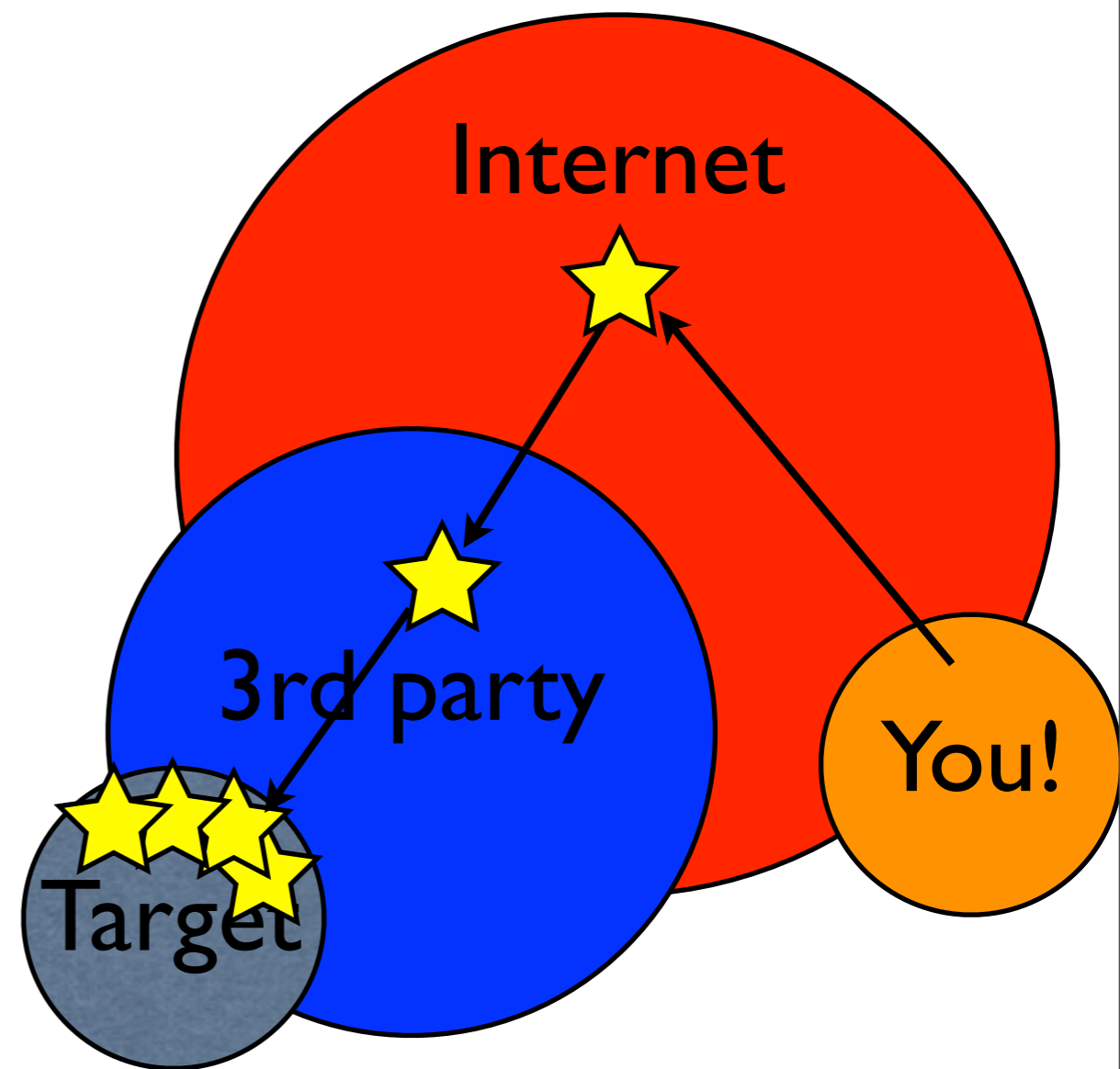
No* updates

*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...



3. Exfiltration

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



Under the radar

- What does the radar look for?

- Text



How about them SSLs?

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



So...

-----BEGIN PGP MESSAGE-----

Version: GnuPG/MacGPG2 v2.0.14 (Darwin)

hQMOA IjQIm6UkL4eEAv/W3r/eYLUmqRNi/Jegt72IK6qdBiBfkg9PZ5YKqI9CUZp
FGnVk029K3gEVcrA4k7w2aOtP7tYKRF8v4yrZQ9GZ7eXzR7+Tbflg+7dveH6U8Bf
BHo8LRovj5OIGghrvpyKYRPIf/NAgzL2G8dyi/FVB0YB4J7/4x0YFEalQHaLiKyt
/gkikyV92njPJ6tPm2sdKUqUHSb20r9AdowZ0VVRrWwdRgUhdNXajjwcbH I BjVuS
Gilw8MnmQkmJAT+TAFkTqC9fjiwtnNMNANJbo2Z36RqsAcKbhVh I eMA7ev0pUakp
Tm4xN64syk/ I DEc0VHFbanAreTV3tCbUUloPQDFGFpiu3oS6/089oUvRtBBbC5p6
leYKEnDIlcGWAomRSiYBFWjTca/Dlw43QIW//lmdBnwcVLUQmDCmwr3HuhEaOmqfO
hdgaxM4GuVdJCDdwXzwpuaPEICd I 8weH2XNzudLdeRKN+wjl/4D6blo+038BcLei
SyhWrMFB7mKSmEzQufQUDACFamtMCn9YOo3mgo+YYk505qhIDLNwZXqyVUqOHvIG
vu7gzuNwUdY5idLqsGEs0K0xVwYntTKUh6 I tNS/HDfNTVm4Y3p8M88JHhcg7npY5
gJuhWuHkGP2CTsQT+gRjthm3I3AlnlvAfuC5uVLMsjA4sCw2FRDOARxrN9EI8maX
/vCxN9aB3dK4S9MSGJ5HhaYpTfpc9CdFkFryzb2sFWfW85nSzNo7dVFCy0jmSr I 9
o4Jsfj0J0izS3MeGYYz5NSsfBz+6o/IYURL3OXrm4DujNHY0DvVbYqSQRRx3o2S+
uZekwXwYsqpei/f/sYo875p5NeX3g62zgJy2Vly+n58WaZWohb5Y0QCxNfpjdcAQ
3tuZQaUvlqrkQeSRxKXD7pxlHdwHDgfvw0 I RU8NsMkfsBoTZY27BjFvlG5S/pv9O
6lznXaju9jRWDj6tvSypx8X2iiVgtSHYahlqEUH I RusAMCILkx0DydCvUud/qRbT
YcnkVVgA8ojeDoVpp3AabRrSmgEAOwV6M0KvnSuMKniLIKe7kolqGjEuLAX7s5Kg
mMHfNki5dYWvQzHv03ID9UG+uW6o54BnsajEVe2EcYTPT+8pg2bCxnMEIK0ds9Is
qvf2Kx4kqO0qMeJG I II2zfAFqmMiTMtgA2CZ0Y42hA/bQK/CCM8QVo9JcGn3Jf6N
0X I TVob7xD0/fkRROHv74dlh2Kxa0SH8iGdb4kl=
=jN3t

-----END PGP MESSAGE-----



Still “too detectable”

hQMOA IjQIm6UkL4eEAv/W3r/eYLUmqRNi/Jegt72IK6qdBiBfkg9PZ5YKql9CUZp
FGnVk029K3gEVcrA4k7w2aOtP7tYKRF8v4yrZQ9GZ7eXzR7+TbfI g+7dveH6U8Bf
BHo8LRovj5OIGghrvpyKYRPIf/NAgzL2G8dyi/FVB0YB4J7/4x0YFEalQHaLiKyt
/gkikyV92njPJ6tPm2sdKUqUHSb20r9AdowZ0VVRrWwdRgUhdNXajjwcbH I BjVuS
Gilw8MnmQkmJAT+TAFkTqC9fjiwtnNMNANJbo2Z36RqsAcKbhVh I eMA7ev0pUakp
Tm4xN64syk/ I DEc0VHFbanAreTV3tCbUUloPQDFGFpiu3oS6/089oUvRtBBbC5p6
leYKEnDIlcGWAomRSiYBFWjTca/Dlw43QIW//ImdBnwcWLuQmDCmwr3HuhEaOmqfO
hdgaxM4GuVdJCDdwXzwpuaPElCd I 8weH2XNzudLdeRKN+wjl/4D6blo+038BcLei
SyhWrMFB7mKSmEzQufQUDACFamtMCn9YOo3mgo+YYk505qhIDLNwZXqyVUqOHvIG
vu7gzunwUdY5idLqsGEs0K0xVwYntTKUh6 I tNS/HDfNTVm4Y3p8M88JHhcg7npY5
gjuhWuHkGP2CTsQT+gRjthm3I3AlnlvAfuC5uWLMsjA4sCw2FRDOARxrN9EI8maX
/vCxN9aB3dK4S9MSGJ5HhaYpTfpc9CdFkFryzb2sFWfW85nSzNo7dVFCy0jmSr I 9
o4Jsfj0J0izS3MeGYYz5NSsfBz+6o/IYURL3OXrm4DujNHY0DvVbYqSQRrx3o2S+
uZekwXwYsqpei/f/sYo875p5NeX3g62zgJy2Vly+n58WaZWohb5Y0QCxNfpjdcAQ
3tuZQaUvlqrkQeSRxKXD7pxlHdwHDgfvw0 I RU8NsMkfsBoTZY27BjFvlG5S/pv9O
6lznXaju9jRWDj6tvSypx8X2iiVgtSHYahlqEUH I RusAMCILkx0DydCvUud/qRbT
YcnkVVgA8ojeDoVpp3AabRrSmgEAOWV6M0KvnSuMKniLIKe7kolqGjEuLax7s5Kg
mMHfNki5dYWvQzHv03ID9UG+uW6o54BnsajEVe2EcYTPT+8pg2bCxnMEIK0ds9Is
qv2Kx4kqO0qMejG I I2zfAFqmMiTMtgA2CZ0Y42hA/bQK/CCM8QVo9JcGn3Jf6N
0X I TVob7xDo/fkRROHv74dlh2Kxa0SH8iGdb4kl=
=jN3t

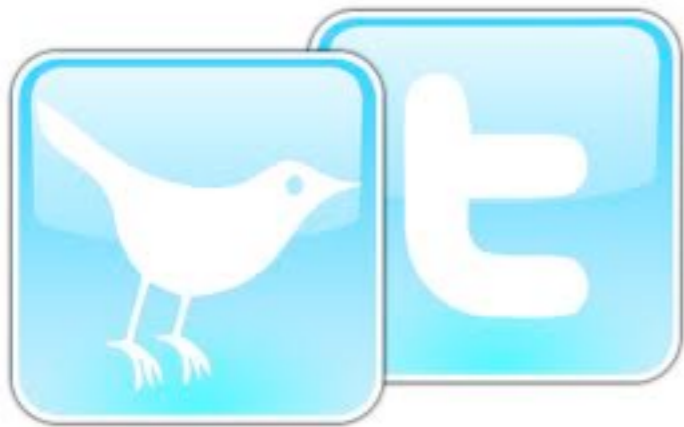


Much better

- 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!

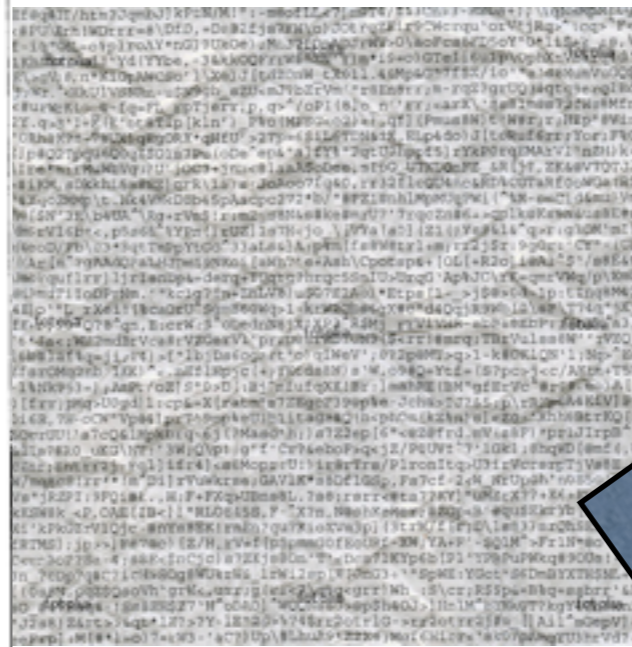


Kill some trees

```
Ef@g#1T/htm?JqmbJ)kPtN/M!":-m%ofLLx7]mST4/T13Cn>3-H200+;;\iqNHMPm;0y4
<#PU\Xrh!WDrrr=8\DfD,=Ds82fjs7XW\o)JOtrqZEr9CWerqu'orV'jRq>^lcq>^F<j
f-ig"OAL-otplroAY*nG]?UkOe);MaJ7fOnADJRwV>O\aoFcs8FD5oY"O*li$;k;s,%p
1KhffotoliaJ'Yd(YYbe,-3&kkoQFrrW#m2N'Y)m*i9=0)GTeli6ulp\OphXnVha;gd'p
E\>gV;8;n*KIGpAWCSO'l\Xo)J[tdZOnW tX01l.4sMp&G*7f$X/io'"e's8MumVuQ$W
fj>Wr.'<HkUlVSNRn-uSN9gb_sZU<mJ7bZrVm'"r8En8rr;m-rqZ?grUQ34gtg9erq1EdP
<#urWrKlo_@-fq=FL_xpTjerr;p,q>^/oPI(8]o n'rr;<arX\'#s8lms72fws8Mfn5
2Y.q>s'I=K(K'ot8TIp[kln') Pvo(MFSG<o2)<j,qf](Pmus8W)t'W#r;r;Hzp^8Ving
"ORh8K?n+78UX)gBgORX*ghFU">2Tp=6SiL6TDN&iK,ELp4do)J[toRuf6rr;Yor;F%Gq
Z]p#Q2Tppqu6QoqZ$O1s7Pu(oDe^ep&"a]fy%"PqtU0hppf5)rYkP0rqEMArVl'nZH)k=c
lIre*mrMuWbVqu?U'jOC3+jnn<8laaA$0Dee;#IpO_UTKUQnFZ_&R[j?,ZK&@VTOTJlx
=#iKM,sDkKhL5s8NZ)qrR\1s)s:JoAoo7fq&0,rr32flcQU4nc&RD%CGTArf0oWG0(R1]
'4XgoZMmp\t.Hk4VM<D0b45pAacpc272*b/"#PZ1snhlMpMUqPWi(^%M-smCld&mu)Vmc
2N6[SN'3E\b4UA^Rq+rVm$!r:m2gs8N&s#ke#mrU?'7rqcZn#6+>qplk@Ks9N&us8E#ss
/dsRv16b+<,p5s68^%YPn(jrUZ]ls7H<jo_\jVYa(s0](Z1(jYs8&15^q>r:g3OM'mI)y
p/4eoD/Fb\c3*3gtTmPpYtGo^33aLs&)A:p^n[fs8W#trl+m;rr2jSr:9gOr:'CY"- (Uhg
7/(Ar[m^?gAAoQPaLHJDM19NKoi[awh'^e+Ash\Cpotsp&+[OL[+R2o]i@Ai^$'/s8E&tr
23eorquflrr)ljrIenDp&-derq+IUqtg?hrqc5S=IU>UrQG'Ap%JC\rK=qmrVWg/p\XmU^
@i3mdTiIoDPrNm.'"kclg?!n+ZhLV8)u$O7E2Ao)*Etps[1->j$@>0d-1p:tInq8M4Qx
4E]o'"L_rXeI!{caOrU^SgmB60Wq>1-krW2Gbs6gX#e"d4QqjR9Wb!0\sf\T74q"jX_x
fk,fotoliaQ?8^qn,B:crW:3^oDednN8jX;XP3^RSMj_rrV1VHR-sbPs8EbP:fotoliaa3/s
'6*Ja<;WH2mdBrVca#rVZGerVl'prxdu51WdPUN9($<rr!#mrq;TBrVulss8W'rvZQ_1
16b#laf%q=jj,Y4)>f"1bjDs6ogaft"o]qIWeV';0?2psMT>q>1-k#OKlQN'1;Ng>^Esa
ZfsrOMq2nb'1KK)^<.neflHpjc(+;YKeds8W)s'W,o9#Q=Ytf=(S?pc>j<c/AKta+T5R;
-1%NkP53=);AsPt/oZ]S"0>D[:Bj^nfufqXX!Br:]mahRE(BM"gfErVc^#rP#.eo)A[fa
0[frr;pMq>U0gd]l:cp&=X[ratm"s7ZEgcF39@p%e-Jcha>0J?&5:p\rRpp0A4KiV]P>
0i6R,7H-ocw"Vp84]prT'9mp%eUIh1itags#Q(h<ph0m(kZtn)s]<Z0:"Xhh6BtrKQ[Br
50erUU!'s7cQ&lMpkbrq-6j(?Mas0'h;)s7Z2ep[6"<@Z0frd.mV(s8F)*priJIrpB^..C
&lls7#R0_uKG\NF:'3W;Q\pl'g'f'Cr?&eboF>q<jZ/P0UVf^7'lgkl:8hqWD[emf(,Uf
cZnr;Entrr2j-rq1]ifr4)<s8Mopr:U!)ir8rTrs/PlronItq>U3irVcrsrpTjVs8E,ss
W/mq&cS!rr*!m^Di]rVuWkrse;GAVlK*s8DflGSp,Fs7cf-2<w_NrUp0h'n0S5o'+jhz
Vs*jRZPI:9FQi#k.,H;F+FXq>UBns8L.?s8;rsrr<#ts7?KY]"uMZrX??+K6+Euq<k6)z
kKSW8k<P,OAE[IB<]!"RLO845S,F-^X?n,NeshKeMer;#ZGp<B'#qu$EkrYb[Gf_tF0s
xi'kPkGZrVlQjc-#nYs8EK!rnEn?qu?KioXVm3p)(3trM/f[r;D\ls83)srQhSER:'ac%
fRTMS);jp>>]Fs7@o)[Z/H,rV=f[p$pmG0fEoURf-XW;YA+F'-$Q1M^>Fr1N*o' *6[<
CeurBoP?Sa-4;s8E<$nCjc)s7ZKjs8On'T'<Dcs7lKYp6b[Pl'YPBPuPWkq#90Ue!-]Ec
3n?cDp?q&C7ich>6Og8WU#rW&_lrwi2sp[F]enG3+'*SpWE:YGet^S6DmBYXTH$NL+k=
[(Us8N,ogZSQsoVh'grW<,urr;g(xl<7)gtq<grr)Wh :S\cr;R$Spa=Btq=ssbrr'&hz
so #fP8s#;!Ss8EH$Z7'H^oDAO)^wQnss0>ep$H4OJ>]HnlM^bYHkGT?kgYfotolia2r
"J2s8)Z&rt>>&gt;LZ?>?Y-1E%2d>%74$rr2otrlG->rr2otrr2j#n_[]Ail^mGepV]+T
eeFrp]:M[#*]=o)7=rW3-'aC?)Up\#Lhu29*ZZX8;Mgf6Hicr<'8k07pAmqYU3hrVd?+\
```



To shred or not to shred?



Yeah, good ol'e DD...



Back to hi-tech (?)

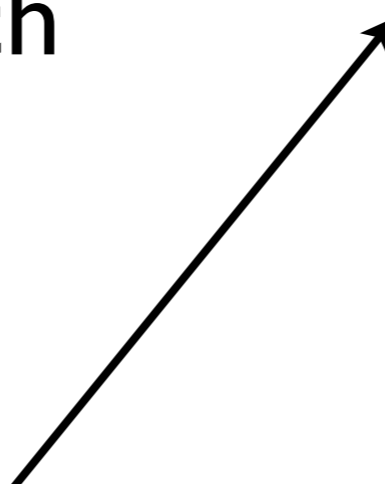
ET Phone Home

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



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



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!



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...



Then...

TEST SOME MORE



Shameless
Plug!

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



Questions?

Thank **you!**

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

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

Need your daily chatter?
twitter.com/iamit

