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
1. 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...)

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...
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)

hQMOAIjQlm6UkJL4eEAv/W3r/eYLUmqRNi/jeg7I6k6qdBiBfk9g9PZ5YKql9CUZp
FNoVko29K3gEVcrA4k7w2aOp79TRKF8v4yrZ9QG7Z7exR7+Tbf1g+7dveH6U8Bf
BHo8LRovj5OIGhrvpyKYRPlf/NNaq3L2G8dyl/FVB0YB4J7/4x0YFEa1QHaLiKyt
/gkikyV92njP]6pm2sdKUqUHSb20r9AdowZ0VVRrWwdRgUhdNXajwcbH1BjVuS
Gilw8MnmQkmjAT+TAFeTqC9fiwtnNMNANjbo2Z36RqsAcKbhVh1eMA7ev0pUakp
Tm4xN64syk/IACe0VHFbanAreTV3tCbgUJloPQDFGFpiu3o56/0890UvRtBbBc5p6
LeYKEnDlcGWAomRSiYBFWJTCa/DIw34Q1W/lmdBnwcWLuQmDCmwr3HuhEaOmqfO
hdgax4GuVdJCdwdxzwpuapEICd18weH2XznudLdeKRN+wjl/4D6bIo+038BcLei
SyhWrMF7bKSmEzQufQUDACFamtMCn9Yo03mgo+YYk505qhDLNwZXqyVUqOHLvIG
vu7gzuNw0dY5IdLqsG65K0xVwYntTKUh61tNS/HDFNTVm4Y3p8M88jHhcq7npY5
GluhlWuHkgp2CTsQT+gRjthm3I3AInLvAfUc5uWLMsjA4sCw2FRDOARxrN9El8maX
/vCnX9aB3dK4S9MSGj5H9shypTfpc9CdFkFryzb2sFWfW85nKzNo7dVFCy0jmSrI 9
o4Jsfj0izS3MeGYYz5NSsfBz+6o/1YURL3OXrmdUjNHY0DvByqSQRXr3o2S+
uZekwXwysasqei/fsYo875p5NeX3g6zgjiy2Vly+n58WazW0Hb5Y0QCXNfpjdcaQ
3tuZQAuvIQrkQeSRxKXD7pxlHdwHDgfvw01RU8NsMkfsBoTZ2BjFvlq5S/pv90
6IznXaj9jRJDj6tvSyphXZi/iVtgS5HYahhUEHIlusAMCILx0Dyd CvUud/qRbT
YcnkVVgA8ojeDoVpp3AabRrSmgEA0wW6M0KvnSuMKniLKe7kolqGjEuLAX7s5Kg
mMHNfNki5dYVWyQzhv031D9UG+uW6o54BnsajEVE2EGCYTPT+8pgzbcXnMeIK0ds9ls
qvfrXx4kqO0qMeJG1I2zfAFqMmTmTgA2CZ0Y42hA/bQK/CM8QVo9JcGn3Jf6N
0X1TVob7xDofkRROHv74dlh2Kxa0SH8ifDgb4kl=
=jiN3t
-----END PGP MESSAGE-----
Still “too detectable”

hQMOAIjQlm6UkL4eEA/3/W3/eYLUmqRNi/Jeg72lK6qdBfkg9PZ5YKqj9CUUZpFGnVko29K3gEVcrA4k7w2aOtP7tyKRF8v4yrZQ9GZ7eXzR7+Tbf1g+7dveH6U8BfBH08LRovj5OGghrvpyKYPRIfl/NAzgL2G8dyi/FVBOYB4j7/4x0YFEalQHaLiKyt/gkiyV92nJ6ctPm2sdKUqUHSb20r9AdowZ0VVRrWwdRgUhdNXajjwcbH1BjVuSGilw8MnmQkmJAT+TAfkTqC9fjiwnMNANjbo2Z36RqsAcKbhVh1eMA7ev0pUakpTm4xN64yk/IJEc0VHFbanAreTVtCblUUioPOQDFGFpiu3oS6/089oUvRtBBbC5p6iEYKEnDIlcGWAomRSiyBFWJtC/Alw43QlW/ImdBnwcWLuQmDCmwr3HuhEaOmqfOhdgaxM4GuVdjCDdwXzwpuPEICd18eH2XNzdLdRKN+wjI/4D6blo+038BcLeiSyhWrMFB7mKSmEzQUDACFatmMCn9Yo3mgo+YYk5o5qhldLNNwZXqyVUqOHvIGu7gzuNwUdY5idLqsGEs0KoxWvYntTKU61tNS/HDFNTVm4Y3p8M888JHhcg7npY5glJuHuHkgp2CTsQT+gRjthm3I3AlnvAfuC5uWLMsjA4sCw2FRDOARxN9E18mAxCvCN9aB3dK4S9MSGJ5HhaYtYfpc9CdFkFryzb2sFWfW85nSzNo7dVFCy0jmSr19o4jsf0j0izS3MeGYYz5NSsfBz+6o/YURL3OXrmd4UjNHY0DvBvYqSQRRx3o2SUZeKxwXwYsqpei/f/sYo875p5NeX3g62zgjy2Vly+n58WaZWoHb5Y0QCxNfjdcAQ3tuZQaUvqlrQeSrxKXD7pxHdWHDgfwv01RU88NsMkfsBoTZY27BjFvlg5S/pv90O6lznXalj9jRWDJ6tvSypx8X2iiVgtSHYahlqEUH1RusAMCIKsx0DydCvUud/qRbTYcnkVvG80jeDoVpp3AaabRrSmgEAOwW6M0KvsnuMKnlKk7kolqGjEuLAXs7s5KgMMHfNkii5dYWvQzHv03I9UG+uW6o54BnsajEVe2EcYTPT+8pg2bCxnMElK0ds9Isqvf2xK4qkQ0qMejG1I2zAFqmMiTTmgA2CZ042h/A/bQK/CCM8QVo9jGn3Jf6N0X1TVob7xDofkRROHv74dlh2Kxa0SH8iGdb4kl=\jnN3t

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
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?
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

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

Shameless Plug!
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/iiamit