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

All rights reserved to Security Art Itd. 2002-2011

Tuesday, September 20, 11

whoami

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



All rights reserved to Security Art ltd. 2002-2011

Ш

ŬĀŬ

Agenda



All rights reserved to Security Art Itd. 2002-2011



All rights reserved to Security Art Itd. 2002-2011



I. Infiltration

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

Infiltration - Technical

All rights reserved to Security Art Itd. 2002-2011

Tuesday, September 20, 11

Infiltration - Technical

• Exploits! of what???

All rights reserved to Security Art ltd. 2002-2011

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

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

- Exploits! of what???
 - Web, FTP, mail, SSL-VPN...
 - Will only get you the basic stuff
 - 3rd party tools used (LinkedIn, SalesForce, SaaS applications)...

- 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

All rights reserved to Security Art ltd. 2002-2011

6

Infiltration - Technical

All rights reserved to Security Art ltd. 2002-2011

Tuesday, September 20, 11

• How about them windows?

All rights reserved to Security Art Itd. 2002-2011

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

- 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

- 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

- 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

All rights reserved to Security Art ltd. 2002-2011

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

All rights reserved to Security Art Itd. 2002-2011

- 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!"

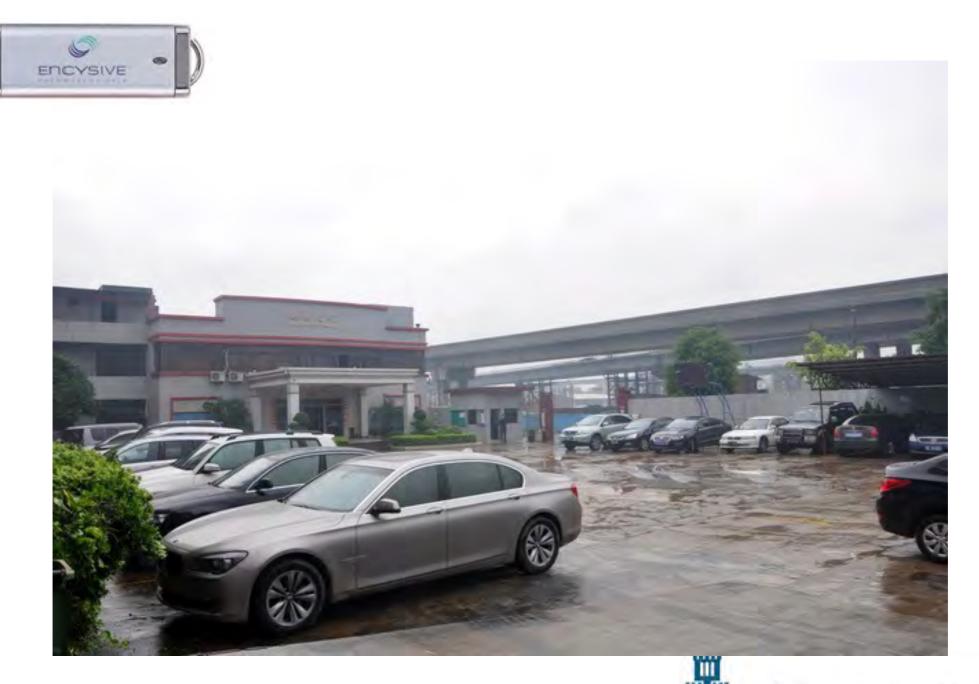
- Not as in "I got your guy and I want \$1,000,000 to set him free"
- More like "dude, check out the pics from the conference we went to last month. Wicked!"
 - "did you get my memo with the new price-list <link to .xls file>"

All rights reserved to Security Art ltd. 2002-2011

- 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...

All rights reserved to Security Art Itd. 2002-2011

Infiltration - Human

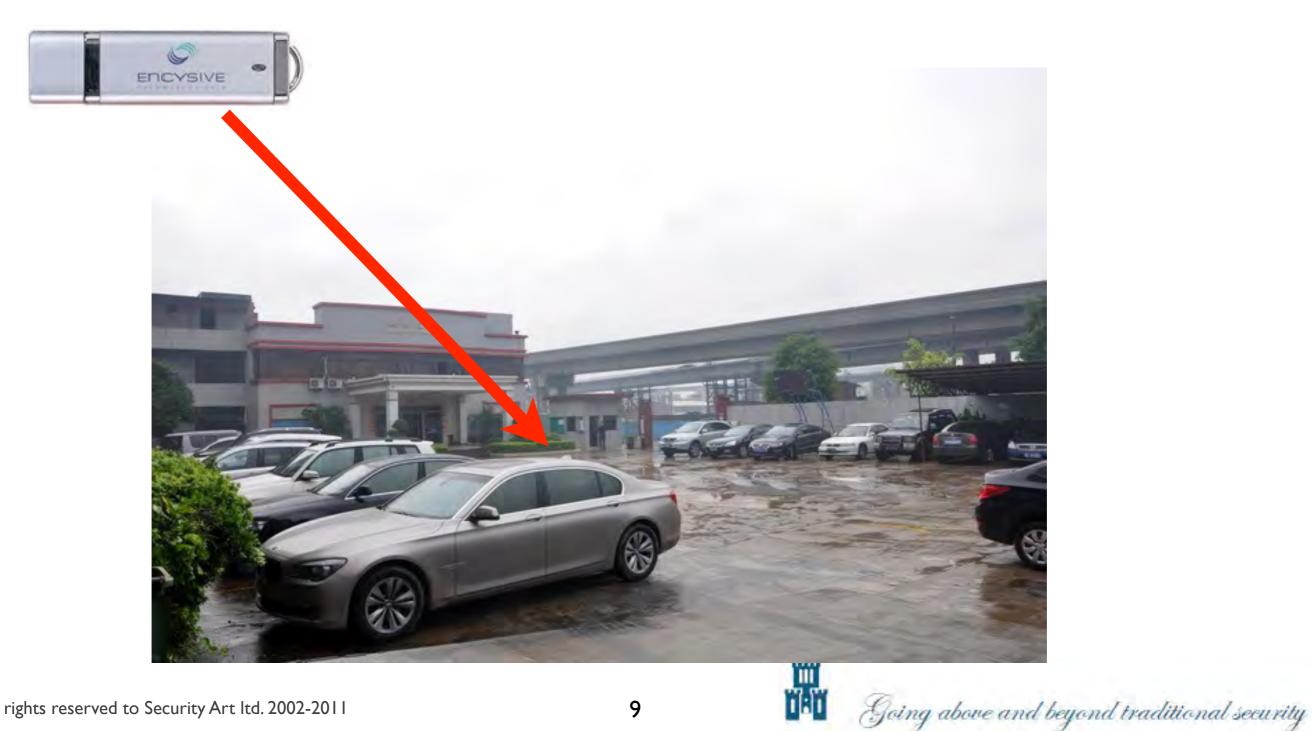


All rights reserved to Security Art ltd. 2002-2011

9

Infiltration - Human

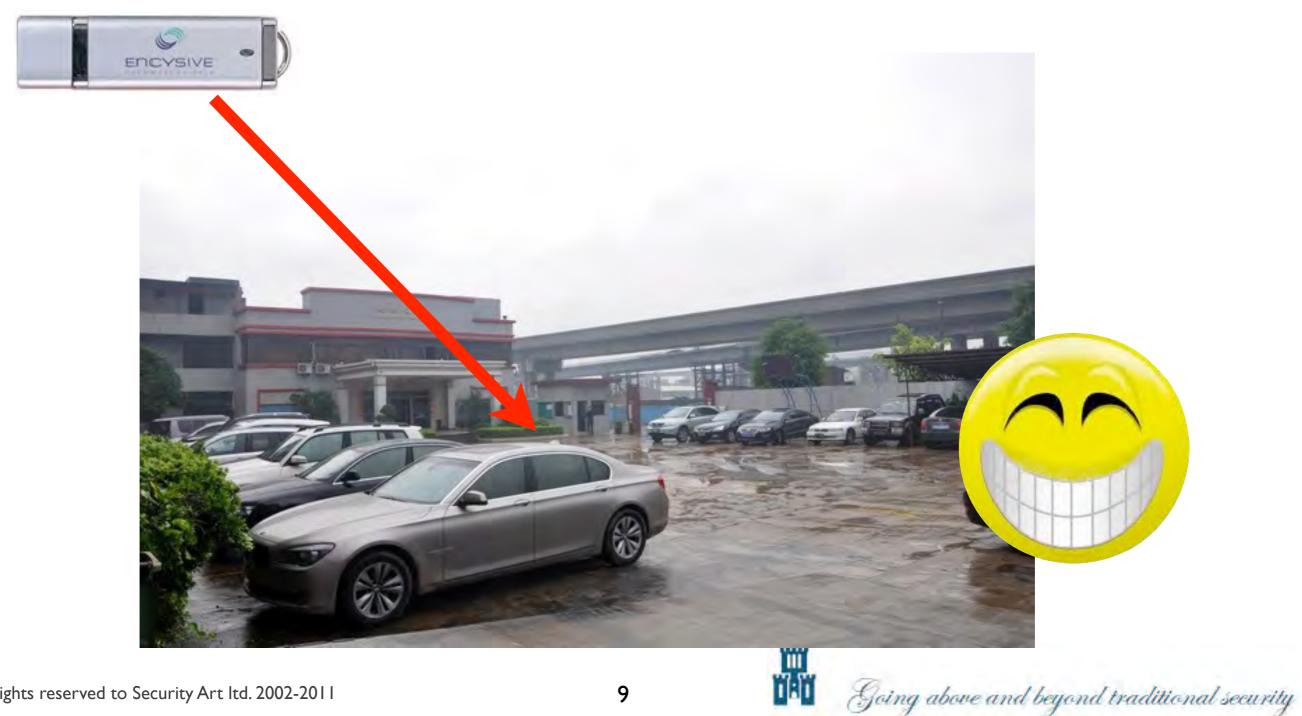
9



All rights reserved to Security Art Itd. 2002-2011

Tuesday, September 20, 11

Infiltration - Human



All rights reserved to Security Art Itd. 2002-2011

Infiltration - Human

All rights reserved to Security Art ltd. 2002-2011

Infiltration - Human

• eMails, web links, phishing...

Tuesday, September 20, 11

Infiltration - Human

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

All rights reserved to Security Art Itd. 2002-2011

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

All rights reserved to Security Art ltd. 2002-2011

Infiltration - Human

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

Select from the menu:

- Spear-Phishing Attack Vectors
- Website Attack Vectors
- Infectious Media Generator
- Create a Payload and Listener
- 5. Mass Mailer Attack
- Teensy USB HID Attack Vector
- SMS Spoofing Attack Vector
- 8. Wireless Access Point Attack Vector
- 9. Third Party Modules
- 10. Update the Metasploit Framework
- 11. Update the Social-Engineer Toolkit
- 12. Help, Credits, and About
- 13. Exit the Social-Engineer Toolkit

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

All rights reserved to Security Art Itd. 2002-2011

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



All rights reserved to Security Art Itd. 2002-2011

Tuesday, September 20, 11

Infiltration - Human

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



All rights reserved to Security Art ltd. 2002-2011

Tuesday, September 20, 11

11

Infiltration - Human

11

Going above and beyond traditional security

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



All rights reserved to Security Art Itd. 2002-2011

Tuesday, September 20, 11

Infiltration - Human

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





Going above and beyond traditional security

2. Data Targeting & Acquisition

- Weaponizing commercial tools
- Creating "APT" capabilities

All rights reserved to Security Art Itd. 2002-2011

Step I: Basic Intel

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

ste blackhat.com filetype:doc Id Type URL Download Download Download Date Size Ar IV 0 doc http://www.blackhat.com/presentations/bh-asia-01/ltch • 4/23/2009 3.29:35 39 KB × IV 1 doc http://www.blackhat.com/presentations/bh-asia-01/ltc.steaton • 4/23/2009 3.29:35 31 KB × IV 2 doc http://www.blackhat.com/presentations/bh-asia-01/ltc.steaton • 4/23/2009 3.29:35 31 KB × IV 3 doc http://www.blackhat.com/presentations/bh-asia-04/bhj • 4/23/2009 3.29:35 327 MB × IV 4 doc http://www.blackhat.com/presentations/bh-usa-02/bh • 4/23/2009 3.29:35 31 KB × IV 6 doc http://www.blackhat.com/presentations/bh-usa-02/bh • 4/23/2009 3.29:47 30 5 KB × IV 6 doc http://www.blackhat.com/presentations/bh-usa-02/bh • 4/23/2009 3.29:47 101 5 KB × IV 7 doc http://www.blackhat.com/presentations/bh-usa-01/bitc • 4/23/2009 3.29:42	Project Network data	F	C	DCA Search ♥ Goog ♥ Live	/e	Extensions Tokac I daca I a Total I cons I a Total I cons I a Total I cons I a I da I da I a I da I da I a	idi 🗹 pdi imi 📝 upi	
W 0 doc http://www.blackhat.com/presentations/bh-asia-01/ltch 4/23/2009 3:29:35 39 KB × V 1 doc http://www.blackhat.com/presentations/bh-asia-01/ltk-sheraton 4/23/2009 3:29:35 91 5 KB × V 2 doc http://www.blackhat.com/presentations/bh-asia-01/ltk-sheraton 4/23/2009 3:29:35 91 5 KB × V 3 doc http://www.blackhat.com/presentations/bh-asia-04/bhj 4/23/2009 3:29:35 31 KB × V 4 doc http://www.blackhat.com/presentations/bh-asia-04/bhj 4/23/2009 3:29:35 31 KB × V 4 doc http://www.blackhat.com/presentations/bh-asia-04/bhj 4/23/2009 3:29:35 31 KB × V 6 doc http://www.blackhat.com/presentations/bh-usa-05/BH 4/23/2009 3:29:37 30.5 KB × V 6 doc http://www.blackhat.com/presentations/bh-usa-02/bh-u 4/23/2009 3:29:41 529 KB × V 8 doc http://www.blackhat.com/presentations/bh-usa-01/bfr	률 Users	ste blackh	at.com fil	etype:doc		Search	Search .	HC.
W 0 doc http://www.blackhat.com/presentations/bh-asia-01/itch 4/23/2009 3/29/35 39 KB x W 1 doc http://www.blackhat.com/presentations/bh-usa-99/Sara 4/23/2009 3/29/35 91.5 KB x W 2 doc http://www.blackhat.com/presentations/bh-usa-01/hk-sheraton 4/23/2009 3/29/35 91.5 KB x W 3 doc http://www.blackhat.com/presentations/bh-asia-01/hk-sheraton 4/23/2009 3/29/35 31 KB x W 4 doc http://www.blackhat.com/presentations/bh-asia-01/hk-sheraton 4/23/2009 3/29/35 51.5 KB x W 5 doc http://www.blackhat.com/presentations/bh-usa-02/bh-u 4/23/2009 3/29/31 30.5 KB x W 6 doc http://www.blackhat.com/presentations/bh-usa-02/bh-u 4/23/2009 3/29/41 529 KB x W 7 doc http://www.blackhat.com/presentations/bh-usa-01/0fr 4/23/2009 3/29/41 529 KB x W 9 doc http://www.blackhat.com/presentations/bh-usa-01/0fr 4/23/2009 3/29/41 529 KB x W 10 doc ttp://www.bl	Printers	Id	Туре	URL	Download	Download Date	Size	Ar
W 1 doc http://www.blackhat.com/presentations/bh-usa-99/Sara 4/23/2009 3/29/35 91.5 KB x W 2 doc http://www.blackhat.com/html/bh-asia-01/hk-sheraton 4/23/2009 3/29/35 31 KB x W 3 doc http://www.blackhat.com/presentations/bh-asia-04/bhj 4/23/2009 3/29/35 31 KB x W 4 doc http://www.blackhat.com/presentations/bh-usa-03/bh 4/23/2009 3/29/35 51.5 KB x W 4 doc http://www.blackhat.com/presentations/bh-usa-05/BH 4/23/2009 3/29/36 51.5 KB x W 5 doc http://www.blackhat.com/presentations/bh-usa-05/BH 4/23/2009 3/29/37 30.5 KB x W 6 doc http://www.blackhat.com/presentations/bh-usa-02/bh-u 4/23/2009 3/29/41 529 KB x W 7 doc http://www.blackhat.com/presentations/bh-usa-01/Ofr 4/23/2009 3/29/42 101.5 KB x W 8 doc http://www.blackhat.com/presentations/bh-usa-01/Ofr 4/23/2009 3/29/43 166 KB x W 10 doc http://www.blackhat.com/present	Software	W O	doc	http://www.blackhat.com/presentations/bh-asia-01/ltch		4/23/2009 3:29:35	39 KB	×
W 3 doc http://www.blackhat.com/presentations/bh-asia-04/bhj. 4/23/2009 3:29:51 3.27 MB x W 4 doc http://www.blackhat.com/presentations/win-usa-03/bh 4/23/2009 3:29:51 51.5 KB x W 5 doc http://www.blackhat.com/presentations/bh-usa-05/BH 4/23/2009 3:29:51 31 KB x W 6 doc http://www.blackhat.com/presentations/bh-usa-05/BH 4/23/2009 3:29:37 30.5 KB x W 6 doc http://www.blackhat.com/presentations/bh-usa-02/bh-u 4/23/2009 3:29:41 529 KB x W 7 doc http://www.blackhat.com/presentations/bh-usa-01/db 4/23/2009 3:29:42 101.5 KB x W 8 doc http://www.blackhat.com/presentations/bh-usa-01/Ofr 4/23/2009 3:29:43 105 KB x W 9 doc http://www.blackhat.com/presentations/bh-asia-03/rsv-form-Bl 4/23/2009 3:29:49 719 KB x W 10 doc http://blackhat.com/presentations/bh-asia-01/ltchfield/li 4/23/2009 3:29:50 39 KB x W 11 doc http://blackhat.com/presentations/bh-usa-02/bh-us-02 4/23/2009 3:29:51 30.5 KB x	Emails		doc	Construction of the second s		4/23/2009 3:29:35	91.5 KB	×
W 4 doc http://www.blackhat.com/presentations/win-usa-03/bh		W 2	doc	http://www.blackhat.com/html/bh-asia-01/hk-sheraton		4/23/2009 3:29:35	31 KB	×
W 5 doc http://www.blackhat.com/presentations/bh-usa-05/BH 4/23/2009 3:29:51 31 KB W 6 doc http://www.blackhat.com/presentations/bh-usa-02/bh-u 4/23/2009 3:29:37 30.5 KB W 7 doc http://www.blackhat.com/presentations/bh-usa-02/bh-u 4/23/2009 3:29:41 529 KB W 8 doc http://www.blackhat.com/presentations/bh-europe-01/d 4/23/2009 3:29:42 101.5 KB W 9 doc http://www.blackhat.com/presentations/bh-usa-01/Ofr 4/23/2009 3:29:43 166 KB W 9 doc http://www.blackhat.com/presentations/bh-usa-01/Ofr 4/23/2009 3:29:43 166 KB W 10 doc http://www.blackhat.com/presentations/bh-usa-01/Ofr 4/23/2009 3:29:49 719 KB W 11 doc http://blackhat.com/presentations/bh-asia-01/it.chfield/i 4/23/2009 3:29:50 39 KB W 12 doc http://blackhat.com/presentations/bh-usa-02/bh-us-02 4/23/2009 3:29:51 30.5 KB W 13 doc http://blackhat.com/presentation		W 3	doc	http://www.blackhat.com/presentations/bh-asia-04/bh-j		4/23/2009 3:29:51	3.27 MB	×
W 6 doc http://www.blackhat.com/presentations/bh-usa-02/bh-u. 4/23/2009 3:29:37 30.5 KB W 7 doc http://www.blackhat.com/presentations/bh-europe-01/d. 4/23/2009 3:29:41 529 KB W 8 doc http://www.blackhat.com/presentations/bh-europe-01/d. 4/23/2009 3:29:41 529 KB W 8 doc http://www.blackhat.com/presentations/bh-europe-01/d. 4/23/2009 3:29:42 101.5 KB W 9 doc http://www.blackhat.com/presentations/bh-usa-01/Ofr 4/23/2009 3:29:43 166 KB W 9 doc http://www.blackhat.com/presentations/bh-usa-01/Ofr 4/23/2009 3:29:49 719 KB W 10 doc http://blackhat.com/presentations/bh-asia-01/ltc:hfield/i 4/23/2009 3:29:50 39 KB W 11 doc http://blackhat.com/presentations/bh-usa-02/bh-us-02 4/23/2009 3:29:51 30.5 KB W 12 doc http://blackhat.com/presentations/bh-usa-02/bh-us-02 4/23/2009 3:29:51 30.5 KB W 13 doc http://blackhat.com/presentations/win-usa-03		W 4	doc	http://www.blackhat.com/presentations/win-usa-03/bh		4/23/2009 3:29:36	51.5 KB	×
W 7 doc http://www.blackhat.com/presentations/bh-europe-01/d 4/23/2009 3:29:41 529 KB W 8 doc http://www.blackhat.com/presentations/bh-federal-03/b 4/23/2009 3:29:42 101.5 KB W 9 doc http://www.blackhat.com/presentations/bh-usa-01/Ofr 4/23/2009 3:29:43 166 KB W 9 doc http://www.blackhat.com/presentations/bh-usa-01/Ofr 4/23/2009 3:29:43 166 KB W 10 doc http://www.blackhat.com/presentations/bh-usa-01/Ofr 4/23/2009 3:29:49 719 KB W 10 doc http://blackhat.com/presentations/bh-asia-01/itchfield/i 4/23/2009 3:29:50 39 KB W 12 doc http://blackhat.com/presentations/bh-usa-02/bh-us-02 4/23/2009 3:29:51 30.5 KB W 13 doc http://blackhat.com/presentations/win-usa-03/bh-win-0 4/23/2009 3:29:52 51.5 KB		W 5	doc	http://www.blackhat.com/presentations/bh-usa-05/8H		4/23/2009 3:29:51	31 KB	×
W 8 doc http://www.blackhat.com/presentations/bh-federal-03/b 4/23/2009 3:29:42 101.5 KB W 9 doc http://www.blackhat.com/presentations/bh-usa-01/Ofr 4/23/2009 3:29:43 166 KB W 10 doc http://www.blackhat.com/presentations/bh-usa-01/Ofr 4/23/2009 3:29:43 166 KB W 10 doc http://www.blackhat.com/presentations/bh-usa-03/isv-form-Bl 4/23/2009 3:29:49 719 KB W 10 doc http://blackhat.com/presentations/bh-asia-01/ltchfield/li 4/23/2009 3:29:50 39 KB W 12 doc http://blackhat.com/presentations/bh-usa-02/bh-us-02 4/23/2009 3:29:51 30.5 KB W 13 doc http://blackhat.com/presentations/win-usa-03/ibi-win-0 4/23/2009 3:29:52 51.5 KB		W 6	doc	http://www.blackhat.com/presentations/bh-usa-02/bh-u		4/23/2009 3:29:37	30.5 KB	>
9 doc http://www.blackhat.com/presentations/bh-usa-01/Ofr 4/23/2009 3:29:43 166 KB 10 doc http://www.blackhat.com/images/bh-asia-03/isv-form-Bl 4/23/2009 3:29:49 719 KB 11 doc http://blackhat.com/presentations/bh-asia-01/ltchfield/i 4/23/2009 3:29:50 39 KB 12 doc http://blackhat.com/presentations/bh-usa-02/bh-us-02 4/23/2009 3:29:51 30.5 KB 13 doc http://blackhat.com/presentations/win-usa-03/bh-win-0 4/23/2009 3:29:52 51.5 KB		W 7	doc	http://www.blackhat.com/presentations/bh-europe-01/d		4/23/2009 3:29:41	529 KB	>
W 10 doc http://www.blackhat.com/images/bh-asia-03/isv-form-Bl 4/23/2009 3:29:49 719 KB W 11 doc http://blackhat.com/presentations/bh-asia-01/ltchfield/li 4/23/2009 3:29:50 39 KB 39 KB W 12 doc http://blackhat.com/presentations/bh-usa-02/bh-us-02 4/23/2009 3:29:51 30.5 KB 30.5 KB W 13 doc http://blackhat.com/presentations/win-usa-03/bh-win-0 4/23/2009 3:29:52 51.5 KB		W 8	doc	http://www.blackhat.com/presentations/bh-federal-03/b		4/23/2009 3:29:42	101.5 KB	>
W 11 doc http://blackhat.com/presentations/bh-asia-01/ltch/ield/i 4/23/2009 3:29:50 39 KB W 12 doc http://blackhat.com/presentations/bh-usa-02/bh-us-02 4/23/2009 3:29:51 30.5 KB W 13 doc http://blackhat.com/presentations/win-usa-03/bh-win-0 4/23/2009 3:29:52 51.5 KB		W 9	doc	http://www.blackhat.com/presentations/bh-usa-01/Ofr		4/23/2009 3:29:43	166 KB	>
W12 doc http://blackhat.com/presentations/bh-usa-02/bh-us-02 4/23/2009 3:29:51 30.5 KB W13 doc http://blackhat.com/presentations/win-usa-03/bh-win-0 4/23/2009 3:29:52 51.5 KB		W 10	doc	http://www.blackhat.com/images/bh-asia-03/rsv-form-Bl		4/23/2009 3:29:49	719 KB	>
13 doc http://blackhat.com/presentations/win-usa-03/bh-win-0		the second se	doc	http://blackhat.com/presentations/bh-asia-01/ltchfield/i			39 KB	>
		W 12	doc					>
14 doc http://blackhat.com/presentations/bh-usa-01/OfirArkon/● 4/23/2009 3/29 53 166 KB >		W 13	doc			4/23/2009 3:29:52		>
		W 14	dec	http://blackhat.com/presentations/bh-usa-01/OfrAkin/		4/23/2009 3:29:53	165 KB	>
		the second se	doc doc doc	http://blackhat.com/presentations/bh-asia-01/ltchfield/i, http://blackhat.com/presentations/bh-usa-02/bh-us-02 http://blackhat.com/presentations/win-usa-03/bh-win-0		4/23/2009 3:29:50 4/23/2009 3:29:51 4/23/2009 3:29:52		39 KB 80.5 KB 51.5 KB
		*		117				

Step I: Basic Intel

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



Who's your daddy?

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

All rights reserved to Security Art Itd. 2002-2011

Who's your daddy?

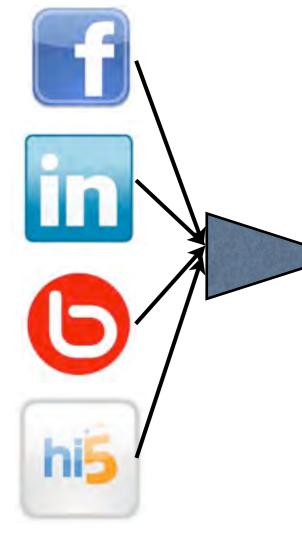
And buddy, and friends, relatives, colleagues...



All rights reserved to Security Art ltd. 2002-2011

Who's your daddy?

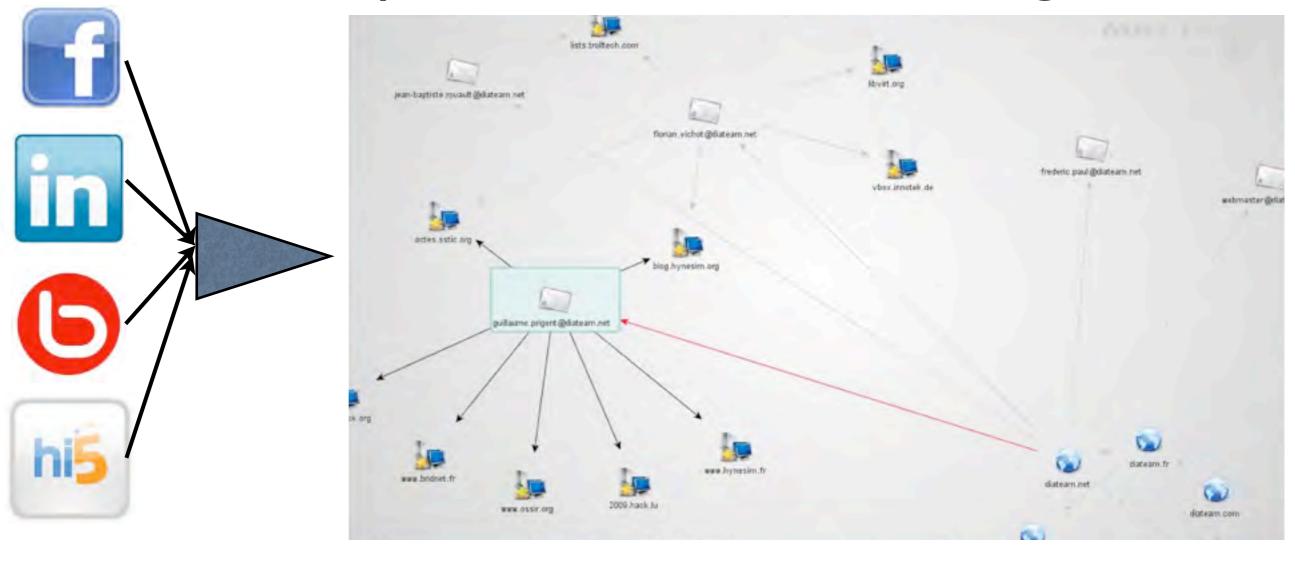
And buddy, and friends, relatives, colleagues...



All rights reserved to Security Art Itd. 2002-2011

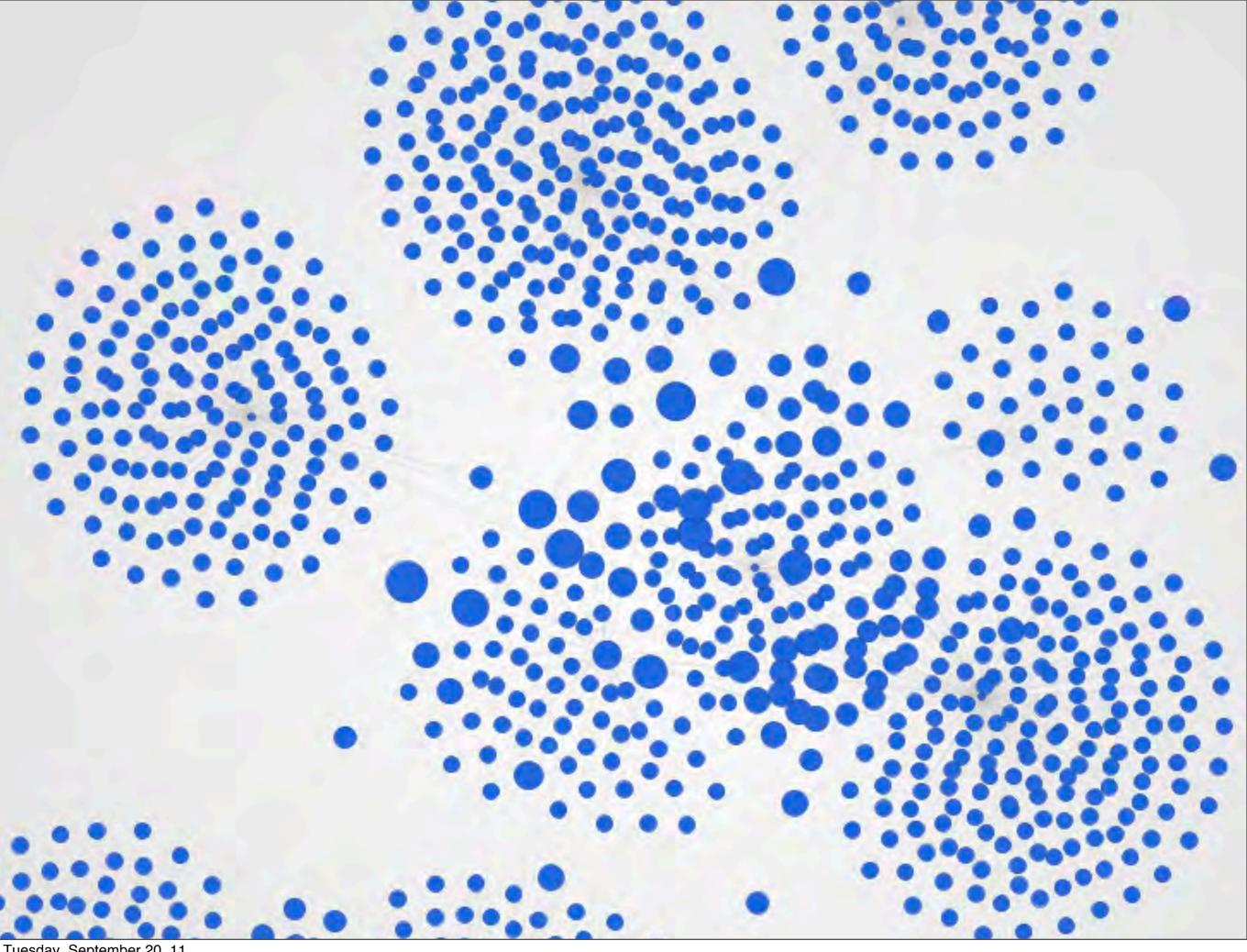
Who's your daddy?

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

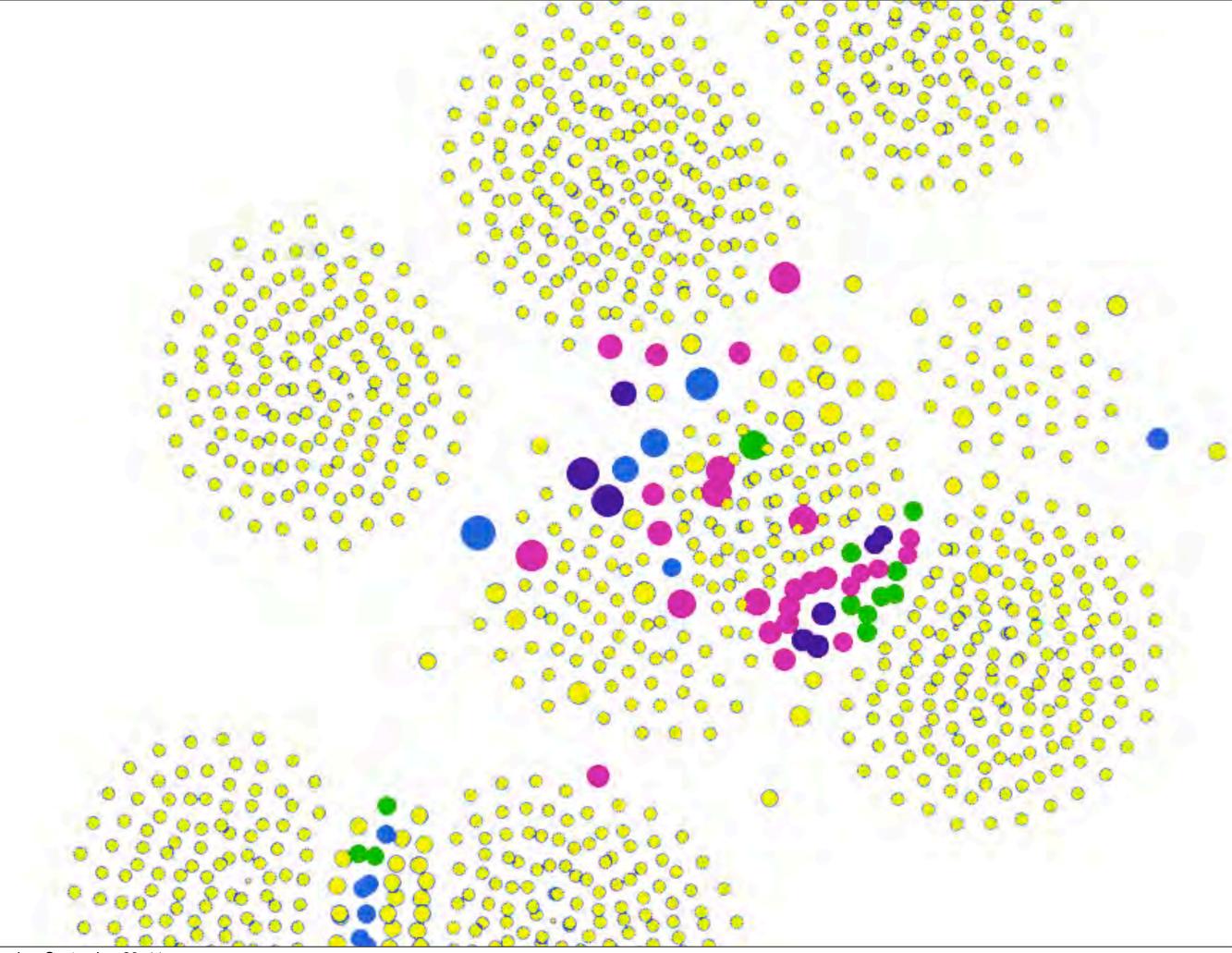


All rights reserved to Security Art Itd. 2002-2011

14



Tuesday, September 20, 11



Select your target wisely

And then craft your payload :-)

All rights reserved to Security Art Itd. 2002-2011

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

Enformation Current version information Version: 1.2.5.1 Build time: 14:51:42 15.06.2009 GMT	
Spyware status on this system Spyware not founded on this system.	
Remove spyware from this system	
	Current version information Version: 1.2.5.1 Build time: 14:51:42 15.05.2009 GMT Spyware status on this system Spyware not founded on this system.

Going above and beyond traditional security

Tuesday, September 20, 11

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

Builder Gyn Builder	Current version information	-
	Spy Eye	
Path to the main control parmi: Atlantative path to the main control parels	http://www.yourbotnet.cn/spyeye/msin/ http://www.yourbotnet2.cn/spyeye/msin/	- 8-
Palh to the formerablar control panels	http://www.yourbotnet.cn/spyeye/formgrabber/	
Encryption key:	Your Enc. Key	
ActionUrl2 : "http://www.pouzh LaboratLadr LaboratLadr LaboratLadr IndexetLadr LaboratLadr IndexetLadr		
	Get build	
	Are you infected by Spytye?	120

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

Se ZeuS Builder		
	mation rent version information	
SpyGye Builder		
uilder		×
Connection Installation Stealth Miscellaneous		
Stealth Mode C Visible mode C Cautious mode Agressive mode	Delayed Connection No delay Delay to next reboot Delay 0 Days, 0 Hours, 0 Min	
Server File Stealth Set attribute hidden Set older file date Mell server	Rootkit	
Kernel level unhooking		
and the user needs to be logged in as administrator.	wpassing more firewalls, It is limited to windows XP only ske the remote computer crash if it fails. Please use it wi	
	Build Cancel	

Going above and beyond traditional security

Tuesday, September 20, 11

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

S. ZeuS Builder		
	ormation Jurrent version information	
🕞 SpyGye Nuilder		-
ílder -	X	
onnection Installation Stealth Miscellaneou	15	
Stealth Mode C Visible mode C Cautious mode Agressive mode	Delayed Connection	
Server File Stealth	Rootkit	
 Set attribute hidden Set older file date Melt server 	T Hide Process	
Kernel level unhocking		
		-
nd the user needs to be logged in as administrato	v bypassing more firewalls. It is limited to windows XP only r make the remote computer crash if it fails. Please use it with	
	Build Cancel	

Going above and beyond traditional security

Tuesday, September 20, 11

Just make sure to pack

Experienced travelers know the importance of packing properly



All rights reserved to Security Art Itd. 2002-2011

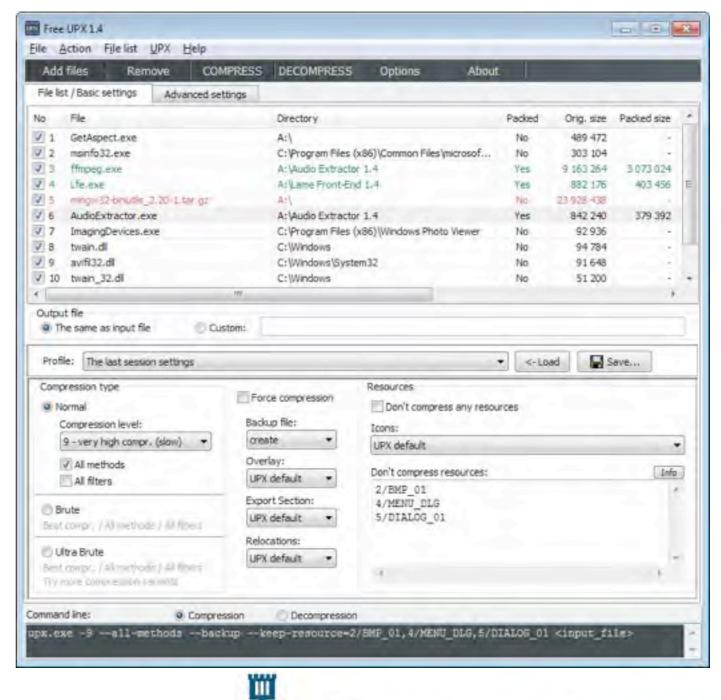
18

Just make sure to pack

Experienced travelers know the importance of packing properly



All rights reserved to Security Art Itd. 2002-2011



18

And set measurable goals

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



From mass infection to APT

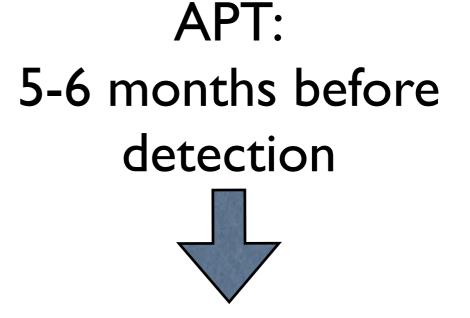
Mass infection: 5-6 days before detection

APT: 5-6 months before detection

Going above and beyond traditional security

From mass infection to APT

Mass infection: 5-6 days before detection



Going above and beyond traditional security

From mass infection to APT



Frequent updates

APT: 5-6 months before detection $\sqrt{}$ No* updates

* Almost

Going above and beyond traditional security

From mass infection to APT

PATIENCE

Mass infection: 5-6 days before detection $\sqrt{}$ Frequent updates

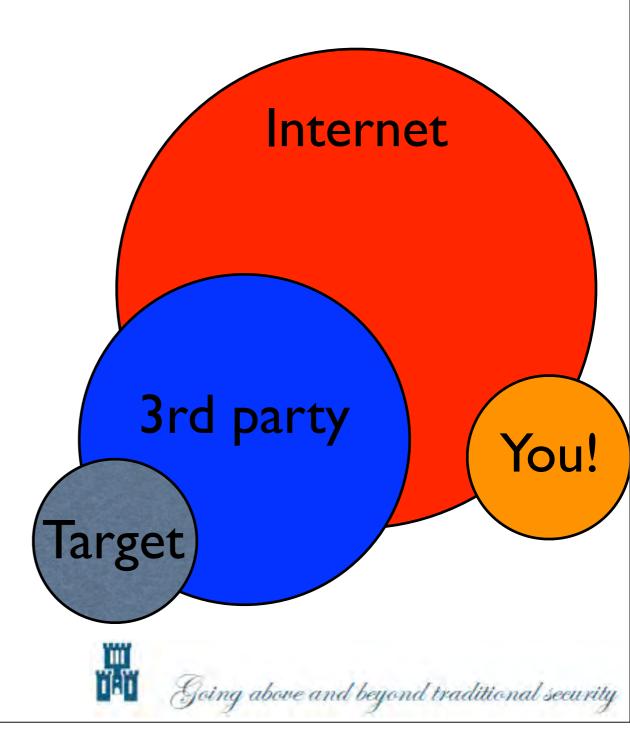
APT: 5-6 months before detection $\sqrt{}$ No* updates *Amos

Going above and beyond traditional security

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...

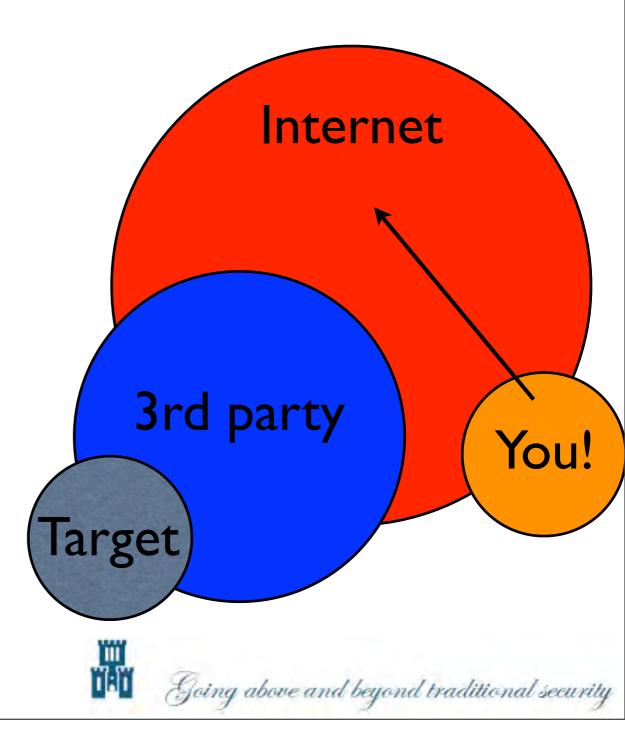


Control?

22

• What happens when you are so far behind?

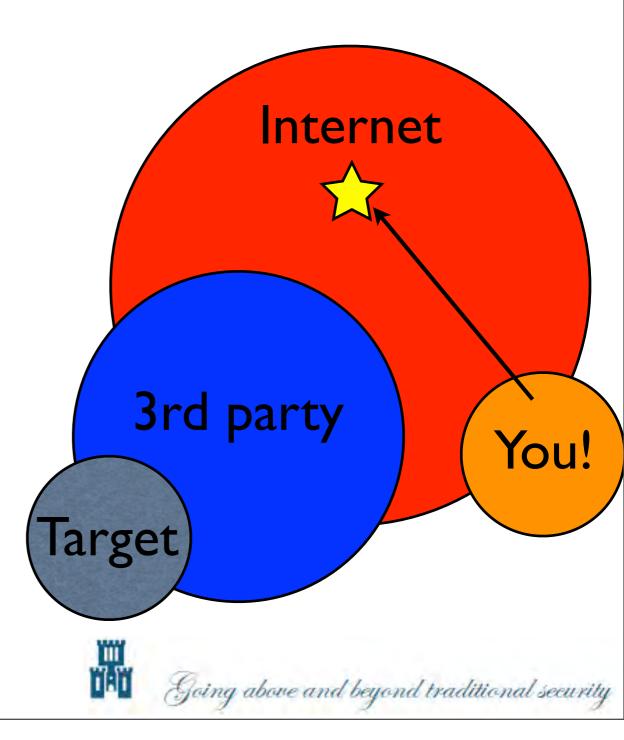
- Just use your friends (peers)
 - Expect a one-way command scheme.
 - Exfiltration is a different animal...



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...

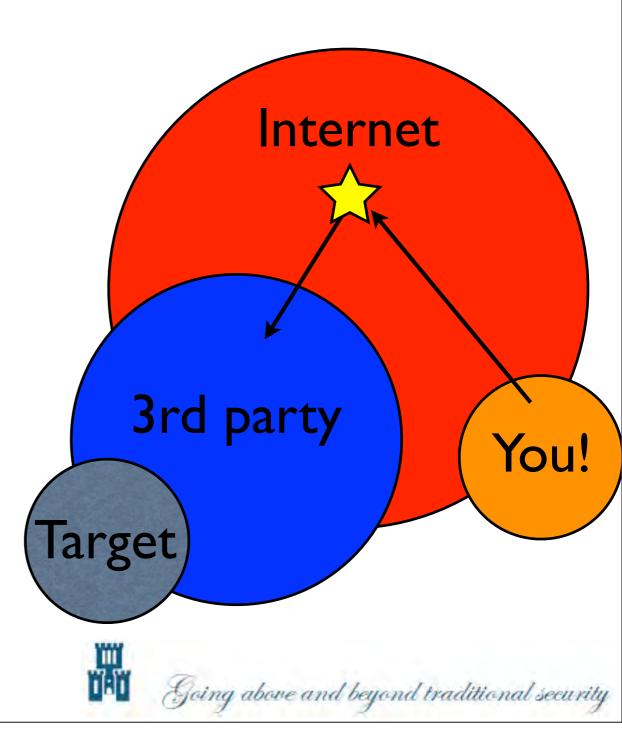


Control?

22

• What happens when you are so far behind?

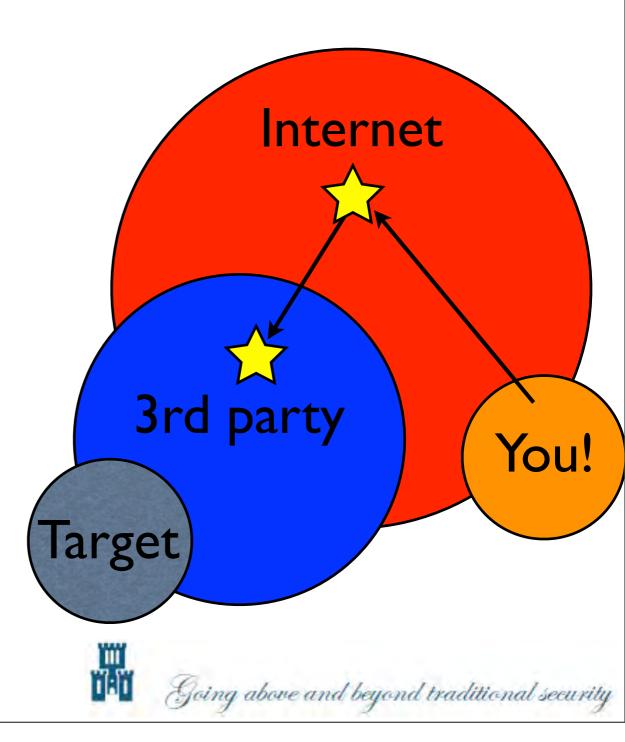
- Just use your friends (peers)
 - Expect a one-way command scheme.
 - Exfiltration is a different animal...



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...

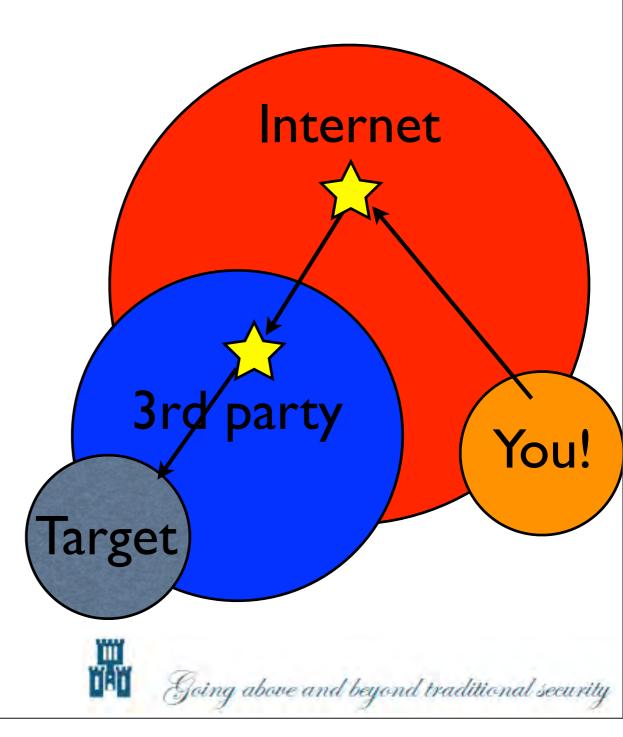


Control?

22

• What happens when you are so far behind?

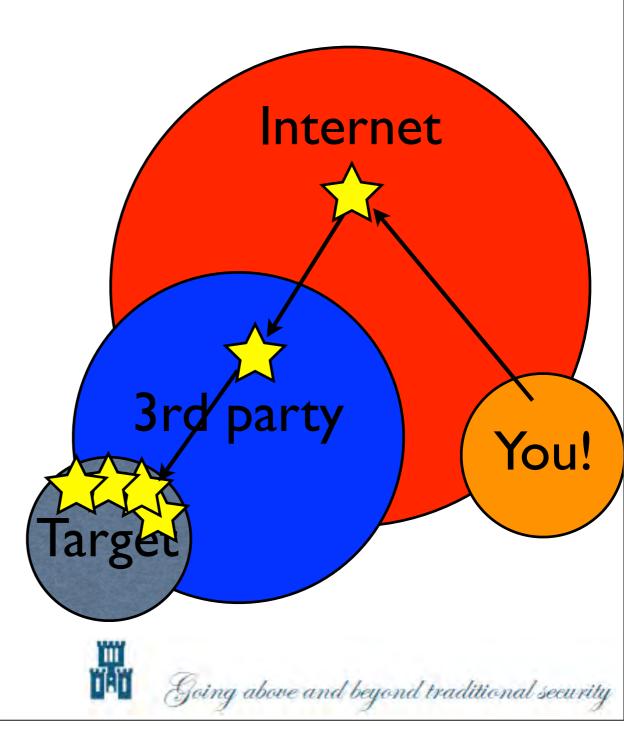
- Just use your friends (peers)
 - Expect a one-way command scheme.
 - Exfiltration is a different animal...



Control?

• What happens when you are so far behind?

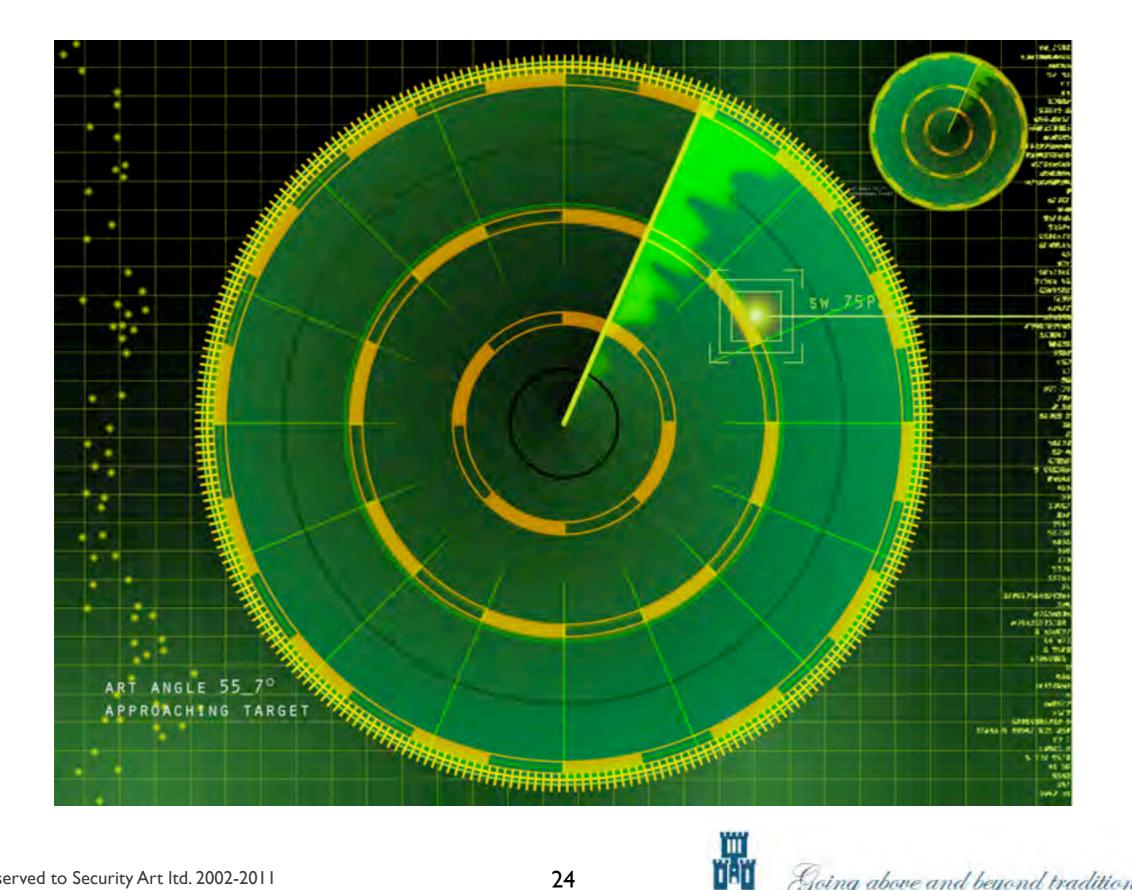
- Just use your friends (peers)
 - Expect a one-way command scheme.
 - Exfiltration is a different animal...



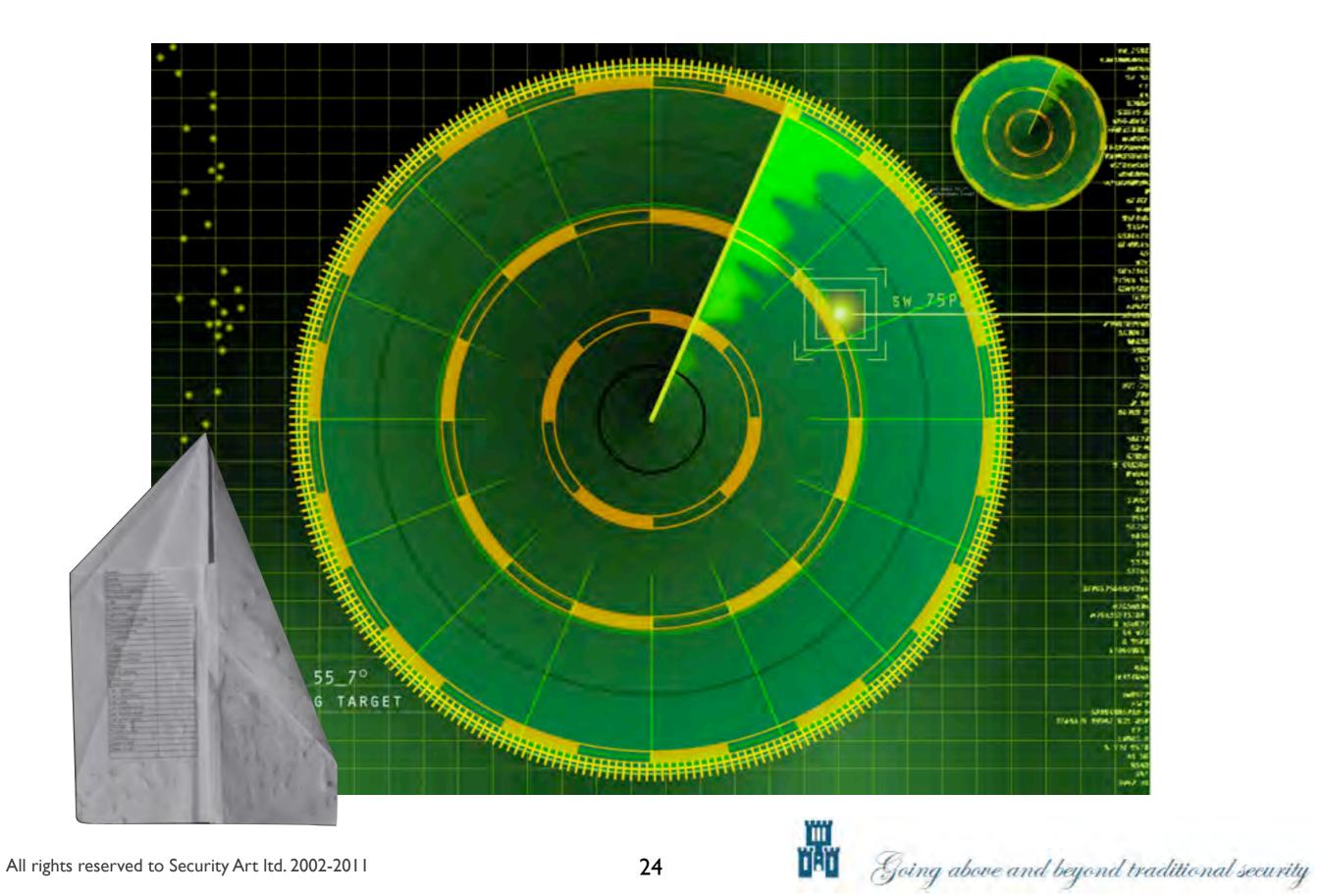
3. Exfiltration

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

All rights reserved to Security Art Itd. 2002-2011



All rights reserved to Security Art Itd. 2002-2011



Tuesday, September 20, 11

How about them SSLs?



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

All rights reserved to Security Art Itd. 2002-2011

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

hQMOAIjQIm6UkL4eEAv/W3r/eYLUmqRNi/Jegt72IK6qdBiBfkg9PZ5YKql9CUZp FGnVk029K3gEVcrA4k7w2aOtP7tYKRF8v4yrZQ9GZ7eXzR7+TbfIg+7dveH6U8Bf BHo8LRovj5OlGghrvpyKYRPlf/NAgzL2G8dyi/FVB0YB4J7/4x0YFEalQHaLiKyt /gkikyV92njPJ6tPm2sdKUqUHSb20r9AdowZ0VVRrWwdRgUhdNXajjwcbH1BjVuS Gilw8MnmQkmJAT+TAFkTqC9fjiwtnNMNANJbo2Z36RqsAcKbhVh1eMA7ev0pUakp Tm4xN64syk/IDEc0VHFbanAreTV3tCbUUIoPQDFGFpiu3oS6/089oUvRtBBbC5p6 leYKEnDIIcGWAomRSiYBFWjTca/DIw43QIW/ImdBnwcWLuQmDCmwr3HuhEaOmqfO hdgaxM4GuVdJCDdwXzwpuaPEICd18weH2XNzudLdeRKN+wjl/4D6blo+038BcLei SyhWrMFB7mKSmEzQufQUDACFamtMCn9YOo3mgo+YYk505qhIDLNwZXqyVUqOHvIG vu7gzuNwUdY5idLqsGEs0K0xVwYntTKUh61tNS/HDfNTVm4Y3p8M88JHhcg7npY5 gJuhWuHkgp2CTsQT+gRjthm3I3AInIvAfuC5uWLMsjA4sCw2FRDOARxrN9El8maX /vCxN9aB3dK4S9MSGJ5HhaYpTfpc9CdFkFryzb2sFWfW85nSzNo7dVFCy0jmSrI9 o4Jsfj0J0izS3MeGYYz5NSsfBz+6o/IYURL3OXrm4DuJNHY0DvVbYqSQRRx3o2S+ uZekwXwYsqpei/f/sYo875p5NeX3g62zgjy2Vly+n58WaZWoHb5Y0QCxNfpjdcAQ 3tuZQaUvlqrkQeSRxKXD7pxlHdwHDgfvw01RU8NsMkfsBoTZY27BjFvlg5S/pv9O 6lznXaJu9jRWDj6tvSypx8X2iiVgtSHYahlqEUH1RusAMCILkx0DydCvUud/qRbT YcnkVVgA8ojeDoVpp3AabRrSmgEAOwW6M0KvnSuMKniLlKe7kolqGjEuLAx7s5Kg mMHfNki5dYWvQzHv03ID9UG+uW6o54BnsajEVe2EcYTPT+8pg2bCxnMElK0ds9Is qvf2Kx4kqO0qMeJG1II2zfAFqmMiTMtgA2CZ0Y42hA/bQK/CCM8QVo9JcGn3Jf6N 0XITVob7xDo/fkRROHv74dlh2Kxa0SH8iGdb4kl=

So

=jN3t

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

Still "too detectable"

All rights reserved to Security Art ltd. 2002-2011

Still "too detectable"

hQMOAIjQIm6UkL4eEAv/W3r/eYLUmqRNi/Jegt72IK6qdBiBfkg9PZ5YKql9CUZp FGnVk029K3gEVcrA4k7w2aOtP7tYKRF8v4yrZQ9GZ7eXzR7+Tbf1g+7dveH6U8Bf BHo8LRovj5OlGghrvpyKYRPlf/NAgzL2G8dyi/FVB0YB4J7/4x0YFEalQHaLiKyt /gkikyV92njPJ6tPm2sdKUqUHSb20r9AdowZ0VVRrWwdRgUhdNXajjwcbH1BjVuS Gilw8MnmQkmJAT+TAFkTqC9fjiwtnNMNANJbo2Z36RqsAcKbhVh1eMA7ev0pUakp Tm4xN64syk/IDEc0VHFbanAreTV3tCbUUIoPQDFGFpiu3oS6/089oUvRtBBbC5p6 leYKEnDllcGWAomRSiYBFWjTca/Dlw43QlW/lmdBnwcWLuQmDCmwr3HuhEaOmqfO hdgaxM4GuVdJCDdwXzwpuaPEICd18weH2XNzudLdeRKN+wjl/4D6bIo+038BcLei SyhWrMFB7mKSmEzQufQUDACFamtMCn9YOo3mgo+YYk505qhIDLNwZXqyVUqOHvIG vu7gzuNwUdY5idLqsGEs0K0xVwYntTKUh61tNS/HDfNTVm4Y3p8M88JHhcg7npY5 gJuhWuHkgp2CTsQT+gRjthm3I3AInIvAfuC5uWLMsjA4sCw2FRDOARxrN9El8maX /vCxN9aB3dK4S9MSGJ5HhaYpTfpc9CdFkFryzb2sFWfW85nSzNo7dVFCy0jmSrI9 o4Jsfj0J0izS3MeGYYz5NSsfBz+6o/IYURL3OXrm4DuJNHY0DvVbYqSQRRx3o2S+ uZekwXwYsqpei/f/sYo875p5NeX3g62zgjy2Vly+n58WaZWoHb5Y0QCxNfpjdcAQ 3tuZQaUvlqrkQeSRxKXD7pxlHdwHDgfvw01RU8NsMkfsBoTZY27BjFvlg5S/pv9O 6lznXaJu9jRWDj6tvSypx8X2iiVgtSHYahlqEUH1RusAMCILkx0DydCvUud/qRbT YcnkVVgA8ojeDoVpp3AabRrSmgEAOwW6M0KvnSuMKniLlKe7kolqGjEuLAx7s5Kg mMHfNki5dYWvQzHv03ID9UG+uW6o54BnsajEVe2EcYTPT+8pg2bCxnMElK0ds9Is qvf2Kx4kqO0qMeJG1II2zfAFqmMiTMtgA2CZ0Y42hA/bQK/CCM8QVo9JcGn3Jf6N 0XITVob7xDo/fkRROHv74dlh2Kxa0SH8iGdb4kl= =jN3t

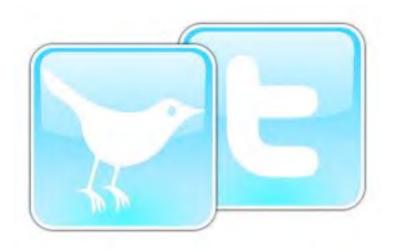
All rights reserved to Security Art ltd. 2002-2011

Much better

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

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

All rights reserved to Security Art ltd. 2002-2011













Going above and beyond traditional security

Resistance is futile

All rights reserved to Security Art Itd. 2002-2011

Ŭ A Ŭ

Tuesday, September 20, 11

But you have no network

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

All rights reserved to Security Art Itd. 2002-2011

Kill some trees

EfegalT/htm?JgmbJ]kPtN/M!":-m#ofLLe7!mST4/tldCn>l-HWWW+::/ltgNHMpM/ <#FU\%rh1WDrrr=8\DfD,=Ds82Ejs7%W\o)JOtrg2Eir9CWcrqu'orV2jRq>^lcq> P<j f-ig"CM:-otplroAY*nG]?UNDe),Mn_TFONADJrWV>O\uoFcs8FD5oY"G*liSt; 18. hp 1KhifctoladJ'Yd(YYbe,-3&kkOOFrrW#MZA'Y)m*i9=o1GTell6u1p\ophXnVHTPL4d'p ElegWie, n*KIGpAWCSo'l\XmlJ[td2OnW_tX011.4cMp6G*7f\$X/io**eleBMumVuGOSM 5;Wr."AHkUlVSNRn-u\$N9gb_sZUcmJ9bZrVm/"r8Ensrr;m-rq27grUQ34gtg9erg1Edp <#urWrKip_@-fq=FL_rpTjerr.p.q>^/oPI(8]o_n 'rr;<arX\'3s81mas72fWs8Mfn5 2Y. q>S'I=K(K'otBTIp[kln') Pro(MFSG<02) <i.gf](PmusBW)t'W#r;r;H2p 2Ving "ORhaKYn "WWWIgRgORX*gHfU">2Tp=6SileTDN51K, ELp4do) J[toRuffrr; Yor; F4Ga 2]p#027pqu600qZS01s7Pu(oDe ep& a]fY% "Pgt00hppf5]rYkP0rqEMArV1'n2H)k=0 lire marHuWbVgu?U' jOC3+jmu<8lanASoDee,mIDC_UTKUOnFZ_&R[j?,ZK&@VTOTJl: #1KM, BDKkHL5w8NZ) grR(15) s: JoAco71960, rr32flc004nc&RD&CGTaRfooWGa(R1) "#X-coZNMp\t.Hk4VMcDob45pAacpc272*b/"#PZ1=nhlMpMUgPWi(^WM-smcld&mu/Vmc IN [SN'3E b4UA (Rg+rVmS]r:m2008N&s=ke#mrU?'7rgc2n#6+>gplk@KuaN&us6E#as d=rV16bte, p5s5% +YPn(]=UZ)1=7H<jo \ WYa(a0](Z1()Ys8616 q>r:g30M'm1) >4eoD/Pb\c3=3qtTmPpYtGo^33aLsk]A:ptn[fs8W#tr1+m;rr2j\$r;9g0r:'CY"-(Uhq / Ar [m ?gAAdOPalHJIMI9NKoi [aWh'P e+Ash Cpotsps+ [OL [+R20] iaAi S'/sBEsti) Horquflrr) ljrlanDp&-derg+TUgtg?hrgc5S=IU>UrgG'Ap%JC\rK=qmrVWg/p\XmU 1: (ImdTiloDPrNm. / "kclg?!n+ZhLVB) uSC7E2Ac) *Etps[1- >jS@>Dd-lp:ting8M4Qr "4E|p' L rXel! [%caDrU SgmB60Wg>1-krW2Qbs6gX#c*d4DgiR9Wb10\sF\T74g" X o is total WH2mdErVcatrVZGerV1 przDubrWD Tens (S<rriamrq:TBrVulss8W' rVZQ ieb#laf%g=1i,Y4)>E*lbjDs6ogart"o)gIWeV*/0%2pmWT>q>1-k#D%lQN'1;Ng> Esm ZfsrOMo2nb'IFK) ^<.nEflHpjc(+;YKcdsEN)='W,09#2=Ytf=(57pc>j<c/AKth+T5R) -1%Nkp52=);AmPt/oZ/S*0>D/:BinfufqXX1Br:]mahRE(BM*qfErVc*#rFf.ec)A(fr 0[trr:pMg>U0gd]1:cp&=X[rabm"g72EgpF39upte-Jch=>002&5:p\rRamA4KiV]P> GifR.7H-oCW VpH4)prT^9mp+e0iblitage#2th<phCm(kZta)e)<20: XhheHtrKQ[Br SOcrUU!'s7cQ&IMpkbrg-6j(?Masd'h;)s7Z2ep[6"<@Z@frd.mV(s8F)"pri/IrpB* Elis7eRO uKG\HT: 3W:Q\pl:g'f'Cr?LeboF>q<jZ/POUVE?7'lGk]:ShqWD[GmE(,U cZnr,Entrr2j=rgl]1fr4]<s6Mopr:Ul)1r5rTrs/PlronItq>U3irVorsrpTjVs8E,m W/magesirr**im"Di]rVuWkrse;GAVlK*s8DflGSp,Fs7cf-2eW_WrOp0h"n055c'+jn VB*jRZPI:9PQ1#E.,H/F+FXg>UBnsEL.?s8:rsrr<#ts77KY]"UMZrX7?+K6+Eug<k6): kKSNBk <F, OAE[IB<]] "RLO845S.F- X?n, NishKeMer;#2Gp<B'#qu\$EkrYb[Gf tFm] x1'kpkc%rVlOjc-#nYs8EKirnEn?gu?KioXVm3p] (3trM/ffr;D\ls83/anQhSEr:'ac fBTMS];jp>>]Fe7mo) [Z/H,rV=f [pSpmmG0fEoURf=WW;YA+F'-S01M'>Fr1N*so'*6[-CeurBoP7Sa-4; sBE<\$nCjc) =72% js80n'T'<Dca71KYp6b [P1'YPBPuPWkg#90Ua:-jBc 3n ?cDp?gaC?icH>SOg8WU%rW& lrWi2sple;SnG3~* "SpWE:YGct*S6DmBYXTH\$NL+k [(OsBW.pqZSOsoVh'grWc,urr/g(rl<7\grgcgrr\Wh ;S\cr/RSSpL=Big=ssbrr`thr so stotsligw::SsssH\$Z7'H'bDAD] WCCNSSD-spSh40J>]Hn1M'bYHkGT?kgYiotgligh2; "J2s8)Z&rt>>&qt*1X?>?Y-1E"2d>"74\$rr2ctr1G->rr2ctr2j#a []Ail"=GepVjan eePrp1:M[#*]=0)7=rW3-'aC7)Up\#LhuA9*Z228;Mg16Hicr<'8k9/pAmgYU3hrVd7+

All rights reserved to Security Art Itd. 2002-2011

Ш

Going above and beyond traditional security

Tuesday, September 20, 11

To shred or not to shred?

TOP SECRET 4 Nor 1944

By some time so here been somerred by the reserving reports on fifting matters. They periodically mathines to only up during the last week, one musshearwed howering over Headblerg MF has but short thirty almotas. They have been reported by so many severes and from some is warriedy of places but a see more instance that they concer be disregaried and and be explained on mane hands that he perhaps slightly beyond the stops of our present intelligence Multing.

Here officers of this Hiereboreks recently visited the basish for initial series. This functions we get to the basis, first ensure we that some reliable and fairly technically initialized people have result to maximum that where phenomen are obtained to be result of a high basis of the second based of any presently income culters or marks." They are therefore assuing that these signate from our section, " they are therefore assuing that these signates from the earth.

One of these objects was observed by a Newligh technical expect near this how an ide edge of a labor. The object created or landed in the labor and he savefully period its axiamils from his point of observation. Swellich initiagence was sufficiently nonlinear to big abservation total a senilaring these and to the labor. Operations more untervery during the visit of their officers. Since had discovered a provinceing outland the stater in the fiber of the labor. We further information is evaluation to the return was reliable, and they believe that the depression on the fiber efforts on the fiber of the labor, the further information is evaluation, but subservation was reliable, and they believe that the depression on the fiber of the labor, main this stat appear on current hydrographic sharts, was in fast assessing a fibre of the labor.

Although screeting this theory of the origin of these objects prove a decise are group of questions and prior much of our thinking in a schemed light, so are justimed not to discretist actively this mannest spectroscie theory, exactly lengths as open alter as the schemet. Much are prove reactions?

....

(IDD OF DOUR THE

To shred or not to shred?



Num CE C

By some time to now here been conserved by the resurring reports on liping enters. They periodically mathine to sky up during the last week, our mus charavel howering over Meddlerg dir has for short Minty almeter. They have been reported by so many sources and from such a variable of pisces that on are socialized that they source to floregative and much be majorized to many have been either they source to floregative and much be majorized to many have added to perhaps whighly hered the stops of our present intalligence Mintage.

Here officients of this disperientwise reventing visited the hardist his initialization beyonds. This is an an an analysis of the second secon

One of these objects use observed by a Mediaki technical expect near bits how one the edge of a late. The object created or landed in the late and he savefully noted the sciencia from his point of observation. Smediak invalidations was sufficiently southern in this observation to be science on a sufficiently southern in the science of the science science of the science, the science of the of the late, which the science of science of the science of the science of the science of the science of science of science of the science of science of science of the science of the science of the science of science of the science of the science of the science of the science of the science of science of science of science of science of science of the science of science of

Although aroughing this theory of the origin of Ohem objects poses a shop are group of questions and pole much of our thinking in a shonged light, we are inviting into the discretist activally this momental spectroclar theory, matching insight an open alled on the endpott. (But are your sections?)

TOP DECENT

(BRO OF DOALSE ITSU

Going above and beyond traditional security

All rights reserved to Security Art Itd. 2002-2011

Yeah, good ol'e DD...



All rights reserved to Security Art Itd. 2002-2011

33

Back to hi-tech (?) ET Phone Home

All rights reserved to Security Art Itd. 2002-2011

Back to hi-tech (?) ET Phone Home

Got VOIP?

All rights reserved to Security Art Itd. 2002-2011

Back to hi-tech (?) ET Phone Home

Got VOIP? Excellent!

All rights reserved to Security Art Itd. 2002-2011

Back to hi-tech (?) ET Phone Home

Got VOIP? Excellent!

Target a handset/switch

All rights reserved to Security Art ltd. 2002-2011

Back to hi-tech (?) ET Phone Home

Got VOIP? Excellent!

Target a handset/switch

All rights reserved to Security Art Itd. 2002-2011

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

All rights reserved to Security Art ltd. 2002-2011

Tuesday, September 20, 11

Back to hi-tech (?) ET Phone Home

Got VOIP? Excellent!

Set up a public PBX OR a conference call OR a voicemail box

Target a handset/switch

All rights reserved to Security Art Itd. 2002-2011

Back to hi-tech (?) **ET Phone Home**

Got VOIP? Excellent!

Target a handset/switch Set up a public PBX OR a conference call

Collect your data

Going above and beyond traditional security

OR a voicemail box

All rights reserved to Security Art ltd. 2002-2011

Back to hi-tech (?) ET Phone Home

Got VOIP? Excellent!

Target a handset/switch Collect your data Set up a public PBX OR a conference call OR a voicemail box

All rights reserved to Security Art ltd. 2002-2011

Tuesday, September 20, 11

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

All rights reserved to Security Art Itd. 2002-2011

Tuesday, September 20, 11

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

All rights reserved to Security Art ltd. 2002-2011

Tuesday, September 20, 11

Back to hi-tech (?) ET Phone Home

Got VOIP? Excellent!

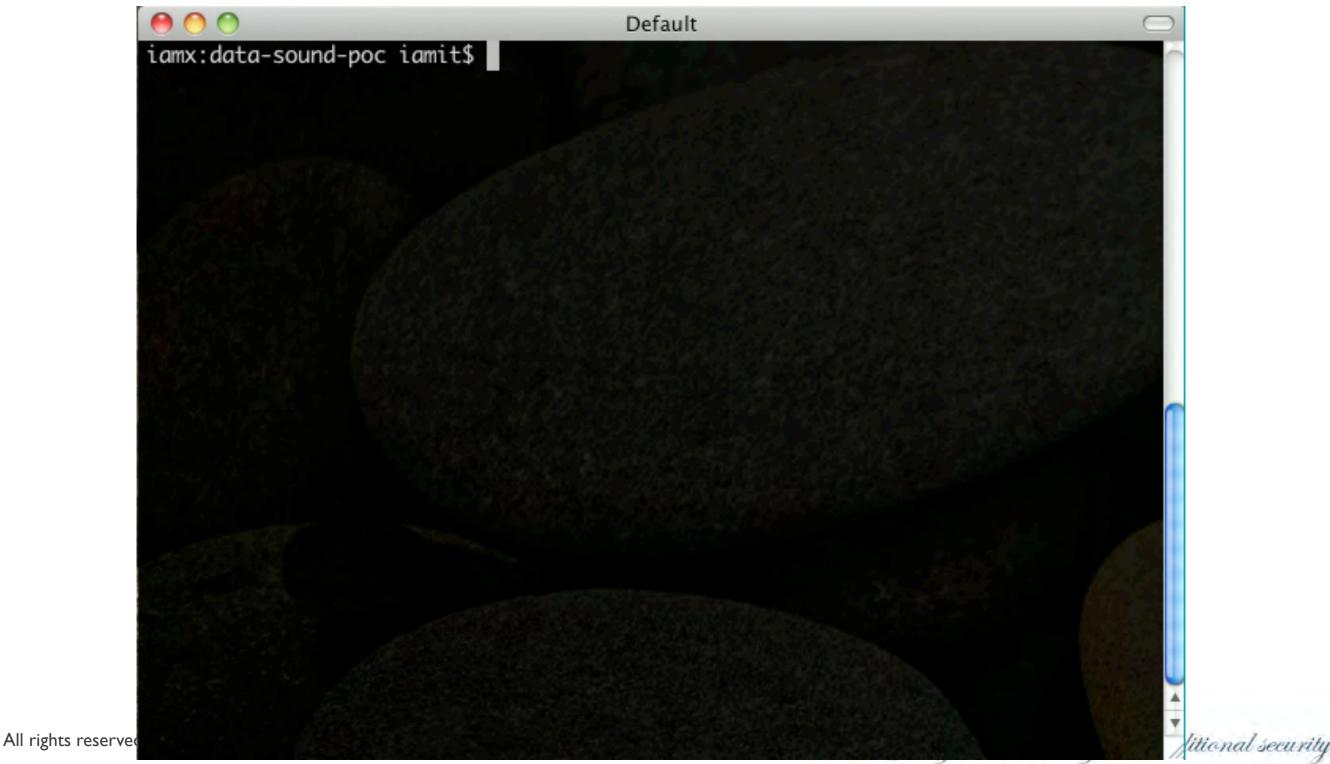
Target a handset/switch Set up a public PBX OR a conference call OR a voicemail box All rights reserved to Security Art Itd. 2002-2011 Call, leave a message, don't expect to be called back...

Tuesday, September 20, 11

Voice exfiltration demo

All rights reserved to Security Art Itd. 2002-2011

Voice exfiltration demo



Tuesday, September 20, 11

Voice exfiltration demo

All rights reserved to Security Art Itd. 2002-2011

Voice exfiltration demo



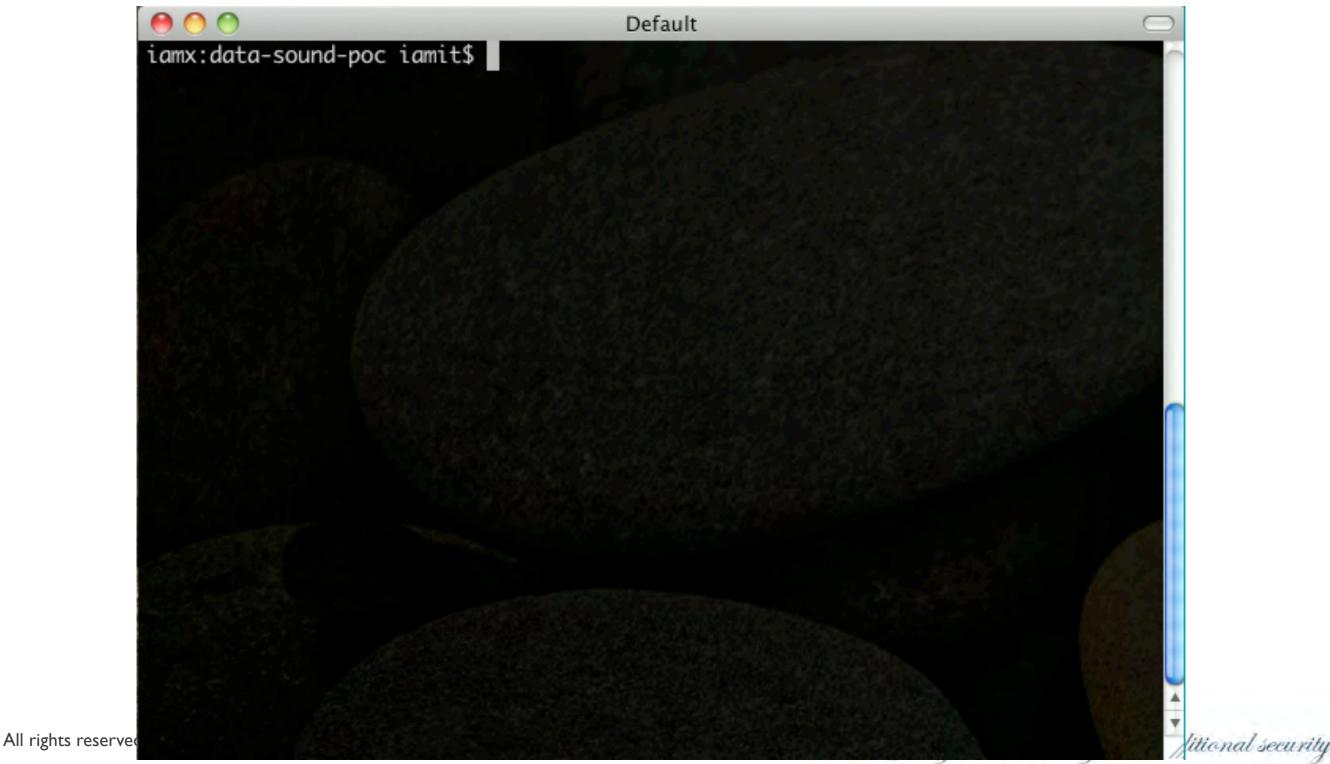
All rights reserved to Security Art ltd. 2002-2011

35

Voice exfiltration demo

All rights reserved to Security Art Itd. 2002-2011

Voice exfiltration demo



Tuesday, September 20, 11



Killing paper isn't nice

- Fax it!
- Most corporations have email-to-fax services
 - heard of the address
 <u>555-7963@fax.corp.com</u> ?
- 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



- Start with the human factor
- Then add technology

Controls

- Start with the human factor
- Then add technology







Going above and beyond traditional security

- Where people leave data
 - **Hint** spend time with developers.
- "Hack" the **business** process

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

All rights reserved to Security Art ltd. 2002-2011

Map your assets



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

Old chinese proverb

All rights reserved to Security Art ltd. 2002-2011

41

And monitor them!

They are YOUR assets after all

No reason to be shy about it...



Going above and beyond traditional security

And remember to add honey...

All rights reserved to Security Art Itd. 2002-2011

Tuesday, September 20, 11

2 tips for monitoring

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

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

All rights reserved to Security Art ltd. 2002-2011



TEST SOME MORE



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



All rights reserved to Security Art ltd. 2002-2011



Questions?

Thank **you**!

Whitepapers: <u>www.security-art.com</u>

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? <u>twitter.com/iiamit</u>

Going above and beyond traditional security

All rights reserved to Security Art Itd. 2002-2011