

Data Exfiltration Not just for Hollywood!

Iftach Ian Amit VP Consulting

DC9723 CSA-IL Board member IL-CERT Visionary tienna Annual FIRST Conference

All rights reserved to Security Art Itd. 2002-2011

Tuesday, May 31, 2011

whoami

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

All rights reserved to Security Art Itd. 2002-2011



- I. Infiltration
- 2. Data targeting & acquisition
- 3. Exfiltration

All rights reserved to Security Art ltd. 2002-2011

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

All rights reserved to Security Art ltd. 2002-2011

6

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...

All rights reserved to Security Art Itd. 2002-2011

Infiltration - Human





Going above and beyond traditional security

All rights reserved to Security Art Itd. 2002-2011

9

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
- Create a Payload and Listener
- 5. Mass Mailer Attack
- 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

11

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



All rights reserved to Security Art ltd. 2002-2011

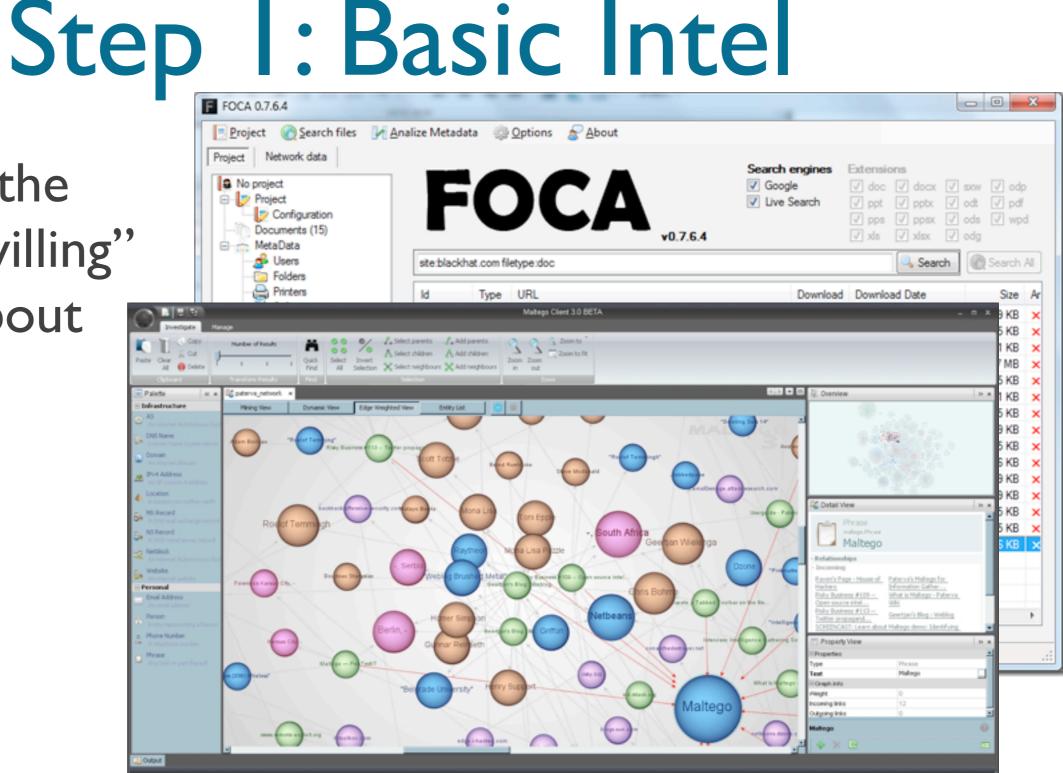


2. Data Targeting & Acquisition

- Weaponizing commercial tools
- Creating "APT" capabilities

All rights reserved to Security Art Itd. 2002-2011

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

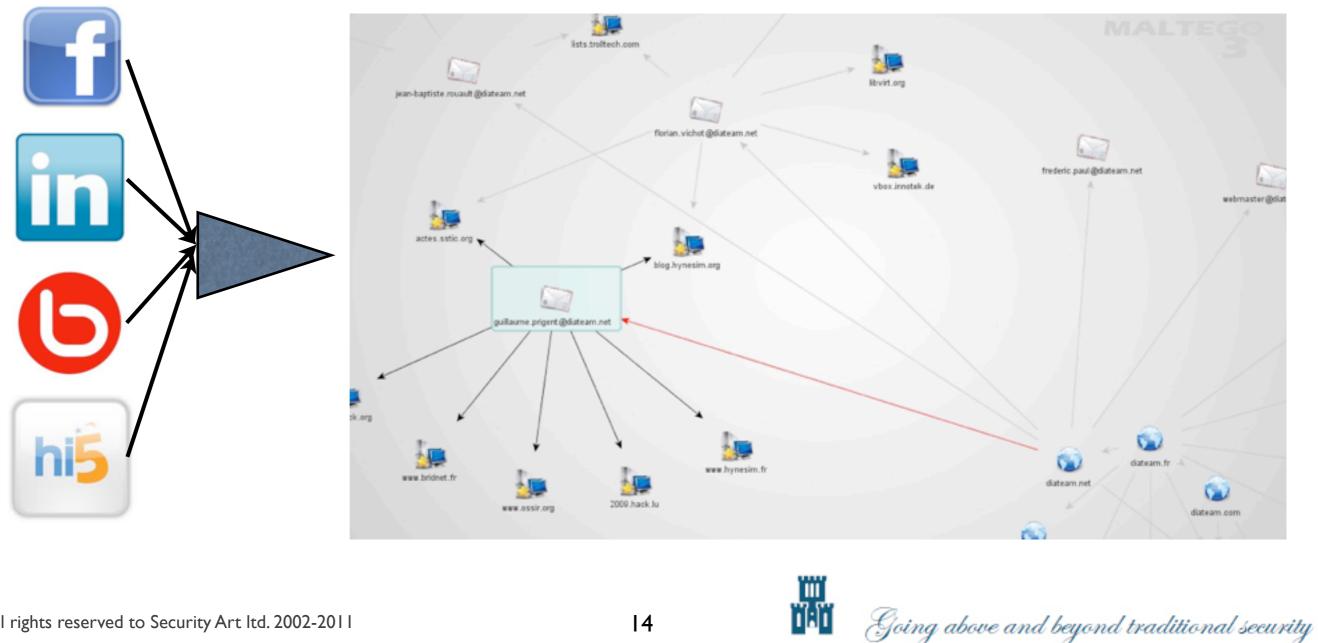


Î

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

Tuesday, May 31, 2011

Select your target wisely

And then craft your payload :-)

All rights reserved to Security Art ltd. 2002-2011

Not as expensive as you think

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

😂 ZeuS Builder	
111011180011	mation rrent version information
👁 SpyEye 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 Melt server	Rootkit
This option will unhook kernel mode hooks to allow t and the user needs to be logged in as administrator.	bypassing more firewalls. It is limited to windows XP only
vARNING: This function is still in beta and could ma aution.	ake the remote computer crash if it fails. Please use it with Build Cancel

Going above and beyond traditional security

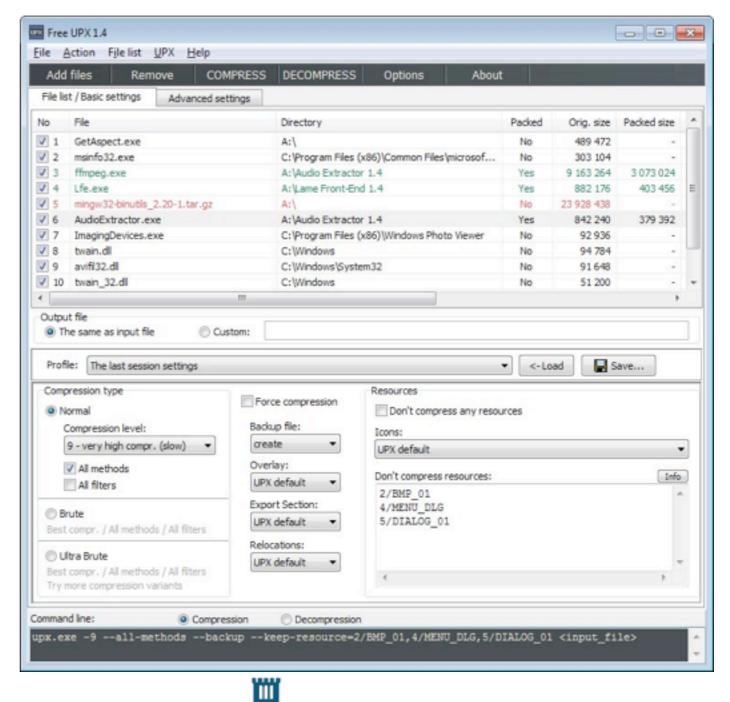
Tuesday, May 31, 2011

Just make sure to pack

Experienced travelers know the importance of packing properly



All rights reserved to Security Art Itd. 2002-2011



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 <section-header>

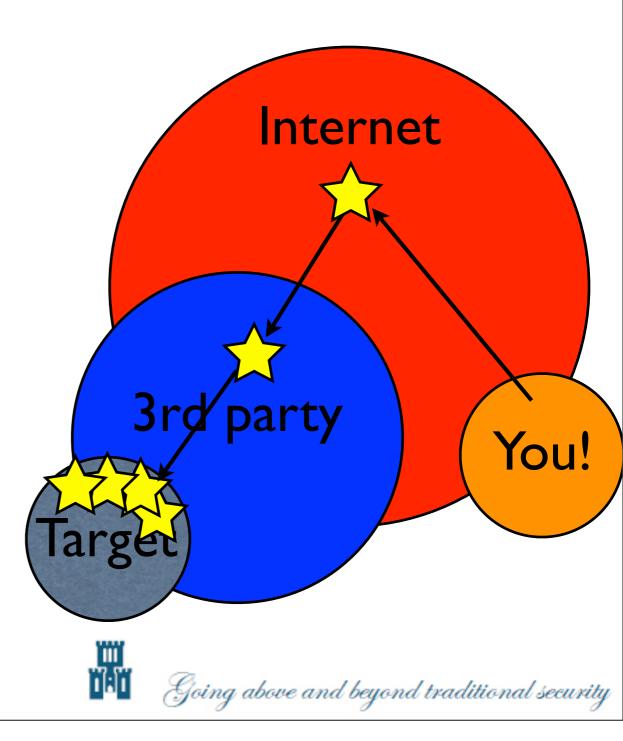
Going above and beyond traditional security

All rights reserved to Security Art Itd. 2002-2011

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...



All rights reserved to Security Art ltd. 2002-2011

3. Exfiltration

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

All rights reserved to Security Art ltd. 2002-2011

Under the radar

• What does the radar look for?



All rights reserved to Security Art ltd. 2002-2011

How about them SSLs?



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

All rights reserved to Security Art ltd. 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"

hQMOAIjQIm6UkL4eEAv/W3r/eYLUmqRNi/Jegt72IK6qdBiBfkg9PZ5YKql9CUZp FGnVk029K3gEVcrA4k7w2aOtP7tYKRF8v4yrZQ9GZ7eXzR7+Tbf1g+7dveH6U8Bf BHo8LRovj5OlGghrvpyKYRPlf/NAgzL2G8dyi/FVB0YB4J7/4x0YFEalQHaLiKyt /gkikyV92njPJ6tPm2sdKUqUHSb20r9AdowZ0VVRrWwdRgUhdNXajjwcbH1BjVuS Gilw8MnmQkmJAT+TAFkTqC9fjiwtnNMNANJbo2Z36RqsAcKbhVh1eMA7ev0pUakp Tm4xN64syk/IDEc0VHFbanAreTV3tCbUUIoPQDFGFpiu3oS6/089oUvRtBBbC5p6 leYKEnDIIcGWAomRSiYBFWjTca/DIw43QIW/ImdBnwcWLuQmDCmwr3HuhEaOmqfO 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

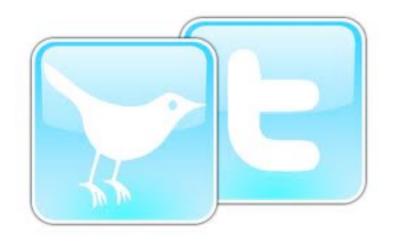
Tuesday, May 31, 2011

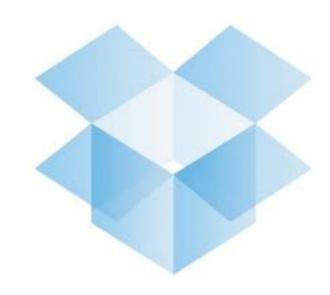
Much better

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

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

All rights reserved to Security Art Itd. 2002-2011













Going above and beyond traditional security

Resistance is futile

All rights reserved to Security Art Itd. 2002-2011

u Man Dan

But you have no network

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

All rights reserved to Security Art ltd. 2002-2011

Kill some trees

Ef@q#IT/htm?JqmbJ]kPtN/M!":-m@ofLL<7]mST4/tl3Cn>3-H200+;;\lqNHMpMpc <#PU\Xrh!WDrrr=8\DfD,=Ds82fjs7XW\o)JOtrgZEir9CWcrqu'orV*jRq>^lcq> F<j f-iq"OML-otplroAY*nG]?UkOe);MnJ7fOnADJrWV>O\aoFcs6FD5oY"G*liS+k :8,*p 1KhifotpliadJ'Yd(YYbe,-3&kkOQFrrW#mZN'Y)m*i9=0)GTeli6ulp\OphXnVATLad'p E\>gV;8;n*KiGpAWCSo'l\XoJJ[tdZOnW_tX011.4sMp&G"7f\$X/io'"a)s8MumVuGQSW j,Wr.*«HkUlVSNRn-u\$N9gb_sZU<mJ?bZrVm'"r8En8rr;m-rqZ?grUQ34gtg9erglEdP <#urWrKlo_@-fq=FL_rpTjerr:p,q>^/oPI(8]o_n'rr;<arX\`#s81m@s72fWs8Mfn5 2Y.q>S'I=K(K'otaTIp[kln')_Pto(MFSG<02)<; gf](Pmus8W)t'W#r;r;Hzp*8Ving "ORhaK?s+78UX1gEgORX*gHfU'>2Tp=6SiL6TDN&iK,ELp4do)J[toRuf6rr;Yor;F%Gq Z]p#Q27pqu6QdqZ\$O1s7Pu(oDe^ep&"a]fY%"PqtU0hppf5]rYkP0rqEMArV1'nZH)k=c lire m:rMuWbVqu?U'jOC3+jnu<8laaA\$oDee;mIpO_UTKUQnFZ &R[j?,ZK&@VTOTJl: =#iKM, sDkkhL5s8NZ) grR\1S)s. JoAco7fg&C, rr32flcQU4nc&RD%CGTaRf0oWGa(R1) "#XgoZMMp\t.Hk4VM<D0b45pAacpc272*b/"#PZ1@nhlMpMUgPWi(^%M-smCld&mu)Vmc Be[SN'3E\b4UA^\Rg+rVm\$!r:m2gs8N&s#ke#mrU?'7rqcZn#6+>qplk@Ks8N&us8E#ss /dm5rV16b*<,p5s68^%YPn(]rUZ]1s7H<jo \[VYa(s0](Z1()Ys8&1&^q>r:g3OM'mI)) p/4eoD/Fb\c3*3qtTmPpYtGo~33aLs&)A:p*n[fs8W#trl+m;rr2j\$r:9gQr:'CY"-(Chq /(Ar[m^?gAAdQPaLHJDmI9NKoi[aWhWe+Ash\Cpotsp&+[OL[+R20]i@Al^\$'/s8E&tr)3morquflrr)ljrIsnDp&=derg+IUqtg?hrqc5SmIU>UrqG'Ap%JC\rK=qmrVWq/p\XmU' Wi3mdTiIoDPrNm. ' "kclg? !n+ZhLV8) u\$07E2Ao) *Etps [1- >j\$@>0d-1p:tIng8M4Qr 4E]o'"L rXei![%caOrU^SgmB60Wq>1-krW2Gbs6gX#c"d4QqjR9Wb!0\sF\T74g"jX_1 fK+totohaQ?8°qn, E:crW:3°oDednN8jX;XP3°R\$Mj rrViVHR-sbBs8EbP; fobaliaa3/3 '6'da<;WH2mdBrVca#rVZGerV1'przDuSTWDTUN9(\$<rr!#mrq;TBrVulss8W''rVZQ_ 16b#laf%q=ji,+4) >f"1bjDs6ogart"o)qlWeV';0?2p@MT>q>1-k#OKlQN'1;Nq> Est ZfsrOMa2nb)1KK) ^<.nEf1Hpjc(+;YKtds8W)s'W,09#Q=Ytf=(S?pc>j<c/AKtn+T5R) -1%Nkp53=);AmPt/oZ]S"0>D(:Bi^nfufqXX!Br:]mahRE(BM"gfErVc^#rp1.eo)A[f 0 [frr;pMg>U0gd)1:cp&=X[ratm"s7ZEgcF39sp%e-Jchs>0J?&5:p\rRHp6A4KiV]P> Oi6R, 7H-oCW"Vp84]prT-9mp%eUlh1itags#Qih<phOm(kZ%n)s]<ZO: *Xhh6BtrKQ[Bt SOcrUU!'s7cQ&lMpkbrg-6j(?Maso'h;)s7Z2ep[6"<@Z@frd.mV(s8F)*prlJIrpB^. &lis7#R0 uKG\HT:'3W;Q\p!:g'f'Cr?&eboF>q<jZ/POUVf^7'lGkl;8hqWD[@mf(,U cZnr;Entrr2j-rql]ifr4]<s6Mopr:U!)ir8rTrs/PlronItq>U3irVcrsrpTjVs8E,ms W/mg8cSirr**im^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): kKSW8k <P,OAE[IB<]]"RLO845S,F- X?n,N@shKeMer;#ZGp<B'#qu\$EkrYb[Gf tF@s xi'kPkGZrVlOjc-#nYs8EK!rnEn?qu?KioXVm3p] (3trM/f[r;D\ls83)srQhSEr:'ac fRTMS]; jp>>] FE7@0) [Z/H, rV=f [pSpmmG0fEoURf-XW; YA+F'-SQ1M >Fr1N*@0'*6[< C<urBoP?Sa-4;s8E<\$nCjc)s7ZKjs8On'T'<Dcs71KYp6b[P1'YPBPuPWkg#90Ue:-]Ec 3n ?cDp?q#C?icH>SOg8WU%rW& lrWi2sp[F{@nG3+'"SpWE:YGct*S6DmBYXTH\$NL+k [(0s8N,oqZ\$QsoVh'grW<,urr;g(r1<7\grq<grr)Wh_:S\cr;R\$\$p4=B%q=ssbrr'&hr s0 #09943#:!Ss8EH\$Z7'H'oDAO] 'WQCNs8D>ep\$h40J>]HnlM'bYHkGT?kgYi0teHan2r "J2s8) Z&rt>>&qt*1Z?>?Y-1E"2d>%74\$rr2otr1G->rr2otrr2j#n []Ai1^mGepV]+7 eeFrp]:M[#*]=0)7=rW3-'aC?)Up\#LhuA9*Z2X8;Mgf6Hicr<'8k07pAmgYU3hrVd?+'

All rights reserved to Security Art ltd. 2002-2011

Ш

To shred or not to shred?

TOP SECRET L BUT 1966

Num CE C

By some time to now here been conserved by the resurring reports on liping enters. They periodically mathine to sky any during the last work, one was characted howering over Neutlersy sir has not short thirty almeter. They have been reported by a many sources and from such a variaty of pisces that on are socialized that they source to floregative and next be explained to many hards which is perhaps whighly haven the source of our present intelligence Mathing.

Here officients of this disperientwise reventing visited the hardisch for initialization devices. This denotes we put to the Monders. They's account must hast some reliable and folicy technically initialized people have reacher the maximum that "Share phenomena are obticably the result of a high matching will within account be available to any prevently from cultors o match." They are thereafters assuming that there shipsing acting factor from extinging a statement of the section of the section of the section pertonsity memory or unidentified betweening, pertonsity relative to earth

One of these objects was observed by a Mediah technical experimentics how one that edge of a late. The object created or landed in the late and he carefully moted its asianth free his point of observation. Sensitiv insisting was and interactly socilations in the observation was a social asing interaction of the late. Operations more underway during the state of digits of filters. The state of order observation that the state of digits of filters. Since, the forther inderwation is a socitical of digits of filters. Since, the forther inderwation is a social interaction may compare the index of the results. In their optimize, the state of the state of the state of the results. In their optimize, the state optime are reliable, and key believe that the depression on the filter of the late, which this and appear on current hydrographic during, was in fact assess in preliming severe.

Although according this theory of the origin of Uses objects poses a shop are group of theritons and yoks much of our blacking in a thought light, as are justiked into it deteredit activity this somethic spectroclar theory, sensites insering an open alled on the subject. They are your "sensition"

TOP

(BRO OF DOURS ITTER

Going above and beyond traditional security

All rights reserved to Security Art Itd. 2002-2011

Yeah, good ol'e DD...



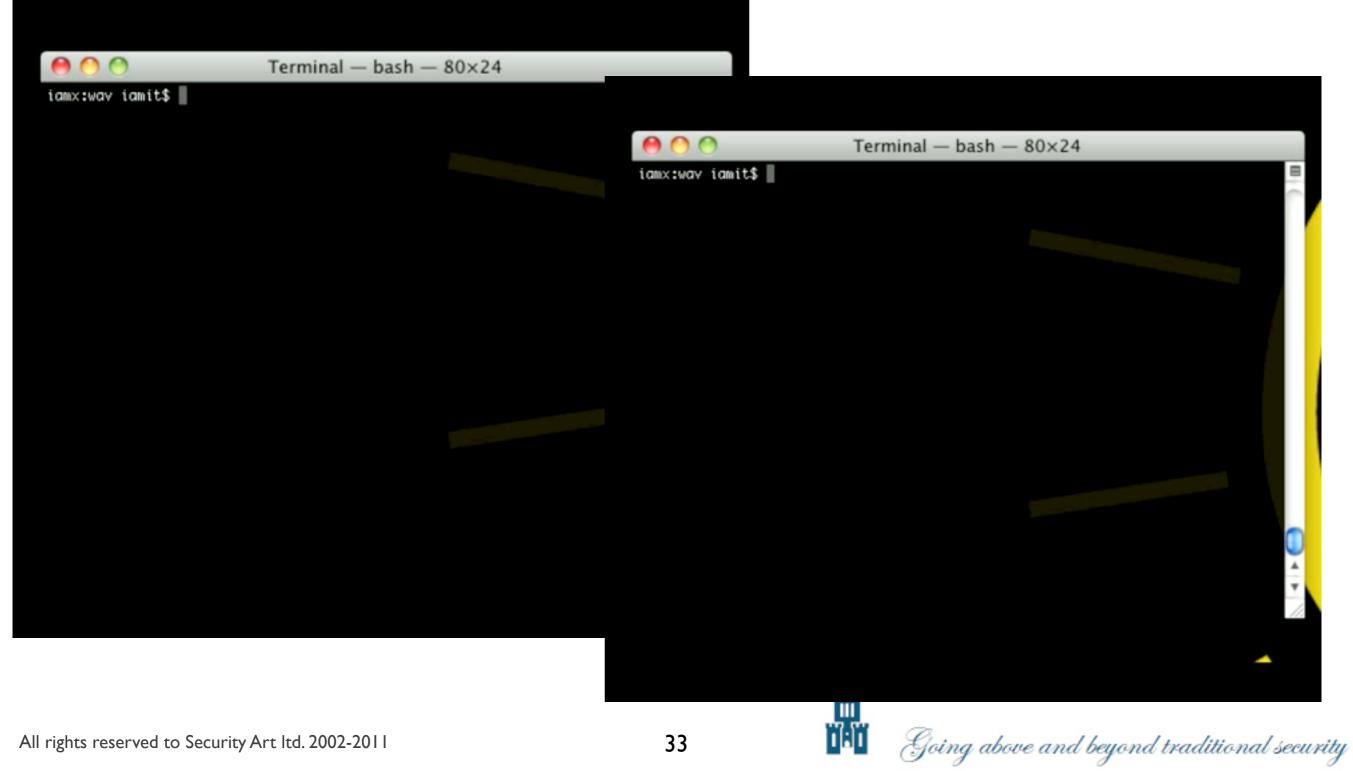
All rights reserved to Security Art Itd. 2002-2011

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...

Voice exfiltration demo



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

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!

All rights reserved to Security Art Itd. 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

38

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 ltd. 2002-2011



TEST SOME MORE



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

All rights reserved to Security Art Itd. 2002-2011



Going above and beyond traditional security

Shameless Plug!

Questions?

Go get your fix here: <u>www.security-art.com</u>

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

Need your daily chatter? <u>twitter.com/iiamit</u>

Going above and beyond traditional security

Thank **you**!

All rights reserved to Security Art ltd. 2002-2011