Rootkits are Awesome:

Insider Threat for Fun and Profit

Michael Kemp
clappymonkey@gmail.com

clappymonkey

TROOPERS 09
get skilled or get owned

I don't want to be sued...

- It should be noted that any ideas, views or opinions expressed in this presentation or supporting materials, are in to way indicative, reflective or representative of the views, opinions, or ideas held by my current or any previous employer. Additionally, this talk will probably annoy a number of vendors. Sorry, about that (honest)...

/end disclaimer

Before we begin...

- This is the 2nd Troopers con and my 2nd time here
- Last year I spoke about Virtualisation – this year I'm co-author of the upcoming 'Hacking Exposed: Virtualisation' from McGraw Hill – largely thanks to the con
- My thanks to the ERNW crew for organising such a great event
- I'm sure that this talk will completely ruin the l33tness of the event...

Apropos of Nothing...

- “The average man does not want to be free. He simply wants to be safe”

  H.L.Mencken

- “Just think how stupid the average person is, and then realise that half of them are even stupidier”

  George Carlin

What will I be ranting about?

- Taking Cows to Market
- Realities and Illusions
- Trusting Trust

Taking Cows to Market

Taking Cows to Market

- Recent years (well since about 2006) have seen a substantial rise in the number of vendors seeking to address the insidious threat of the internal
- There are a number of reasons for this, not least regulatory
- The use of Data Loss Prevention tools is growing across sectors
- Vendors are falling over themselves to facilitate this emerging market

Taking Cows to Market

- Data Loss Prevention Tools have a host of aliases
  - Information Loss / Leakage protection
  - Content monitoring and filtering / protection
  - My favourite is 'extrusion prevention'
    (that sounds like something nuns do)

Taking Cows to Market

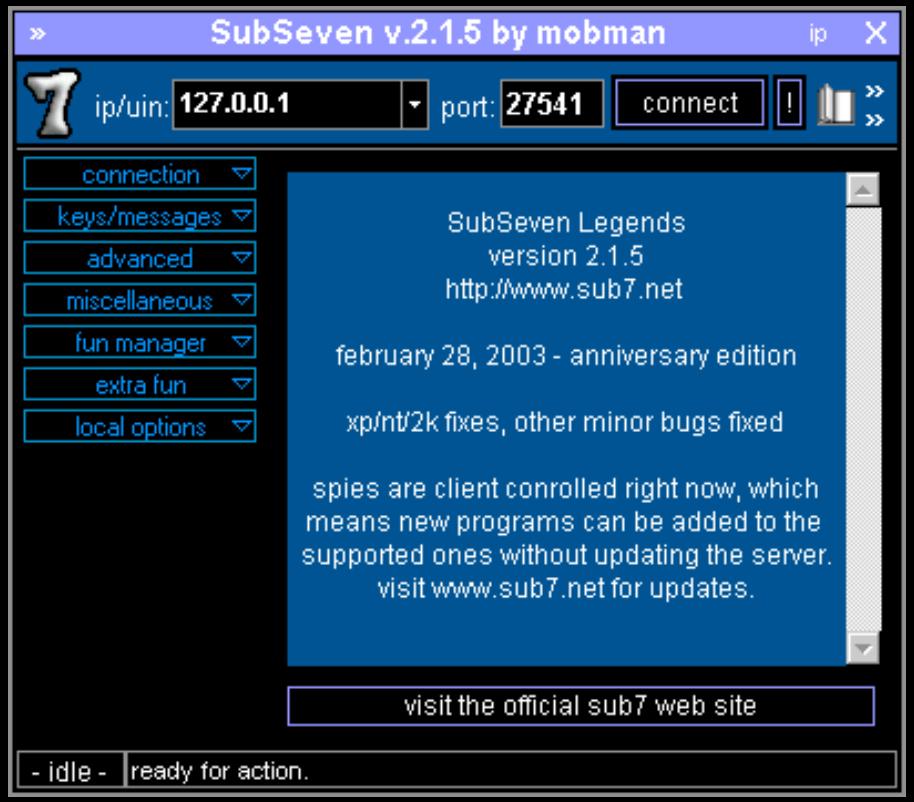
- DLP Products are being sold in an adolescent market
- Depending on your take DLP is part of the 'endpoint' security market
- Gartner reckons that the market is worth billions (http://www.gartner.com/it/page.jsp?id=500694) – that was before the current financial meltdown though...
- Vendors are rapidly trying to re-engineer current endpoint suites – the focus has shifted though...

Taking Cows to Market

- DLP Software
  ha
  s a number of key components (depending who you buy it from)
  - Centralised Management
  - Coverage of content across platforms and locations
  - Analysis / Capture of content

  Any of that sound vaguely familiar?

Taking Cows to Market



Taking Cows to Market

- Call these apps what you will; personally I tend to think they are nothing more than rootkits
- Don't believe me? Consider the following:

Taking Cows to Market

Taking Cows to Market

- Other vendors aren't slow to promise stealth (your employers need never know of your nosiness)
- Both McAfee and Symantec solutions can be run in stealth mode
- Smaller vendors are even more vocal about the obfuscated nature of their solutions

Taking Cows to Market

- There's a split across DLP solutions at the moment: Gateway and Agent based
- The agent based approach is worrying and includes vendors such as McAfee (formerly Reconnex and Onigma) and Trend Micro (Provilla) as well as a host of other smaller companies

Taking Cows to Market

- Lots of noise about
  DLP
  s
  oftware being the great panacea (and making compliance easy)
- Less focused research on how it does what it does, what that means, and the
  po
  tential threats that can be presented by its implementation
- Worth looking beyond the vendor hype...

Realities and Illusions

Realities and Illusions

- So, how do DLP apps work?
- Well, they monitor user activities for deviation from policies
- They do this in one of seven ways traditionally
- The current seven deadly sins are...

Realities and Illusions

- *The RegEx approach* – Software analyses user content for known regular expression (e.g. 16 digits = CC #, etc.). Rule based approach used in pretty much every solution (most ship with default rule sets).
- The issues with regex approach are well known e.g. you *will* get false positives and you won't catch deviations from the rule set...
- Still the most popular way of doing stuff though

Realities and Illusions

- *File Matching* – As the name suggests, take a hash of a file and monitor for deviation in hash. Not analysing content, but context
- Not useful at all if files are edited, and pretty trivial to evade...

Realities and Illusions

- *Categorisation* – Both rules and dictionaries used to discover common sensitive data in tr
  ansit (e.g. credit card numbers / violations of the PCI DSS)

- Useful for data that fits into simple categories or policies – one size does not
  fit all, and for custom protection not great to configure...

Realities and Illusions

- *Database matching* – this approach uses DB dumps
  or
  live ODBC connections to discover data that matches exactly
- Only useful if the DB is linked in, also ignores anything not in the DB (so great for stopping CC #'s but do you really want to put them in one central DB anyway??)
- Performance issues and lag with large DBs

Realities and Illusions

- *Cyclical hash matching* – otherwise known as partial file matching. A hash is taken of content, offset by characters, and then another hash taken until document completion
- You must know what documents (exactly) you want to protect, and there is limited volume. Because of common phraseology false positives may pop up
- Also like some of the other detection mechanisms can often be overcome with encryption

Realities and Illusions

- *Statistical Analysis* – Uses statistical techniques such as Bayesian analysis to determine
  deviations from partial document matches across repositories
- Require
  s
  a huge source of content (lag and risk exposure as a result)
- Produces false positives but good for nebulous content

Realities and Illusions

- *Lexical Analysis* – Seeks to analysis content according to dictionaries, rules and resemblance and can help find loose policy deviations
- Usually deviations as defined by vendor not implementer
- Because of the loose nature, prone to inaccurate reporting

Realities and Illusions

- That's how things claim to work; how do they actually work?
- I wanted to examine solutions, and actually find out how they do what they do
- If you can discover how something works you can break it!

Realities and Illusions

- Es
  tablishing what is going on with DLP software is not easy...
- I approached numerous vendors and was largely ignored
- Symantec are a good example...
- Symantec purchased
  Von
  tu and now offer DLP software (Vontu Data Loss Prevention 8)

Realities and Illusions

- Hav
  e
  y
  ou ever tried to contact Symantec? (If so, you know my pain)
- 4
  ca
  ll centres, 9 looooong telephone conversations = no software
- Vontu DLP 8
  cos
  ts $25,000 so no wonder I didn't get a freebie to play with

Realities and Illusions

- I did find some stuff out though...
- According to a reliable source the Sophos Anti-Rootkit software does not detect the Utimaco / Sophos DLP software
- I wonder if that holds true for Trend Micro and McAfee? (I'll bet you it does)
- Even with the basic research I've been able to do vendors don't detect each other – interesting...

Realities and Illusions

- Smaller vendors were nicer to play with
- Hardly surprising as they are not selling ridiculously expensive applicatio
  ns and don't have 18 telephone numbers none of which work...
- One such vendor was Interguard (www.interguardsoftware.com)

Realities and Illusions

- The Sonar Management Suite from Interguard / Awareness Technologies is fairly representative of smaller endpoint DLP software
- It works via a simple client / server model
- Admin installs client on target box (requires login). User actions via API hooks are fed back to central Internet server via HTTPS for later analysis

Realities and Illusions

- One thing that raised a chuckle, is that on install the software requests that 'anti-spyware', 'anti-virus' and 'anti-rootkit' applications are turned off... I'm sure everything will be find then...
- So, what information can admins have a look at then?

Realities and Illusions

- Using a web portal (yup the data leaves the networ
  k
  - in this, and many other solutions) an authed user can see
    - All keystrokes (plain text pw - yay!)
    - All incoming and outgoing mail
    - All web traffic
    - All accessed and edited documents
    - All screenshots
    - Pretty much everything

If I can get your auth - it's game over...

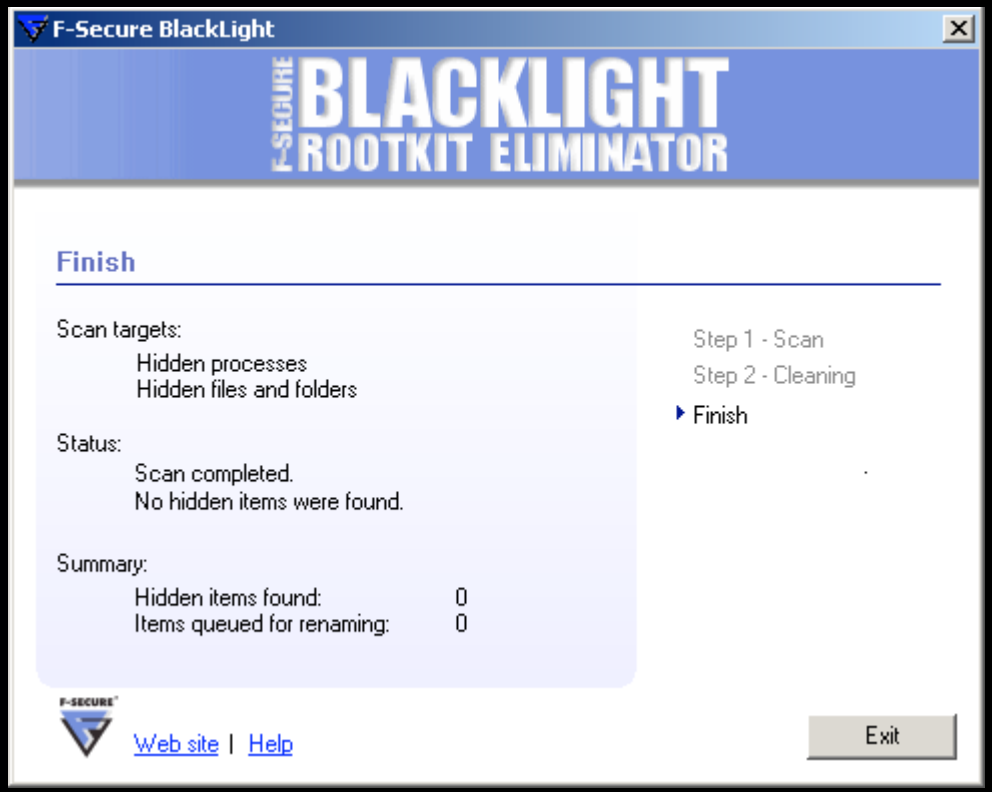
Realities and Illusions

- The vendor claims: “Sonar is a software solution that can be deployed invisibly without end user intervention, and remains undetectable to the user”
- Well, sort of...

Realities and Illusions

- Avast Anti-Virus Version 4.8 doesn't detect anything awry on either a boot or base scan
- Sophos Anti-Rootkit version 1.3.1 (build 108) detects nothing
- M$ Rootkit Revealer version 1.71 detects nothing
- F-Secure Blacklight 2.2.1092 detects nothing too

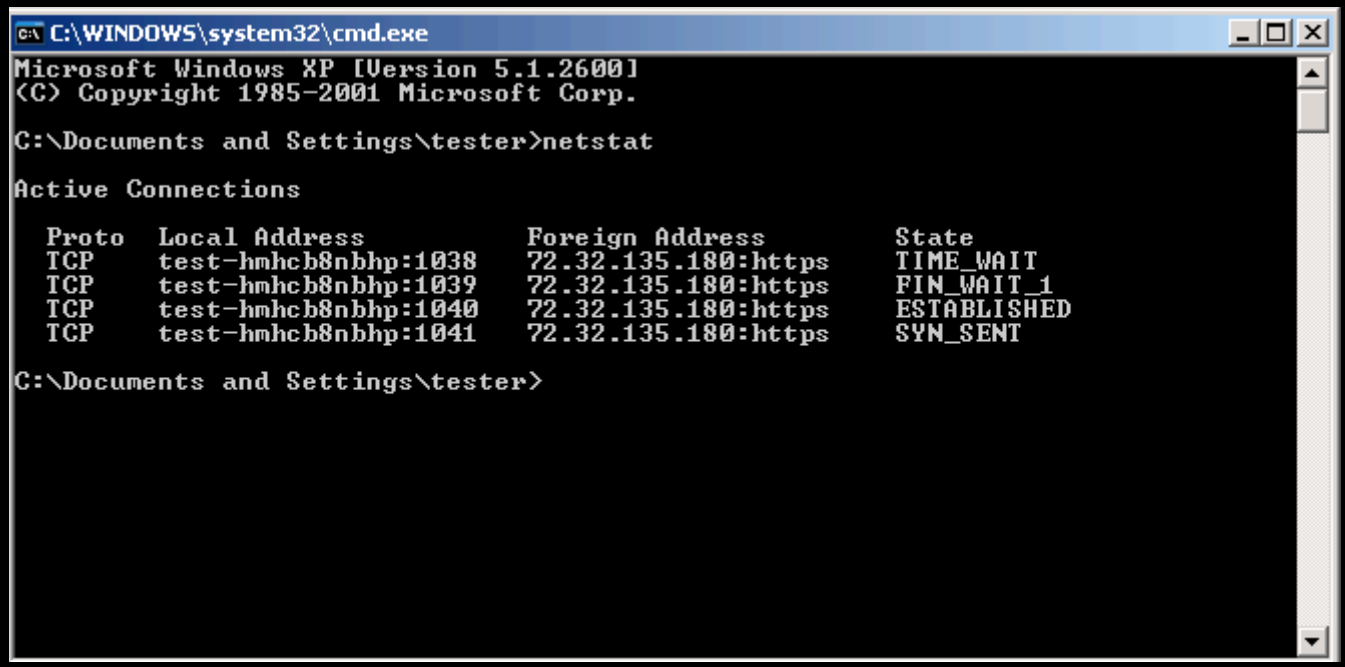
Realities and Illusions



Realities and Illusions

- So, is anything actually going on?
- If a
  us
  er can use netstat they can spot this solution a mile off...
- Because of the centralised server (great idea...) it opens
  a
  n
  umber of ports in the 1000 range over HTTPS to 72.32.135.180
- Th
  a
  t IP belongs to Awareness Technologies who make the software
- That was hard to discover! ;)
- Let's see what else it does...

Realities and Illusions



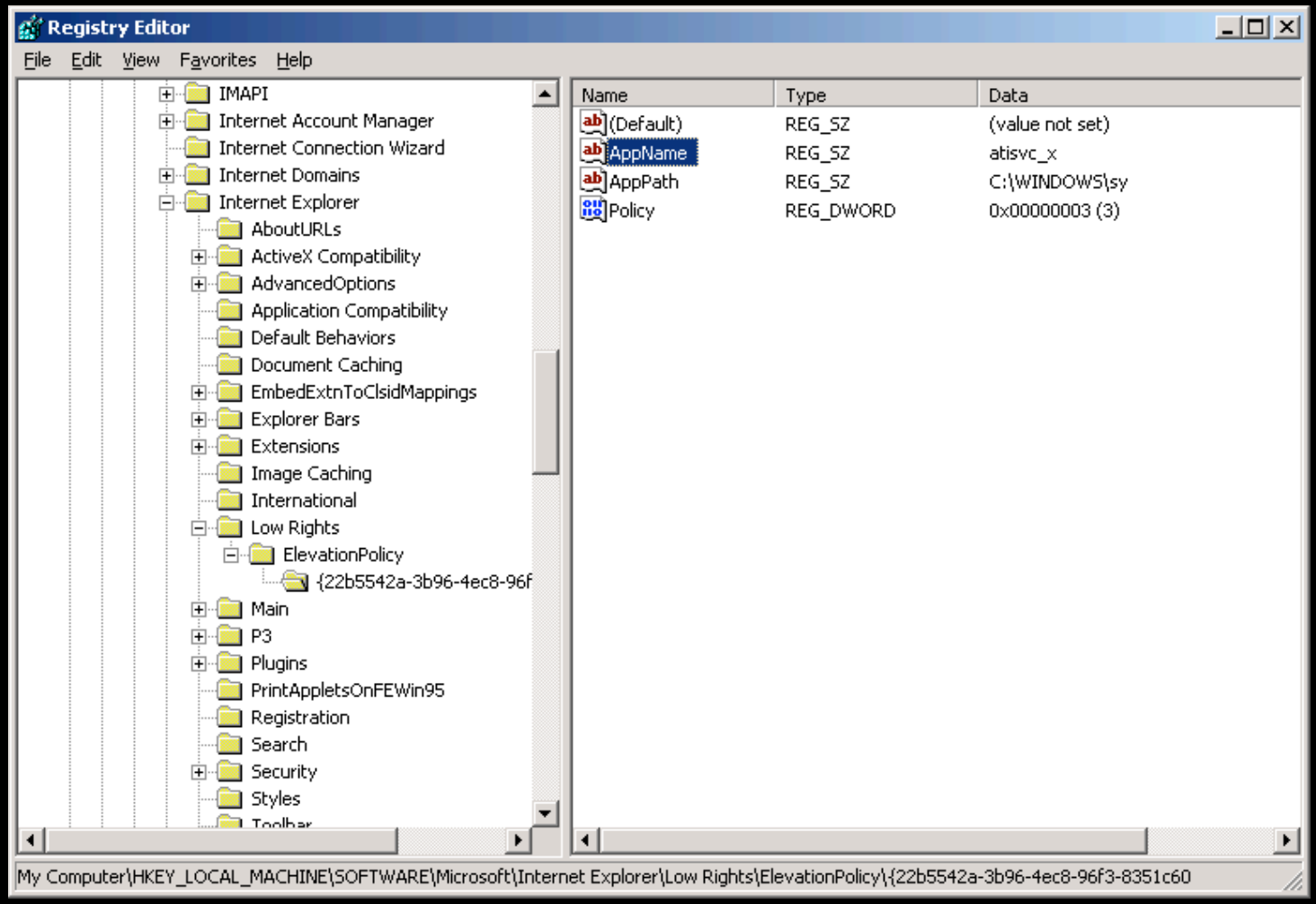
Realities and Illusions

- Required two images – 1 with flat XP SP2 and one with XP SP2 and Integuard installed
- Simple diff grep between the two go some very interesting results...

Realities and Illusions

- The anomalies between the two file sets were immediately noticeable
- Artefacts in the registry and also a 'hidden' directory that contained all sorts of interesting components
- Reg entries were stored in HKEY_LOCAL_MACHINE

Realities and Illusions



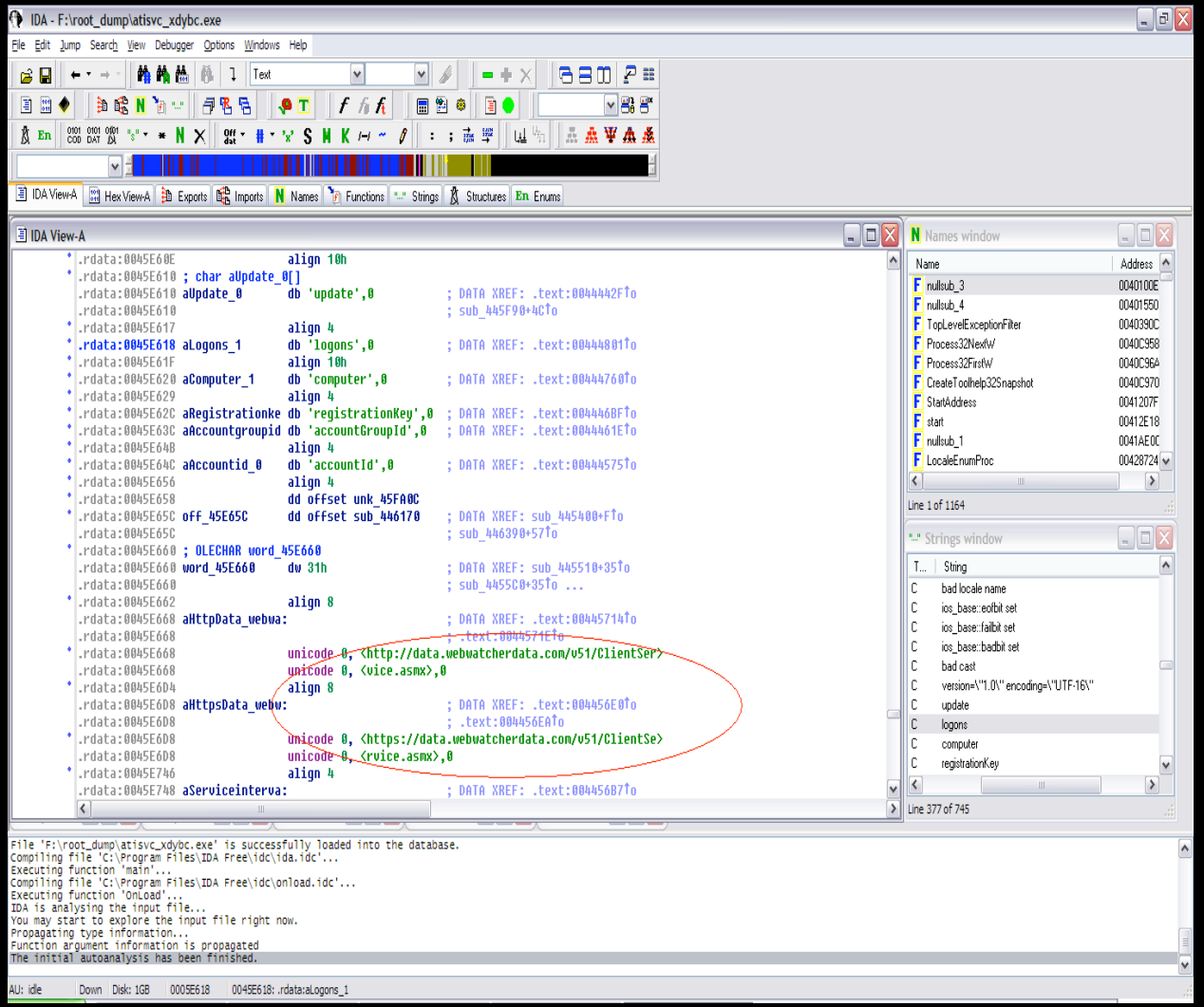
Realities and Illusions

- Why interesting? Well, Sy.exe (AppPath) is used in a LOT of malware (including the small.sy rootkit)
- [illegible] even though it isn't displayed as such (thanks silentrunners)
- Looks to me like a rootkit (and not a great one)
- Definitely not 'invisible'

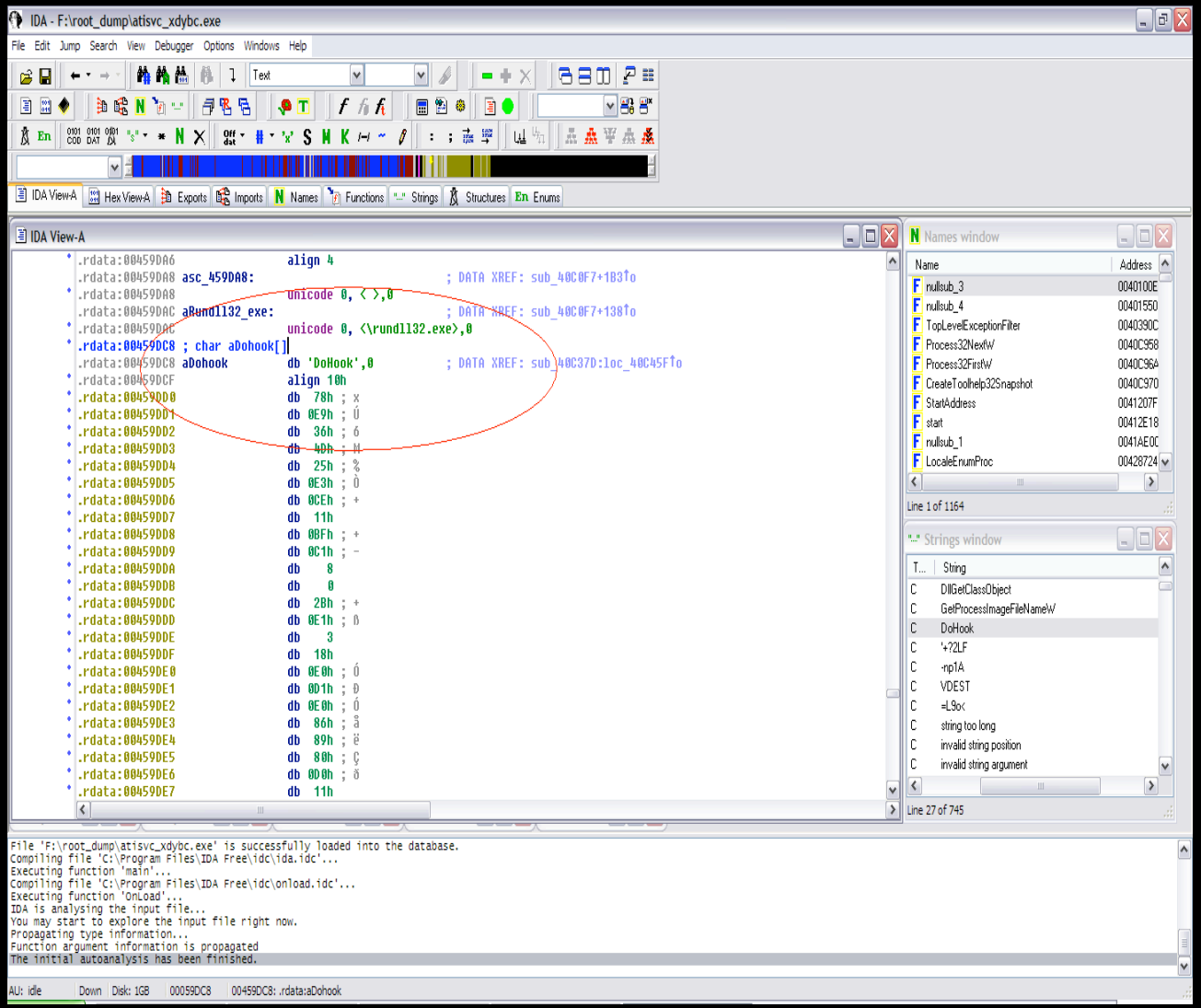
Realities and Illusions

- I am NOT a malware analyst – but thought I'd have a lo
  ok at atisvc_xdybc.exe using IDA Pro Free (www.hexrays.com)
- Interesting results:
  - DllRegisterServer (uses cscui.dll)
  - DoHook (uses rundll32.exe)
  - S
    ource contains links to webwatcherdata.com – Awareness Technologies again
  - Ladies, and gents we have a winner...

Realities and Illusions



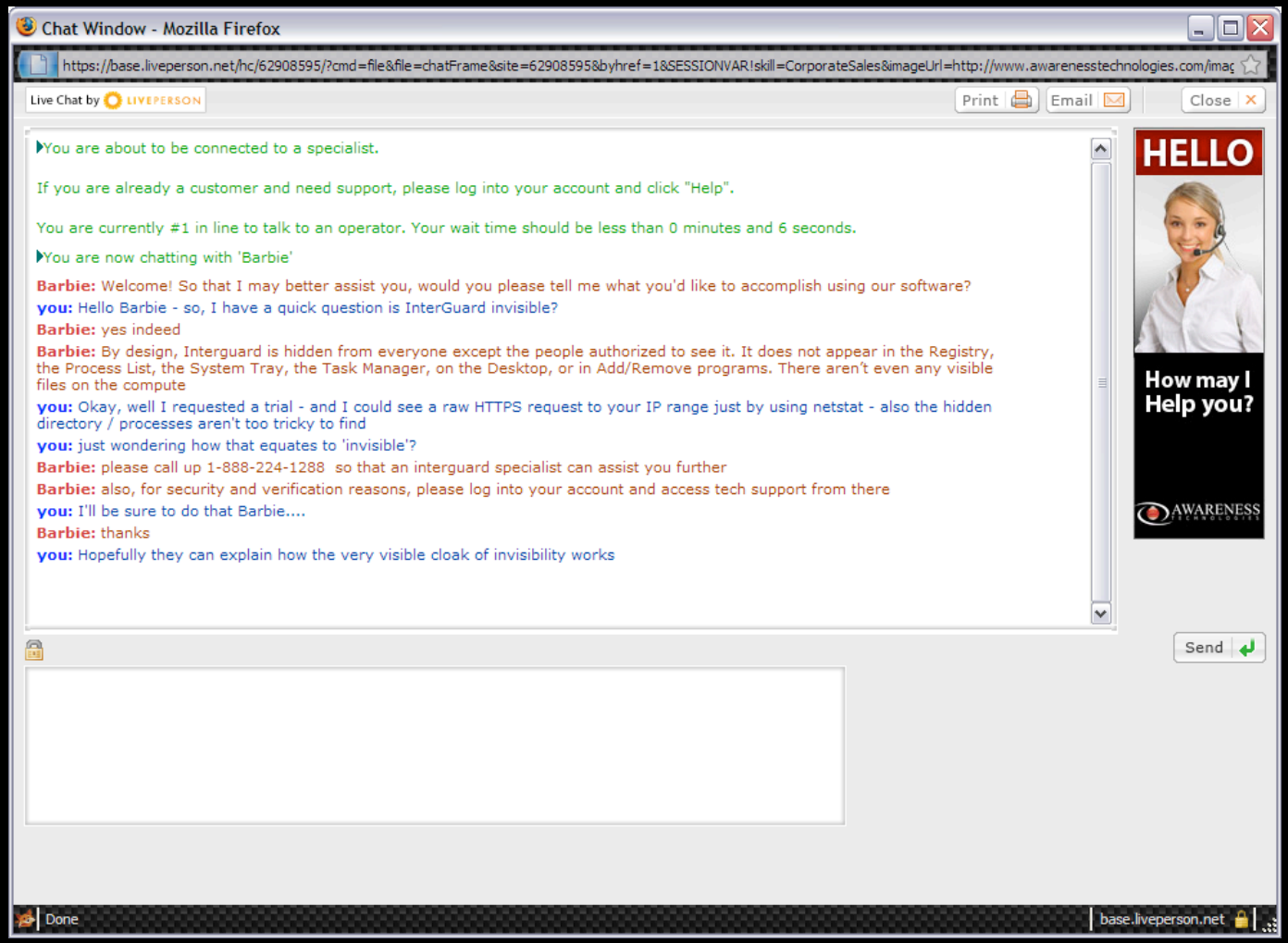
Realities and Illusions



Realities and Illusions

- Why is any of this interesting (other than vendors making very detectable software)?
- Well HackerDefender utilises some of the same dll hooks
- Do you think a 'legitimate' security vendor could possibly just have made a rootkit?
- Because I'm not totally rotten, I thought I'd try to talk to the vendor about this...

Realities and Illusions



Realities and Illusions

- The point here is not to attack particular vendors, but – if it looks like a
  duck, walks like a duck, and talks like a duck – it's a duck
- This software (and others of its cl
  ass) are clearly rootkits (and not particularly subtle ones)
- So what though?

Trusting Trust

Trusting Trust

- DLP tools are being treated as a panacea for all manner of security ills
- They'll help with regulatory compliance, and better yet, stop your organisation getting ripped off
- Maybe, they are introducing more risk than managers may think

Trusting Trust

- How difficult would it be to
  repack
  age one of these applications, and put in your own endpoint?
- Not detected / or ignored by deployed AV and network staff
- The impact isn't too vast on the software analysed, but if you
  can
  monkey with Vontu, and then replace the iteration deployed??
- Stealing data, just
  go
  t a *lot* easier (now comes complete with management buy in)

Trusting Trust

- Many places that maybe shouldn't be are deploying DLP solution without careful analysis
- Why bother with actual hacking any more, just make a rootkit that looks like a legitimate one, and then sit back and wait for data to roll in...

Trusting Trust

- Conclusions (in brief):
  - Vendors lie (shocking eh?)
  - Test your solution (how does it *actually* work?)
  - Question why you need it (if you don't trust your staff, why not?)
  - Make sure you don't trust the communications channels in use
  - Solutions are rootkits – and you may not be able to control data flows!
  - How much damage can an attacker do if they have a play with your deployed solution?
  - Wouldn't it be terrible if someone analysed and published results of how current DLP solutions worked, so people could check if they were being spied on? ;)

Questions?

- Questions?
- Comments?
- Abuse?

Thanks...

- Thanks to you for listening to my ramblings
- The vendors for giving me something to ramble about
- Enno and crew for the con
- MF for the patience
- TS for the assist

Kontakt

- www.clappymonkey.com
- clappymonkey@gmail.com
- Carrier pigeon

- PS: Mike is looking for a job – you should hire him