My Life As A Spyware Developer

Why I’m Probably Going to Hell
Who Am I

• Integrated Solutions Lead for Matrikon Toronto/Chicago
  – Custom software for Power Plants
  – NERC CIP for the past year or so

• Previously developed Pharmacy systems, online casinos, dating websites
  – And spyware
Who Was I?

• Just a programmer with no security/spyware background whatsoever
• Was broke
• Found the job on Craigslist
• Hired as Product Designer\Lead Developer for a spyware company
• 5 other programmers
• Please don’t punch me
Features

• Client Application
  – Run any application we wanted
  – Add links, icons, shortcuts
  – Change homepage search provider
  – Keyword search popups and hyperlinking
  – Check for updates daily

• Server
  – Track installs and updates
  – Manage Multiple Campaigns
  – Upload new versions
Polymorphic Installs

• Random filenames and locations
• Random file contents to get by hash checks
• While I worked there, no malware protection software was able to remove it
• Had started looking into hiding the files in Alternate Data Streams
Affiliate Hijacking

• Abusing affiliate site referrals
• If you went to a site in our list, you got redirected through our affiliate link
• We would get commission off anything purchased
• Hundreds of affiliates
Kernel Module

• Probably called a root kit now
• Hide all the files from the user
• If they were deleted, they would be immediately replaced and randomized once more
Technology Used

• Client Side
  – Internet Explorer Plugin (Browser Helper Object hooks)
  – Visual C++ 6

• Server Side
  – PHP Interface
  – MySQL
How Does This Get Installed?

• My boss said he would pay $10k to whoever found
  • Exploits IE Flaw
  • Our exploit required two things
    – Get the file on the computer and out of protected IE zones
    – Run the file
  • I found one that was able to do this using a custom .chm
    file and exploit in Windows Media Player
    – Was unpatched until XP SP2
• Not Illegal
  – However, we covered our backs with a custom installation dialog
• My boss never paid the $10k
Installation

- Standard IE 6 Installer
Installation

- Custom installer
- Bypasses standard install method
- Legal disclaimer not needed, but just in case
- Tricky to not install
How Did We Deploy The Installer

• Put the exploit in banner ads
• Websites don’t know what ads they run
• And we didn’t know which sites we ran on
• Run the ‘campaign’ for a while and then open the IFrame with the exploit
• Only display to a configurable fraction of viewers
• Keep track of IP addresses and don’t show the IFrame twice to the same person
What Happens When You Install 20 Pieces of Spyware at Once

• Some will install the .NET framework
• Your computer will never be slower
• They try to uninstall each other
  – Including installing AV
How Spyware Makes Money

• Guess how much money our spyware made?
  – Not a dime
• My boss made a lot of money
• How?
  – Installing other peoples spyware
• You can make ~10 cents an install
• My boss would package as much spyware as he could get paid for (around 20 different packages)
• We had over 12 million installs
Want To Be A Millionaire?

• You can!
• The technical part is easy. All the work is making sure the other spyware companies pay you
• My boss was convinced no laws were broken
• All you need is no conscience!
How Did It All End?

• Much like all the internet companies I worked for, they stopped paying me
• Found out the company was founded at an AA meeting
• Went on to work for the person who was paying my boss
• Quit after working 80 hours a week for a few months
• Likes to be able to sleep at night
• This period on my resume is listed as contract work
Questions

• Any?