Inside the Malware Industry
Agenda

• Do the presentation
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 malware
Why Am I Here?

- Never seen anyone talk about the subject from the inside
- Thought it was interesting
- So that you don’t do what I did
Who Was I?

• It was 2004 and I was just a programmer with no security/malware background whatsoever
• Was broke
• Found the job on Craigslist
• Hired as Lead Developer for a malware company
• 5 other programmers
History

• He was being paid by someone else to run this business
• Had tried previously with a group of outsourced developers from India
• Said the time difference was too much and they had some kind of falling out
  – The falling out turned out to be that he didn’t pay them, so he didn’t get the source code
• Hence, us
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

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

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

• Server Side
  – PHP Interface
  – MySQL

• Hosted on Russian servers guaranteed to never take down content
How Does This Get Installed?

- My boss said he would pay $10k to whoever found a way to remotely install our software
- 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
• Don’t try on incompatible browsers
• Keep track of IP addresses and don’t show the IFrame twice to the same person
How Malware Makes Money

• We had over 12 million installs, guess how much money our malware made?
  – Not a dime
    • Affiliate programs know what to watch out for
      – But also don’t do much about it
• My boss made a lot of money
• How?
  – Installing other peoples malware
• You can make ~10 cents an install
• My boss would package as much malware as he could get paid for (around 20 different packages)
  – Companies apparently only paid for ~60% of installs
What Happens When You Install 20 Pieces of Malware at Once

- Some will install the .NET framework
- Your computer will never be slower
- They try to uninstall each other
  - Including installing AV
Want To Be A Millionaire?

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

• Much like all the other internet companies I’ve 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
Other Scams

• Trying to throw search engine results
• Had their own search engines with paid top results
• News video popups
What can be done about malware

• As long as there is money to be made, someone will try
  – Or even if they just think they can
  – Or even if they think they can make money off people who think they can

• Blacklisting is a fools errand
  – Whitelisting is the future (or should be)
    • Guess you can’t make money if you can’t sell virus signature updates
What Did I Learn

• Creating malware is not hard
• You can easily make a lot of money on the internet
• AV/Malware protection seems almost useless
• This kind of software is not going away
• It’s not worth compromising your ethics for money
Questions

• Any?
Contact

garry.pejski@gmail.com