Information Security Threat Vectors

Phil Withers, CISSP, CRISC
Who is this guy?

- 26 Year veteran of Naval Communications
  - Networks, Satellite, Terrestrial
- Project Manager Navy Global DMS HD
  - Requirements Analysis, Design, Installation, Operation, Hardening, Reporting, IAVM, ISSO
- CISSP/CRISC
A Threat Vector is a path or a tool that a Threat Actor uses to attack the target.

Threat targets are anything of value to the Threat Actor. It can be a PC, PDA, Ipad, Your online bank account... or you (stealing your identity)
Threat Vector Types

- Web – Fake sites, Session Hijacking
- Wireless Unsecured Hotspots (Bubba)
- Email – Links, Attachments
- Mobile Devices: Iphone/Ipad/Ithis/Ithat
- Social Networking – Facebook, et al
- Social Engineering (including POTS)
- Malware
- USB (removable) media
What is a “Threat Actor”? 

- **Human (80/20 rule)**
  - Malicious
    - External – Script Kiddies, Crackers, Competitors, Organized Crime, Foreign Governments/Entities
    - Internal – Disgruntled Employee, The Curious
  - Ignorant
    - George the WonderDummy
    - The George Scale

- **System – Misconfigurations**
  - Automated privilege elevations
The Help Desk “George Scale”

0 – Alan Turing
1 – Tim Berners-Lee, Grace Hopper
2 – Linus Torvalds
3 – Sysadmins, clueful developers, QA people
4 – Your average MCSE bootcamp graduate
5 – Your average corporate end user
6 – Your average AOL user
7 – Furry woodland creatures
8 – Algae
9 – A bag of hammers
10 – George
US-CERT lists:
- National Governments (Israel?)
- Terrorists (cyber or otherwise)
- Industrial Spies (France?)
- Organized Crime
- “Hacktivists” (Wikileaks)
- Hackers

Threat Actors possess a motive and seize upon an opportunity
Threat Actors exploit vulnerabilities
What do Threat Actors Want?

• Bragging Rights
• Financial Gain
• Competitive Advantage
• Military Dominance
• Political Advantage
• Economic Advantage
• A New World Order
• Anarchy
Who do They Target?

- IRAN – Stuxnet Boomerang! (HBGary)
- China – DOD/Financial
- North Korea – Anything
- “Anonymous” – Gov. Walker
- Banks – World Bank, Citigroup
- Stores – TJ MAX CC Database
- Your PC – Botnets
- Your online banking credentials
• Edu-ma-cation!
  ◦ Ongoing IA Awareness Program
• Honeytokens
• Defense in Depth (Layers)
• Defense in Breadth (Synergy)
• Framework Built on Industry Standards and Best Practices
• AntiVirus, Firewalls, IDS, IPS, Blackholes
• GRC! (not Governance, Risk and Compliance)
Your Personal Computer
Gibson Research Corp.
- Free!
- Shields Up! (Pentester)
- Free!
- “Perfect Passwords” – 63 Character Pseudo-Random Generator (one time) for your Wireless Access Point
- Free!
- http://www.grc.com
• There’s no place like LOCALHOST
• Free!
• Managed Host File Insert
• Free!
• Blocks Ads, Banners, 3rd Party Cookies, 3rd Party Page Counters, Web Bugs, and even most hijackers

**127.0.0.1 Is Your Friend**

**Countermeasures**
# This MVPS HOSTS file is a free download from:
# http://www.mvps.org/winhelp2002/
# 
# Notes: The Operating System does not read the "#" symbol.
# You can create your own notes, after the # symbol.
# This "must" be the first line: 127.0.0.1 localhost
# 
# Entries with comments are all searchable via Google.
# 
# Disclaimer: This file is free to use for personal use only. Furthermore it is NOT permitted to copy any of the contents or host on any other site without permission or meeting the full criteria of the below license terms.
# 
# This work is licensed under the Creative Commons Attribution-NonCommercial-ShareAlike License.
# http://creativecommons.org/licenses/by-nc-sa/3.0/

127.0.0.1 localhost

#start of lines added by WinHelp2002
# [Misc A - Z]
127.0.0.1 fr.e2ftp.net
127.0.0.1 m.fr.e2ftp.net
127.0.0.1 ad.e2ftp.net
127.0.0.1 asy.e2ftp.net
127.0.0.1 abostats.com
127.0.0.1 a.abv.bg
127.0.0.1 adserver.abv.bg
127.0.0.1 adv.abv.bg
127.0.0.1 bing.abv.bg
127.0.0.1 news.abv.bg
127.0.0.1 www2.a-counter.kiev.ua
127.0.0.1 track.acclamnetwork.com
127.0.0.1 anonserveradsystem.com

Done
Let’s Use Facebook as an Example
DoD Recommended Facebook Privacy Settings

<table>
<thead>
<tr>
<th>Category</th>
<th>Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Posts by me</td>
<td>Friends Only</td>
</tr>
<tr>
<td>Family</td>
<td>Friends Only</td>
</tr>
<tr>
<td>Relationships</td>
<td>Friends Only</td>
</tr>
<tr>
<td>Interested in</td>
<td>Only Me</td>
</tr>
<tr>
<td>Bio and favorite quotations</td>
<td>Friends Only</td>
</tr>
<tr>
<td>Website</td>
<td>Friends Only</td>
</tr>
<tr>
<td>Religious and political views</td>
<td>Only Me</td>
</tr>
<tr>
<td>Birthday</td>
<td>Friends Only</td>
</tr>
<tr>
<td>Places I check in to</td>
<td>Friends Only</td>
</tr>
</tbody>
</table>

Include me in “People Here Now” after I check in
Visible to friends and people checked in nearby (See an example)

Enable

Edit privacy settings for existing photo albums and videos.
DoD Recommended Facebook Settings

DISABLED!
DoD Recommended Facebook Settings

Countermeasures
Accessible through friends!!

*Turn it off*

Countermeasures
• A complete description and rationale for changing the security settings on your FB page can be found at:

http://slideshare.net/USNavySocialMedia/recommended-facebook-privacy-settings-august-2010
• Threats, Vectors, and Actors are a fact of life
• Know your opponent – get smart
• Reduce your online profile and exposure
• Security through Obscurity
Thanks for Listening!

Questions?