Antivirus is NOT Dead
Extending Infosec to Deal with Advanced Persistent Threats

The information contained in these materials is provided for informational purposes only, and is provided AS IS without warranty of any kind, express or implied. Social Exploits shall not be responsible for any damages arising out of the use of, or otherwise related to, these materials.

Social Exploits, the Social Exploits logo, and other Social Exploits products and services are trademarks of Social Exploits LLC, in the United States, other countries or both. Other company, product, or service names may be trademarks or service marks of others.

© Copyright Social Exploits LLC 2014. All rights reserved.
The AV is Dead Challenge

• If you think AV is dead...
  – Try turning it off for 1 month
  – Across the entire enterprise (desktops, servers, etc.)
• Merriam-Webster defines “dead” as
  1) lacking power or effect
  2) no longer having interest, relevance, or significance
• So it shouldn’t matter if it’s turned off... right? 😊
• *I take no responsibility if you actually do this*

The antivirus is dead challenge stemmed from personal communication with Dr. Eric Cole (personal communication, May 2012).

The definition for the word dead is from (Merriam-Webster.com, 08/13/2014).
“Anti-Virus Is Dead” Is a Metaphor

Translates to... (FUD) | Reality (Un-FUD)
--- | ---
- I’m trying to sell you a new product | - How will it augment to reduce risk?
- I’m a parrot | - Education is key
- AV is old technology | - Old threats still exist
- EPS replaces AV | - EPS incorporates AV
- AV won’t stop targeted attacks | - AV isn’t designed to stop targeted attacks

Saying AV is dead because it doesn’t stop targeted attacks is like saying MS word is worthless because it sucks as an HTML editor (it does)
Metaphors + FUD != Solution

- Targeted attacks are a different class
- Street thief vs. foreign intelligence service (FIS)
- “Traditional” solutions aren’t effective
  - Neither are metaphors and FUD
- Street thief
  - Gate
  - Guard dog
  - Alarm system
  - Safe
- FIS
  - Hop the gate
  - Distract/neutralize the dog
  - Steal the alarm code
  - Crack the safe
New Perspectives

• APTs are basically (state sponsored) targeted attacks
  – Specific entity instead of general victim
  – Goals are strategic advantage

• Differences from traditional threats
  – Targeting
  – Methodology
  – Timeframe
  – Persistence
  – Blending

• Similar TT, different P (ops)
Corporate Counterintelligence

- Look to how others have dealt with similar situations
  - Intelligence communities suffer targeted attacks by foreign nation states
  - Counterintelligence is their solution
- Protection from
  - Penetration by a foreign adversary
  - Leakage of sensitive information
  - Foreign espionage, subversion, sabotage, etc.
- Businesses can apply many of the same concepts
  - Combine with existing defense in depth concepts
  - Legal limitations

The definition of counterintelligence is from (Prunckun, 2012).
Defense-in-Depth

• Use several security measures
  – Similar to backups, or multiple locks

• Components
  – Prevent: protecting against attacks
  – Deter: denying attempted attacks
  – Detect: identifying past, present, and future attacks
  – Respond: handling attacks
How DiD Is Commonly Done

Proactive
Prevention + Deterrence  Detection

wait for attack

Reactive
Response

isolated components

all or nothing

linear flow
The model shown on the slide is derived from (Prunckun, 2012).
Guiding Principles

• Systems-centric view
  – Every activity is important
  – Each affect the other
  – Nonlinear environment
  – Whole appears > sum of parts
• Plan to be attacked and compromised
• Focus on *people* and *processes*
  – Not just technology
  – Predictive instead of proactive/reactive

The bullet point on being predictive is from (Cole, 2012).
Through The Lens of Risk

Risk \(\propto\) Vulnerability

Prevention

Deterrence
Detection
Deception
Neutralization

Probability of harm is proportional to Opportunity to cause harm and Agents of harm

© Copyright 2014 Social Exploits LLC
## Prevention & Deterrence

### Prevention
- Multiple layers
  - Firewall, IDS/IPS, HIPS, Antivirus, secure coding, change control, etc.
- Yes it won’t stop everything
  - But something is better than nothing
  - Nor does money buy happiness
  - But it *can* help 😊

### Deterrence
- Psychological methods
  - Publicity / PR
  - Doxing
  - Currently not much options
- Denying operations
  - Response and “active” response
  - Integrate findings with other activities in real time

The discussion on deterrence is based upon (Prunckun, 2012).
Detection

**Defensive**

- Traditional mechanisms
  - Firewalls, IDS, antivirus, etc.
- Important to have broad coverage
  - Application, host, internal network, gateway, people *and* public
- Look for
  - Comm. and control
  - Non-traditional sources

**Offensive**

- This doesn’t *have* to cross legal boundaries
  - Forums
  - IRC channels
- Largely focused on attribution
  - Metasploit-laden docs
  - Web bugs
  - Custom “malware”
## Deception & Neutralization

### Deception
- Intentionally misleading to other actions
- Examples
  - Honeypots
    - Leads into detection and neutralization
  - Code names, stego
  - Joining attacker communities
- Cost-intensive

### Neutralization
- Preemptive and responsive forms
- Two components
  - Hooking
  - Paralysis
- Examples
  - Honeytokens
  - ADHD
  - Taking down domains, botnets
    - With legal permission
Legality Of Offensive Activities

- Title 18 §1030 forbids hacking others
  - Even if they are attacking you
  - You can defend your networks
- Booby traps are also illegal
  - Are you attacking them, or are they accepting a risk?
  - Use warning labels (at a bare minimum)
- **CONSULT YOUR LEGAL COUNSEL**

The material discussing booby traps is based on (Strand & Asadoorian, 2011).
Implementation Challenges

- It’s not “free”
  - Requires additional effort (== cost)
- Defenders need to be cross-trained
- Legal considerations
  - The line can become blurry very quickly
  - Especially with neutralization
  - No concept of “cyber self-defense”
- Much of this is still in its infancy
Conclusion

- Antivirus is *not* dead
  - Using metaphors and FUD as solutions *is*
- APT is a different class of attacker
  - Traditional threats still exist
  - Must defend against both
- Focus on both opportunities and agents to cause harm
- Legal statutes don’t help
  - But that doesn’t mean they can hold you down
  - You do however need to know where the line is
This section is reserved for any questions and comments from the audience.
References

- Referenced works can be found in the notes page below


