



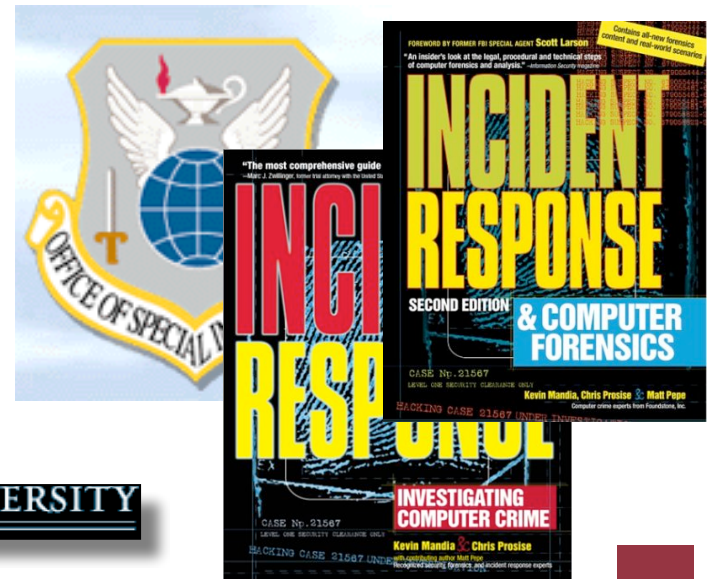
Agile Incident Response: Operating through Ongoing Confrontation

Kevin Mandia



Who Am I?

- Professorial Lecturer
 - Carnegie Mellon University
 - 95-856 Incident Response
 - Master of Information System Management
 - The George Washington University
 - Computer Forensics III
 - Masters in Forensic Science
- Author for McGraw-Hill
- Honeynet Project



Who Am I?

- Last 3 Years
 - Responded to over 300 Potentially Compromised Systems.
 - Responded to Intrusions at Over 40 Organizations.
 - Created IR Programs at Several Fortune 500 Firms.



Agenda

- Incident Detection
- Case Studies
- Performing Agile Incident Response
- Operating through a Constant Aggressor





How Are Organizations Detecting Computer Security Incidents?



1. How are Organization's Detecting Incidents?

■ Antivirus Alerts?

- Perhaps, but do not Count on It...
- Alerts are Often Ignored – and Perhaps Value-less without an In-Depth Review of the System.
- Quarantined Files Often Remain a Mystery



Anti-Virus Merely Alerts an Organization that
Something Bad Might have Occurred. No
Confirmation. Potential Loss of Critical Data

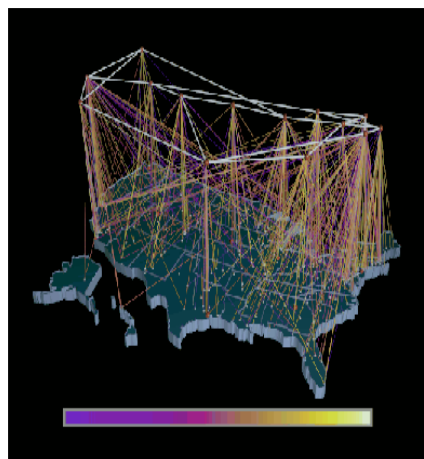
Findings – Ongoing Intrusion

- The Review of 10 Malicious Executable Files Yielded:
 - 12/12 Files were NOT Publicly Available
 - 12/12 Files were NOT Detected by AV
 - 11/12 Files Reviewed were Packed via 2(5) Different Methods

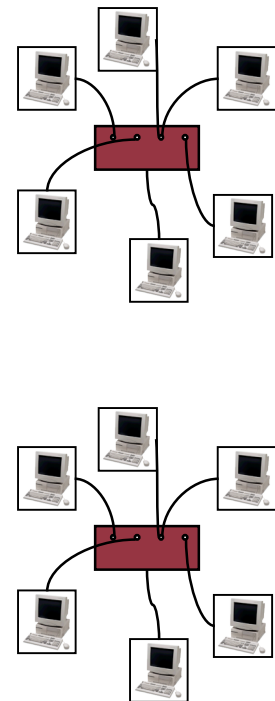
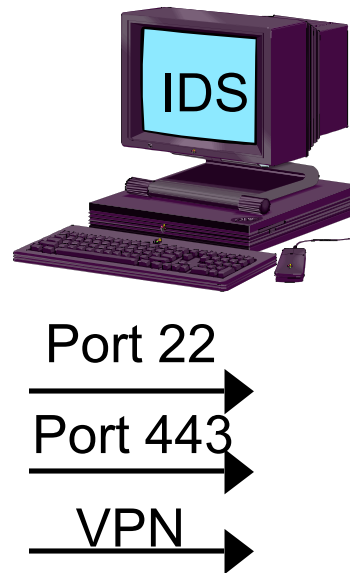
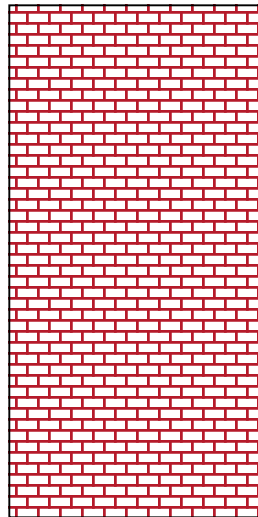
It is Highly Unlikely AV will ever Trigger on Microsoft Tools or Sysinternal Tools.

2. How are Organization's Detecting Incidents?

- IDS Alerts?
 - Rare Detection Mechanism.



Port 22
Port 443
VPN



3. How are Organization's Detecting Incidents?

6

▪ Clients (Outside Company)

- More Often than Pro-Active Countermeasures.
- Malicious Software Discovered on Compromised End-User Systems.
- Recently (December 2005) Found a Keylogger Configuration File that Contained Approximately 1,157 Keyword Search Terms, and URL's for Approximately 74 Online Banking Facilities.

4. How are Organization's Detecting Incidents?

28

▪ End Users (Internal)

- System Crashes (Blue Screens of Death)
- Continual Termination of Antivirus Software.
- Installing New Applications Simply Does Not Work.
- Commonly Used Applications Do Not Run.
- You Cannot "Save As".
- Task Manager Closes Immediately When You Execute It.



5. How Are Organization's Detecting Incidents?

- Something Obvious ...





6. How are Organizations Detecting Incidents?

- Notification from other Victims.
- Notification from Government Agencies.

2



Case Studies

The State of the Hack

The State of the Hack

- End User Attacks
 - Phishing
 - Spam / Rogue Attachments*
- Web Application Compromises
 - Custom App Vulnerabilities
- Valid Credentials
 - VPN Access
 - PSEXEC*

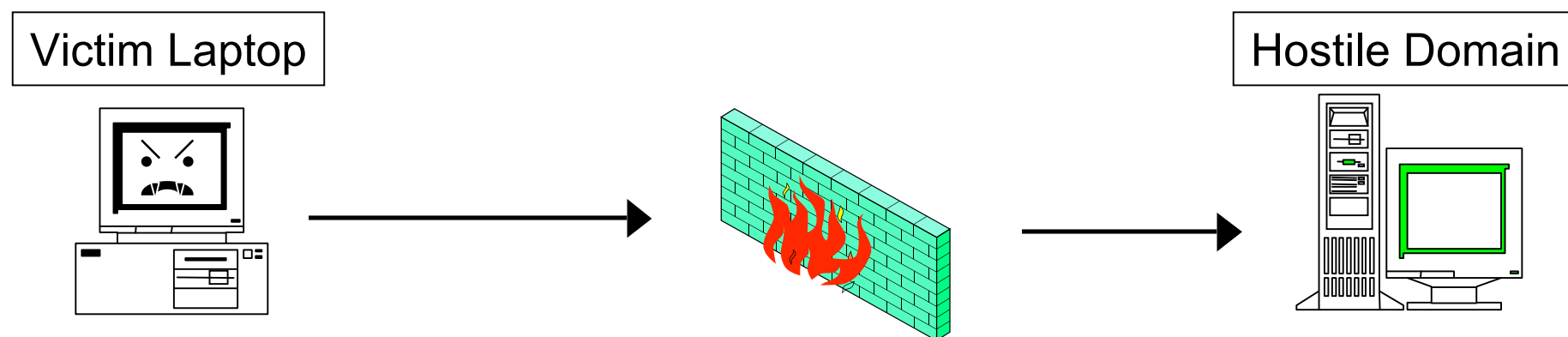




Case Study – Targeted Spamming

Incident Detected

- A Network Intrusion Detection System Observed Traffic Outbound to a Hostile / Uncommon Domain
- Traced IP Address Internally to a Laptop



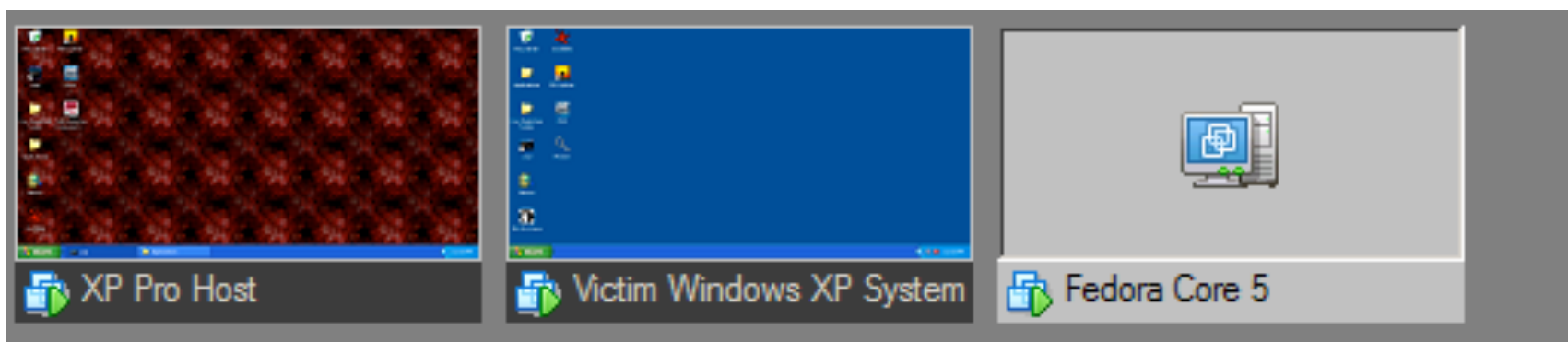


Demonstration



Demo 1

- Victim Receives “Innocuous Email”
 - Command Shell Backdoor sent to Drop Site



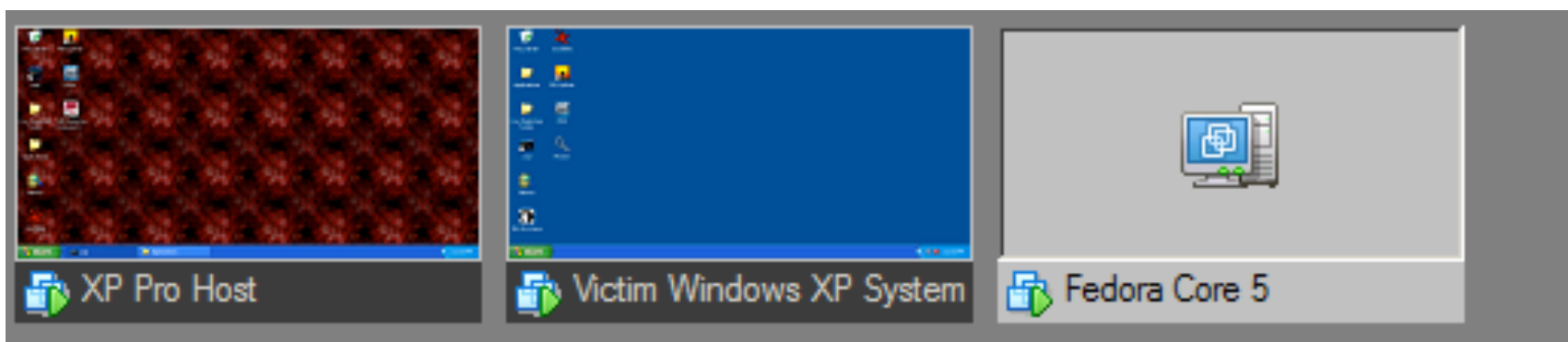
Attacker
66.92.146.247

Victim
66.92.146.248

Drop Site
66.92.146.1

Demo 2

- Victim Receives “Innocuous Email”
 - “Server” Sends Connection to Attacker



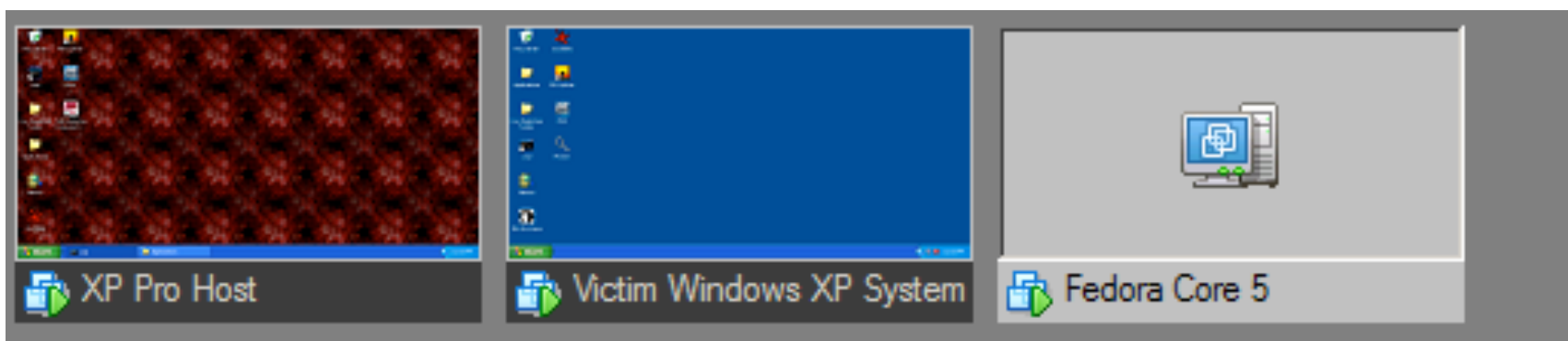
Attacker
66.92.146.247

Victim
66.92.146.248

Drop Site
66.92.146.1

Demo 3

- Attacker Uses Valid Credentials and PSEXEC to Connect and Launch Evil Code on Victim System



Attacker
66.92.146.247

Victim
66.92.146.248

Drop Site
66.92.146.1



Practicing Agile Incident Response

Practicing Agile Incident Response

- Agile Incident Response Requires
 - Understanding the Corporate/Organization Priorities
 - Rapid Data Collection Capability
 - Rapid Data Analysis
 - Focused Response:
 - Identify Host-Based Countermeasures
 - Identify Network-Based Countermeasures
 - Rapid/Concise Documentation



1. Understanding Corporate/Organization Priorities

Understanding Corporate Priorities

- Executive Concerns
- Legal Concerns
- Technical Concerns



Technical

Business

Compliance



Management Concerns (Board and CEO)

- What is the Incident's Impact on Business?
- Do We have to Notify our Clients?
- Do We have to Notify our Regulators?
- Do We have to Notify our Stock Holders?
- What is Everyone Else Doing about this Sort of thing?



Legal Counsel Concerns

- What are the applicable regulations or statutes that impact our organization's response to the security breach?
- Are there any contractual obligations that impact our incident response strategy?
- Are we required to notify our clients, consumers, or employees about the security breach?
- What constitutes a “reasonable belief” that protected information was compromised – the standard used in many states to determine whether notification is required?

Legal Counsel Concerns

- How might public knowledge of the compromise impact the organization?
- What is our liability if the compromised network hosted pirated software, music, or videos?
- Does notifying our customers increase the likelihood of a lawsuit?
- Is it permissible to monitor/intercept the intruder's activities?
- How far can/should we go to identify the intruder?
- Should the organization notify our regulators?
Law enforcement?



Technical Management (CIO)

- How long were we exposed?
- How many systems were affected?
- What data, if any, was compromised (i.e., viewed, downloaded, or copied)?
- Was any Personal Identifiable Information (PII) compromised?
- What countermeasures are we taking?



Technical Management (CIO)

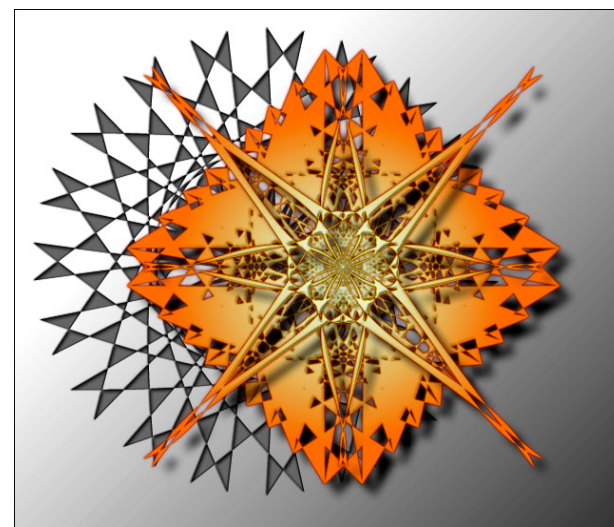
- What are the chances that our countermeasures will succeed?
- Who else knows about the security breach?
- Is the incident ongoing? Preventable?
- Is there a risk of insider involvement?



2. Rapid Data Collection

Performing Live Response

- Cost-Effective Manner to Collect Information
- Collecting Information that is Lost When a Machine is Powered Off
- Collecting Windows/Unix Artifacts that Assist in the Investigation



Volatile Data

- The System Date and Time
- Current Network Connections
- Which Programs are Opening Network Connections (Listening)
- Users Currently Logged On
- Running Processes
- Running Services
- Memory Space of Active Processes
- Scheduled Jobs
- RAM



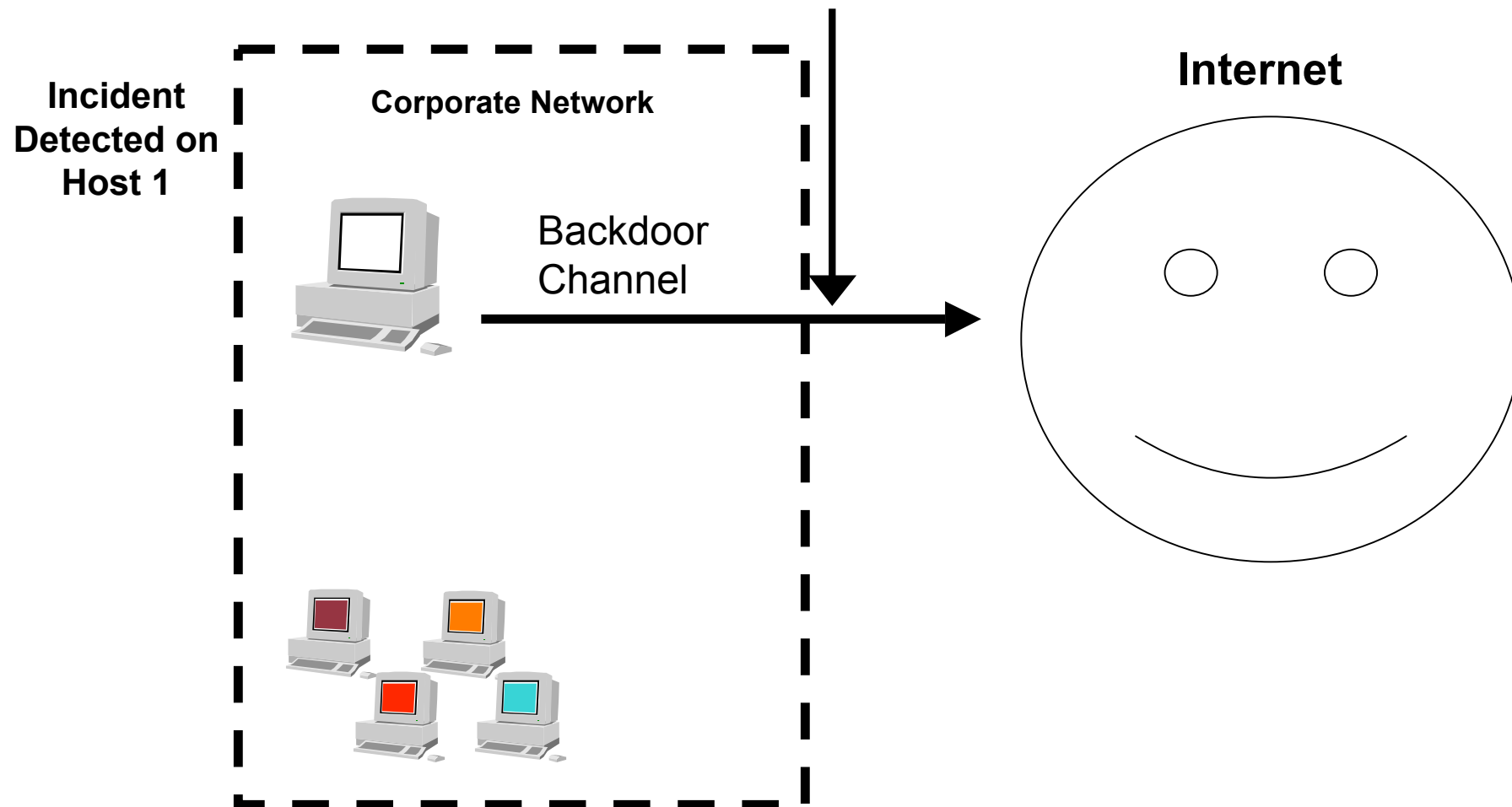
Windows Artifacts Collected from Live Systems

- File Lists
- The Windows Registry
- The Windows Event Logs
- Specific/Relevant Files
- The System Patch Level
- Certain Proprietary Log Files



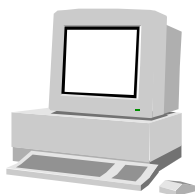
Incident is Detected

Network Monitoring



Performing Live Response

**Incident
Detected on
Host 1**



**Respond
on Host 1**

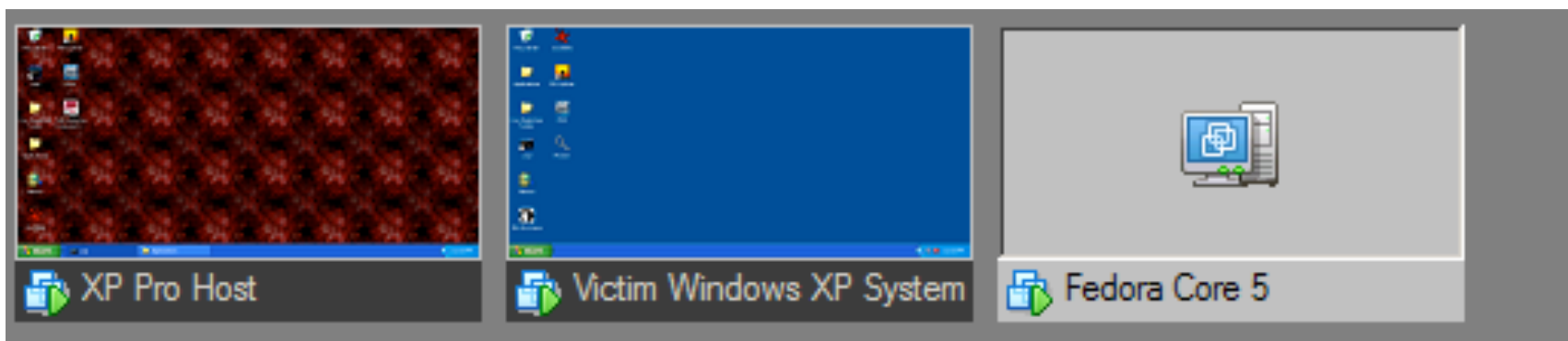
1. **Last Accessed Time of Files**
2. **Last Written Time of Files**
3. **Creation Time of Files**
4. **Volatile Information**
5. **Services Running**
6. **Event Logs**
7. **Registry Entries**
8. **Host Status (Uptime, Patch Level)**
9. **IIS and Other Application Logs**



**Live Data Collection
Performed to Verify
Incident and Determine
Indicators / Signature of
the Attack**

Demo 4

- Live Response



Attacker
66.92.146.247

Victim
66.92.146.248

Drop Site
66.92.146.1



3. Rapid Data Analysis

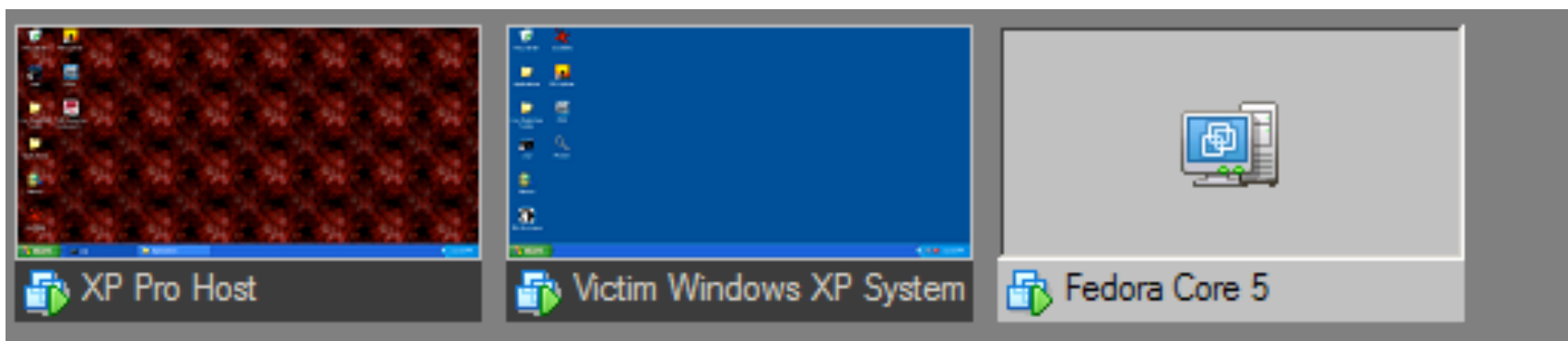
Case 2 - Initial Detection

- Victim Organization Targeted - Ongoing Computer Intrusion
- Victim Organization Tweaked Proxy Server Logs to Review all Outbound Connects to Hostile Domains
- Caught a Bleep on the Radar from a Host
- Performs a Remote Live Response Using First Response



Demo 5

- Rapid Analysis



Attacker
66.92.146.247

Victim
66.92.146.248

Drop Site
66.92.146.1



4. Focus: Countermeasures/Documentation

Focus

- Focus = Defined and Established
 - Goals
 - Roles
 - Expectations
 - Speed
 - Communication
 - Documentation



Know Your Goals

II. Verify Project Scope and Approach

Goals of the Incident Response Effort

- 1. Accomplish Accurate Case Diagnosis**
 - a. Determine the full extent of the compromise.
 - b. Determine if the incident is ongoing.
 - c. Determine how the network was compromised.
 - d. Determine if sensitive data has been compromised.
- 2. Identify Business Objectives and Priorities.**
- 3. Determine Appropriate Countermeasures**
 - a. Identify, Document, and Provide Host-Based Countermeasures to prevent further compromise.
 - b. Identify, Document, and Provide Network-Based Countermeasures to prevent further compromise.
 - c. Provide procedural guidance to ensure a “move fast, move with purpose” response posture.
- 4. Assist in Developing Appropriate Remediation Steps**
 - a. Documentation
 - b. Coordination
- 5. Audit Any Remediation to Verify Effectiveness.**
- 6. Ensure Knowledge Transfer of Tools, Techniques, and Investigative Conclusions**
 - a. Posture Organization to respond to future incidents in a most effective manner.
 - b. Provide information as needed to appropriate personnel.
- 7. Adhere to Appropriate Evidence Handling Procedures.**

All efforts can be prioritized and conducted in parallel.

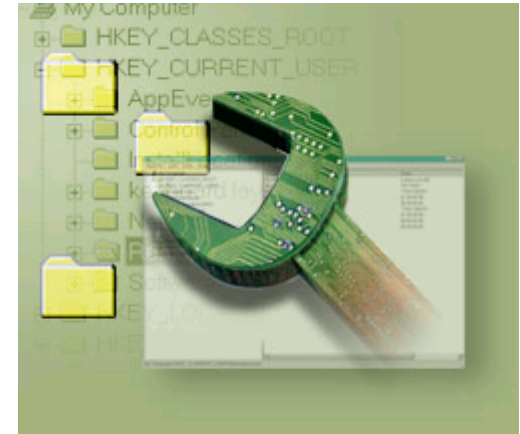
Know Roles

- Data Collection
- Data Analysis
- Malware Analysis
- Network Traffic Analysis
- Host-Based Detection
- Documentation



Speed

- Incident Response – Fast and Steady
- Fast Enough to Get Reliable Answers
- Fast Enough to Provide Simple but Adequate Documentation
- We Strongly Dissuade Briefing Anything that has not been Written.



Documentation

- Establish Champions Responsible for the Necessary Documents:
 - Status Reports
 - Live Response Investigative Steps
 - Hot IPs
 - Host-Based Indicators of Compromise
 - Network-Based Indicators of Compromise
 - Remedial Steps

3. Initiate "Straw Man" Documentation

- Document forensic review methods.
- Document indicators of compromise.
- Begin formal forensic report.
- Begin documentation of appropriate countermeasures.
 - Network-Based Remediation.
 - Host-Based Remediation.
 - Document Procedural Countermeasures.



Operating through an Attack

Operating through an Attack

-  Obtain High-Level Direction
-  Know your Remediation Philosophy
-  Identify the “Zone” You Are In
-  Determine Remediation Plan
-  Determine Readiness
-  Execute



1. Obtaining High-Level Direction

- The Most Difficult and Confusing Aspect of Remediation Planning
- Impacts All Aspects of your Remediation Plan
 - What is Your Leadership's Tolerance of the Status Quo?
 - How Good Does Your Incident Response Need to Be?
 - How Much are You Willing to Spend?
 - What is the Risk?
 - Do you have to Tell Shareholders?
 - Do you have to tell Clients?



2. Know your Remediation Philosophy

- Battle Plan
 - Aggressive Remediation
 - Moderate Remediation
 - No Execution of Remediation

Aggressive Remediation

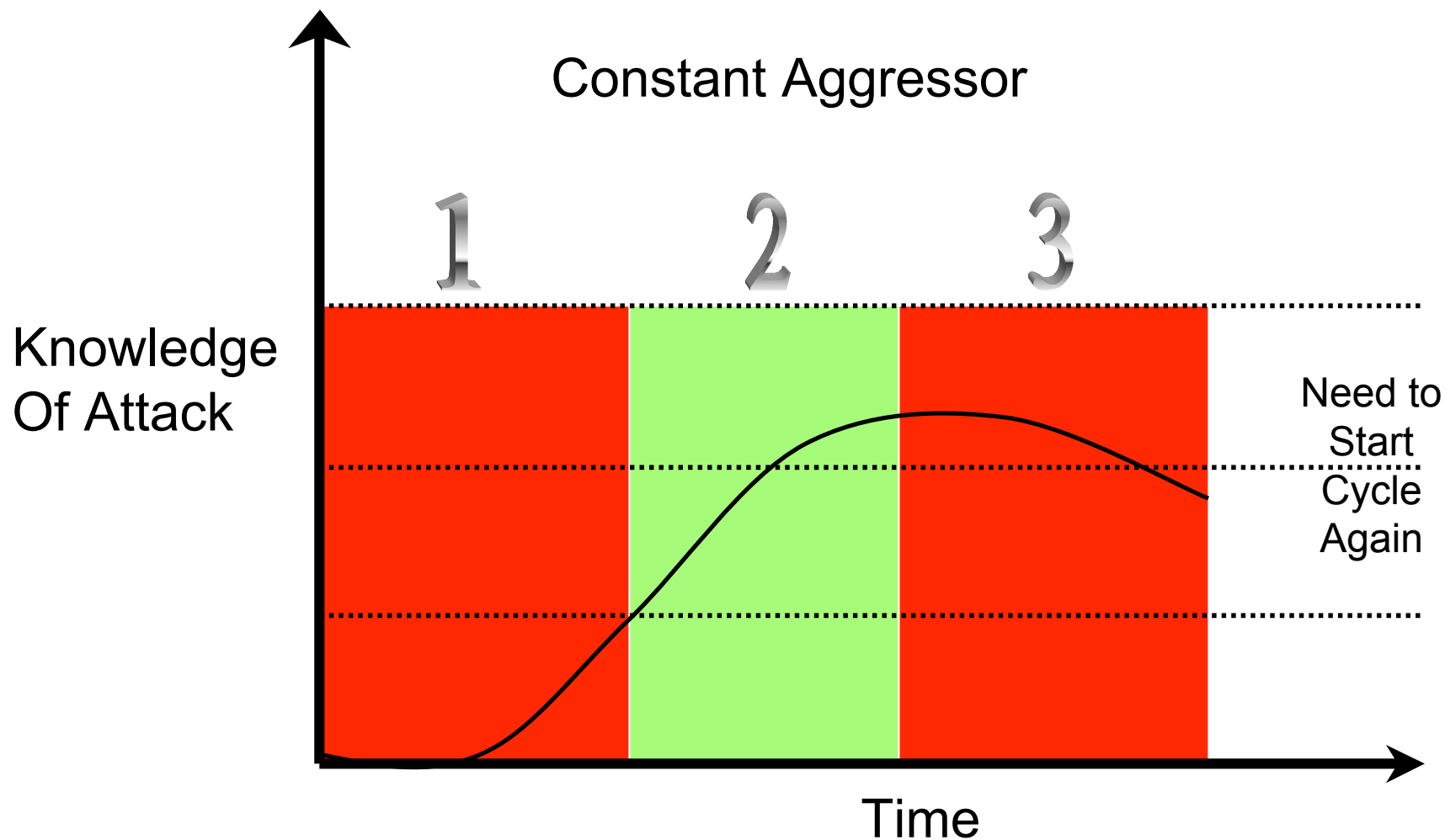
- IR Roles and Responsibilities Are Clearly Defined
- Team Capability Exists
 - Host Based Detection / Countermeasures
 - Network Based Detection / Countermeasures
- Remediation is
 - Planned
 - Coordinated
 - Organization-Wide
 - Executed in Strike Zone
 - Clear Cut Status (Where You Are)
- Ongoing Remedial Activities are DELIBERATE



Moderate Remediation

- IR Roles and Responsibilities are Ad Hoc
- Moderate Team Capability To Execute:
 - Host Based Detection / Countermeasures
 - Network Based Detection / Countermeasures
- Remediation
 - Executed in Bursts
 - Not Coordinated Well Among Seperate Business Units
 - Different BLs Have Different Posture
 - Current Status Sometimes Confusing
- Few Significant Remedial Efforts
- Reliance on Small, DISPARATE Efforts.

3. Determine the Zone you are In



Zone 1 Symptoms

- Host Based Indicators are Unknown
- Network Based Indicators are Unknown or Transaction Based
- New Compromised Hosts are Still Being Detected at a High Rate (more than 1 per day)
- There Seems to be No Established Pattern to Assist your Organization in Anticipating the Next Compromised Host
- There is Little Coordination between Business Lines (Staff) Concerning Remediation

Remediation will Likely FAIL!

Zone 2 – “Strike Zone”

- Host Based Indicators are Stable
- Network Based Indicators are Stable
- The Delta to Detect New Compromised Hosts is Shrinking Consistently
- Your Organization can Anticipate which Systems may be Compromised Next
- Your Organization is Postured to Actively Anticipate and Address the “Next Generation” of Attacks
- There is Active Communication and Coordination between Business Lines (Staff) Concerning Remediation

Zone 3 Symptoms

-  Host Based Indicators are Becoming Less Reliable
-  Network Based Indicators are Becoming Less Reliable
-  No New Compromises have been Detected
-  Staff Motivation and Concern has Waned Considerably
-  Remedial Activities have Evolved from Corporate-Wide Efforts to Independent “Splinter Cells”



Remediation
will Likely
FAIL!

How Do You Miss Strike Zone?

📁📌 Assets Impacted are Too Important

📄📌 Analysis Paralysis / Indecision

- Too Much Consider of 'What if'

📄📌 Lack of High-Level Buy-In

- Remediation and Business Objectives Diverge

📄📌 Too Much Consensus Building

📄📌 Common Goal Not Established or Understood

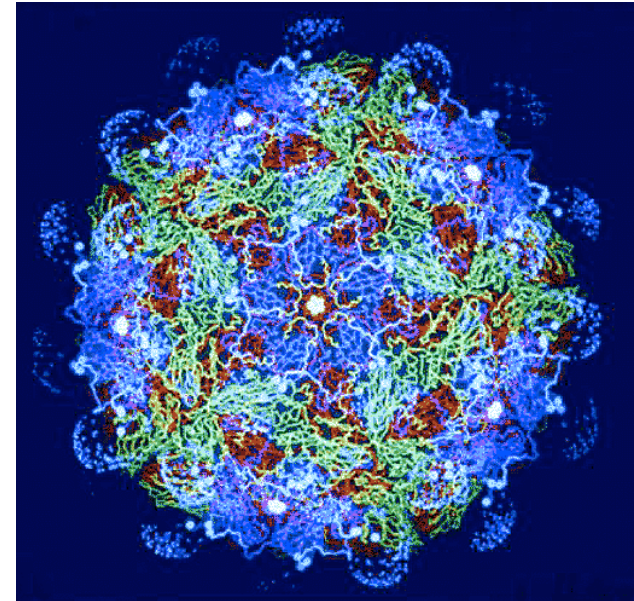
🕒📌 Remediation Not Feasible

- Lack of Resources



4. Assess Your Remediation Plan

- Criteria:
 - Documented
 - Coordinated
 - Feasible
- Can it be Implemented?
 - Appropriate Skills
 - Appropriate Coordination
- Can it Meet Organization's Objectives?



5. Assess your Readiness

 Do you have a Move Fast, Think Fast Diagnosis Team?

 Can They Collect the Data the Need Fast Enough?

 Can you Deploy Rapid Network-Based Countermeasures for

- Incident Detection?
- Incident Prevention?

 Can you Deploy Rapid Host-Based Countermeasures for

- Incident Detection?
- Incident Prevention?

5. Assess your Readiness

- Have you Coordinated Amongst the Appropriate Service Lines?
- Have you Documented the Remediation Plan?
- If the Aggressor “ups the ante”, will your Improvement for Next Iteration of Attacks be Fast Enough?



Questions?