Computer Virus Response Using Autonomous Agent Technology

Changing the Paradigm

Christine M. Trently
crently@mitretek.org
Outline

0 Brief Perspective on Computer Virus Response
0 Overview of Autonomous Agent Technology
0 Agents for Computer Virus Response
0 Example Using Agents for Virus Response
0 Comparison - Current versus Future
0 Future Considerations
0 Conclusions
Brief Perspective - Computer Virus Response

- Viruses?
- Current Response
- Trends
- Need for Change
- Automated Response
Autonomous Agent (AA) Technology

0 Agent Characteristics

- Simple, singular task

- Mobile

- Intelligence - Reasoning

- Cooperation

0 Operating Environment
Autonomous Agent (AA) Technology (concluded)

- Agent Coordination Engine (ACE)
  - Launch
  - Authenticate
  - Repair
  - Communicate

Agent Programs

Agent Coordination Engine

Operating System

Communication Protocol
The Agents of Virus Response

- Detect Virus
- Identify Virus
- Capture Sample
- Remove Virus
- Make Report
- Compile Report

External activities

[Diagram showing the process flow]
Responding to Boot Sector Virus Using Agents

0 Detect
- Trigger: Insertion of diskette
- Activity: Check for boot sector virus on diskette
- Notification: Virus found message sent to ACE

0 Identify
- Trigger: ACE
- Activity: Identify virus detected or Verify (virus) signature from detection
- Notification: Virus identification to ACE

0 Sample
- Trigger: ACE
- Activity: Make copy of Boot sector / disk image
- Notification: Virus sample sent to repository and completion status sent to ACE
Response for Boot Sector Virus Using Agents (concluded)

0 Recovery
- Trigger: ACE
- Activity: Remove virus from boot sector using appropriate technique
- Notification: Completion status to ACE

0 Report
- Trigger: ACE
- Activity: Generate incident report
- Notification: 1) Report sent to administrator;
2) Report sent to repository
3) Completion status to ACE
Virus Response - Comparison
Current vs. Future

<table>
<thead>
<tr>
<th>Current (User Activity)</th>
<th>Future (Agent Activity)</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Scan computer periodically</td>
<td>- Activity on computer is checked by agents</td>
</tr>
<tr>
<td>- Notified by AVS that BS virus detected</td>
<td>- BS virus found on diskette inserted into computer</td>
</tr>
<tr>
<td>- Boot from known clean, write-protected diskette</td>
<td>- Virus identified, if applicable</td>
</tr>
<tr>
<td>- Take a sample by inserting new diskette</td>
<td>- Sample taken</td>
</tr>
<tr>
<td>- Use Recovery diskette or Run Clean-Up routine for given</td>
<td>- Virus removed</td>
</tr>
<tr>
<td>virus to remove virus</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Report generated and administrator notified</td>
</tr>
<tr>
<td>- Re-scan</td>
<td></td>
</tr>
<tr>
<td>- Return to Work</td>
<td></td>
</tr>
</tbody>
</table>
Future Considerations and Conclusions

- Reduce Processing Overhead
- Prevent Misuse
- Maintain Agent Integrity
- Identify Target Response
- Provide Identification and Recovery Techniques

-------------------------------------------

Changing the Paradigm
- Providing a loaded gun

I’ve got what?!?