>THIS IS **THE WAY**

The Inspector

Automating the forensic investigation of infected computers

Presented by: John Morris and Eric Kedrosky

Oct 2006

>THIS IS NORTEL

The Inspector Agenda

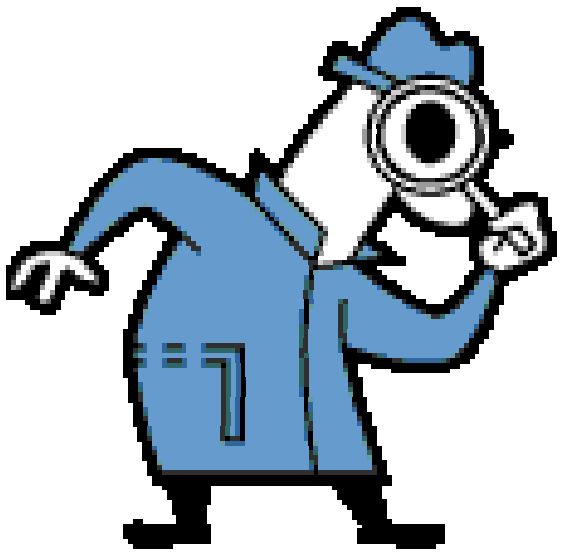
- An overview of the inspector and the reason it was created.
- What functions the inspector performs
- What have been the benefits
- Questions & Comments ….

The Inspector Non-Agenda

> Inspector, the greatest forensic tool ever created

> Inspector, now available in the lobby at special conference pricing ….

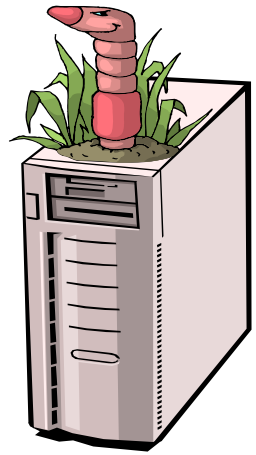
What is Inspector

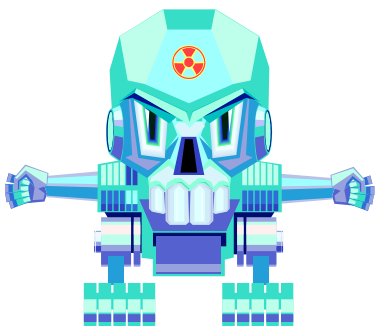


> A tool used to remotely examine machines that are suspected of being infected.
  - Gathers useful information about the computer
  - Conducts a high level vulnerability assessment
  - Identifies “Malware Candidates” and gathers samples of them
  - Gathers additional directory listings and logs which may be needed for further analysis

The Problem – Changing threatscape

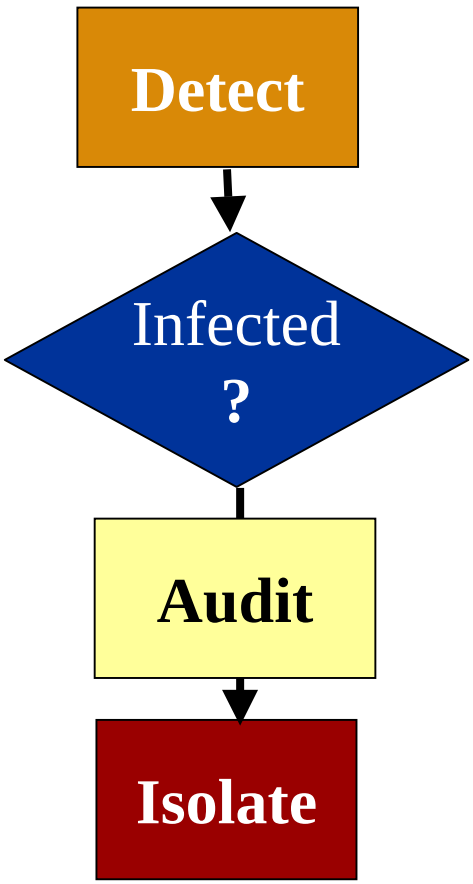
> Prior to 2004, we were primarily fighting network worms
  - Examples: Blaster, Code Red, Funlove
  - Descrete software components - behaved in a predictable fashion
  - New worms typically resulted in large, network outbreaks followed by small “After shocks”.





> Starting in 2004, we started to experience “Bots” on our corporate network
  - Took us several months before we fully understood that the threat had changed
  - Now seeing smaller, regionalized outbreaks
  - No longer descrete software components - Human controlled and thus unpredictable
  - Bots used a “Swiss Army Knife” approach to gaining access to systems.

Reaction to Change



> We were very good at:

- Rapidly detecting infected systems on the network.
- Rapidly neutralizing the threat

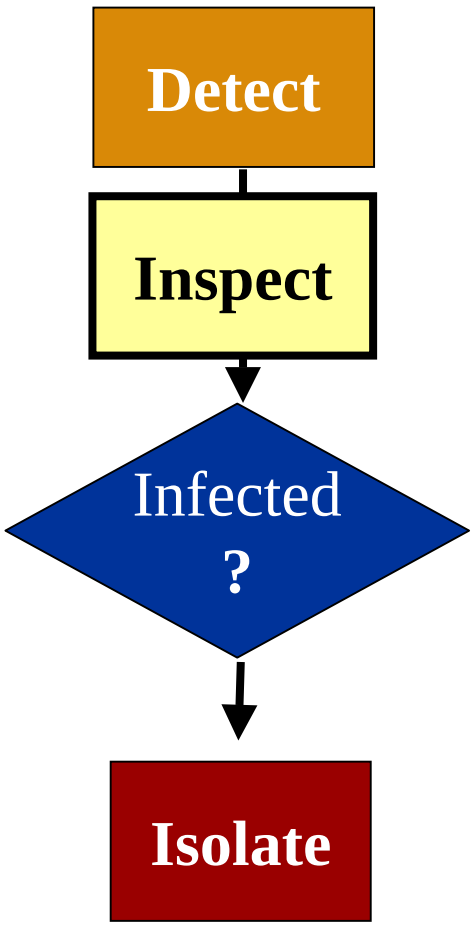
> What we needed to improve:

- Identifying the specific malware involved in the outbreak.
- Finding Typhoid Mary
- Identifying the vulnerabilities being exploited.

> Work around: Audit computers

- Problem: physically accessing remote computers
- Problem: network audits delayed Isolation
- Problem: manual audits were time consuming and conducted in a spotty fashion.

Automating Forensic Analysis



Key Goals

> Take advantage of time between detection and isolation.

> Minimize human involvement

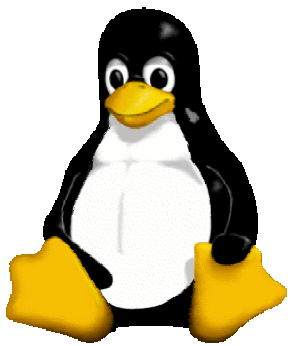
> Speed

> Consistancy

> Collect malware samples

> Keep results for further analysis (metrics, etc)

How was it built?



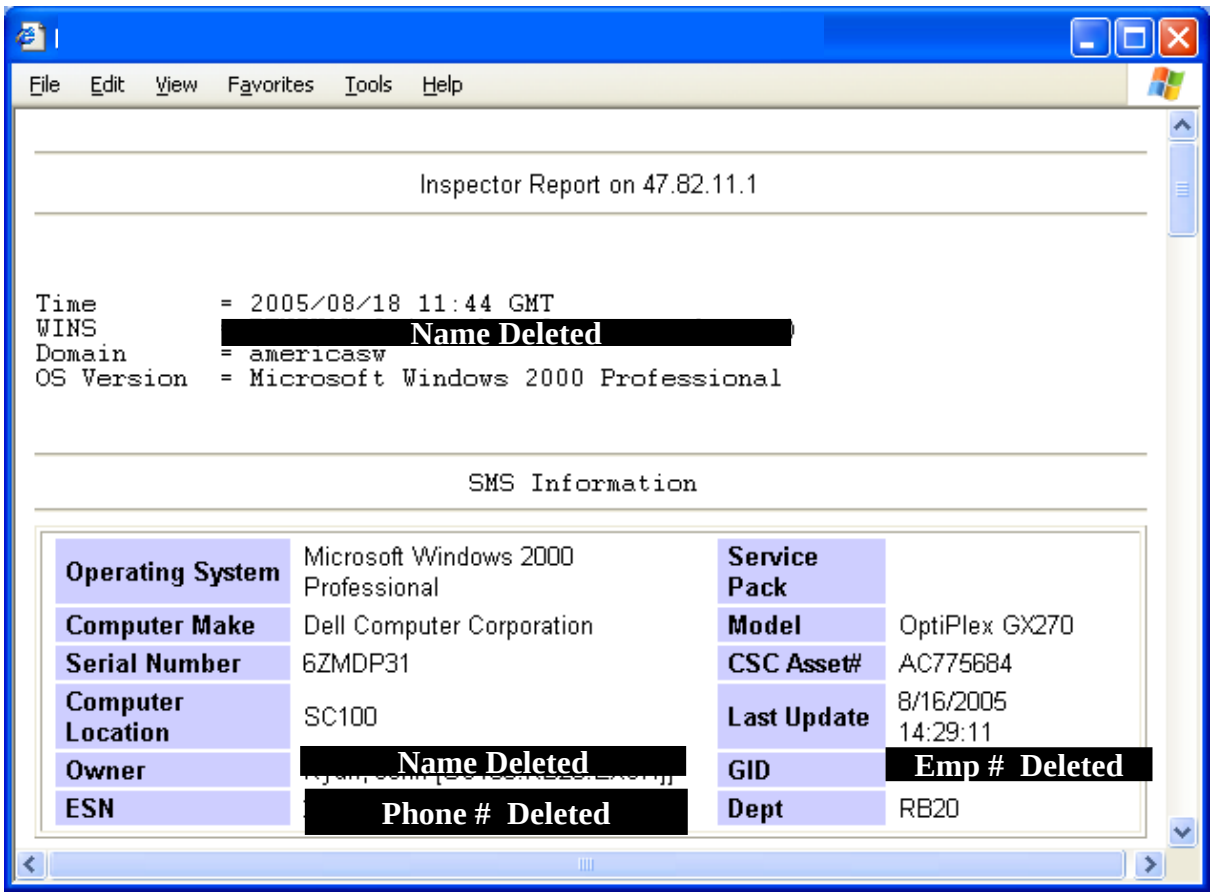
Linux

Perl

samba

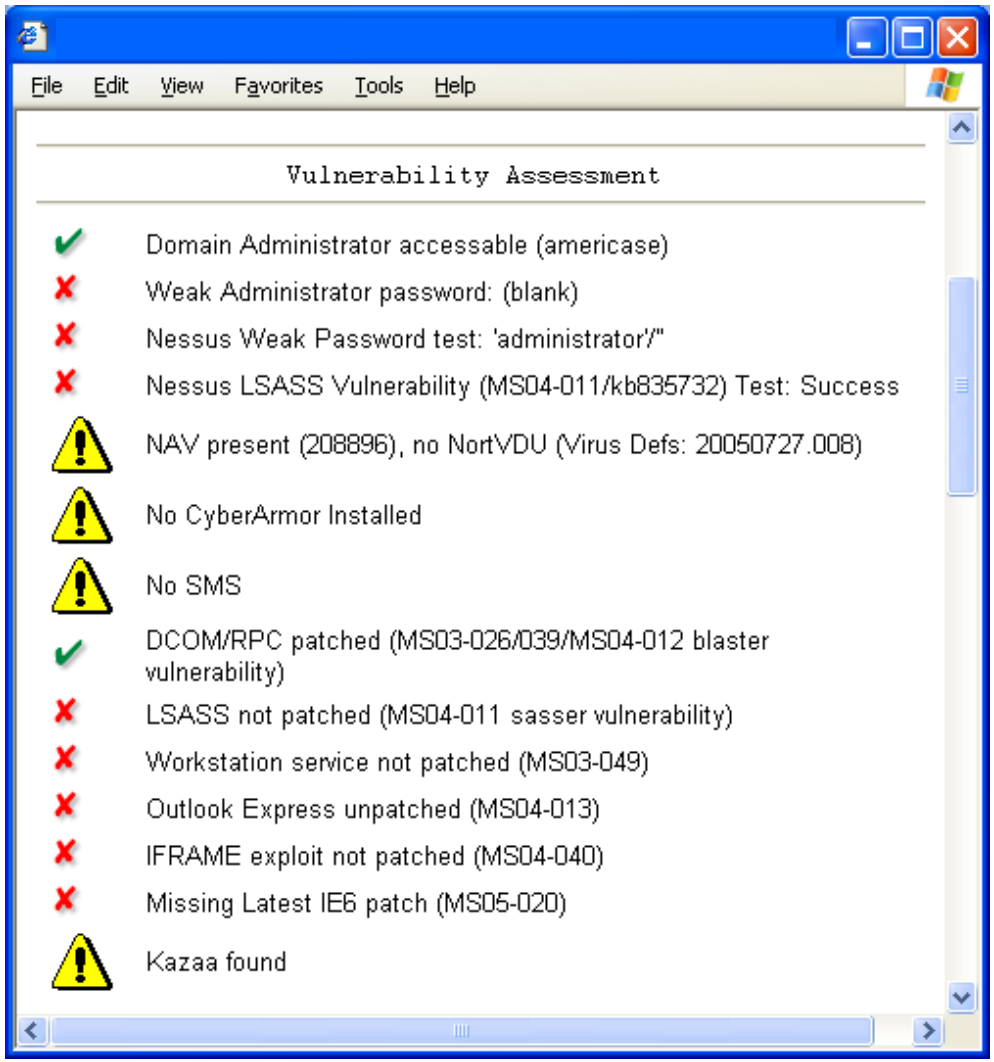
Constructed using Open (“Free”) Technologies

Sample output – System Description



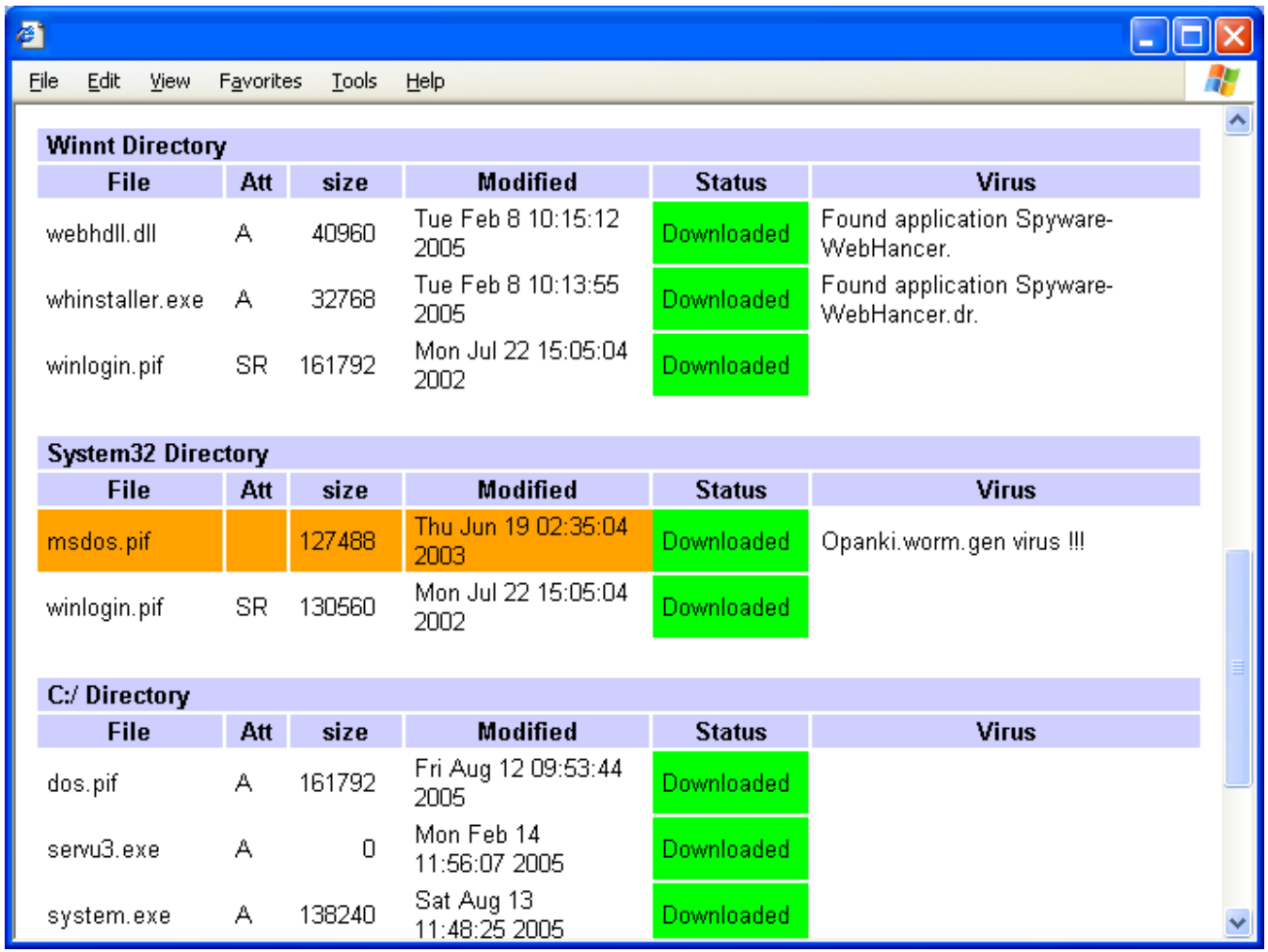
- **Tries to gather identification information from the computer**
- **Consults IT databases to gather further useful information about the computer.**
- **Even if the computer is not found in the IT database, that fact is an important clue!**

Sample Output – Vulnerability Assessment



- **Checks for common vulnerabilities exploited by Bots.**
  - **MS06-040**
  - **MS05-039/047**
  - **MS04-012 (MS03-026)**
  - **MS04-011**
  - **Weak Passwords**
  - **Weak DBA passwords.**
- **Checks for vulnerabilities externally, and if possible, internally.**
- **Checks status of computer's defenses.**
- **Checks for presence of non-standard applications which may have aided the spread of Malware.**

Sample output – Virus Candidates



Winnt Directory

File	Att	size	Modified	Status	Virus
webhdll.dll	A	40960	Tue Feb 8 10:15:12 2005	Downloaded	Found application Spyware-WebHancer.
whinstaller.exe	A	32768	Tue Feb 8 10:13:55 2005	Downloaded	Found application Spyware-WebHancer.dr.
winlogin.pif	SR	161792	Mon Jul 22 15:05:04 2002	Downloaded	

System32 Directory

File	Att	size	Modified	Status	Virus
msdos.pif		127488	Thu Jun 19 02:35:04 2003	Downloaded	Opanki.worm.gen virus !!!
winlogin.pif	SR	130560	Mon Jul 22 15:05:04 2002	Downloaded	

C:/ Directory

File	Att	size	Modified	Status	Virus
dos.pif	A	161792	Fri Aug 12 09:53:44 2005	Downloaded	
servu3.exe	A	0	Mon Feb 14 11:56:07 2005	Downloaded	
system.exe	A	138240	Sat Aug 13 11:48:25 2005	Downloaded	

- **Checks common directories for malware files**
- **Ignores common OS & Application files**
- **Looks for some known Malware filenames.**
- **Looks for recently modified files**
- **Looks for “Hidden” files**
- **Downloads samples for further analysis.**

Additional Inspector Actions

> Grabbing list of installed programs

> Grabbing complete file listings from key directories

> Grabbing Anti-virus logs

- Done after sample collection.

Inspection times vary, but usually <5 minutes

The Short-Comings

> Can not tell if a vulnerability existed before infection or resulted from it.

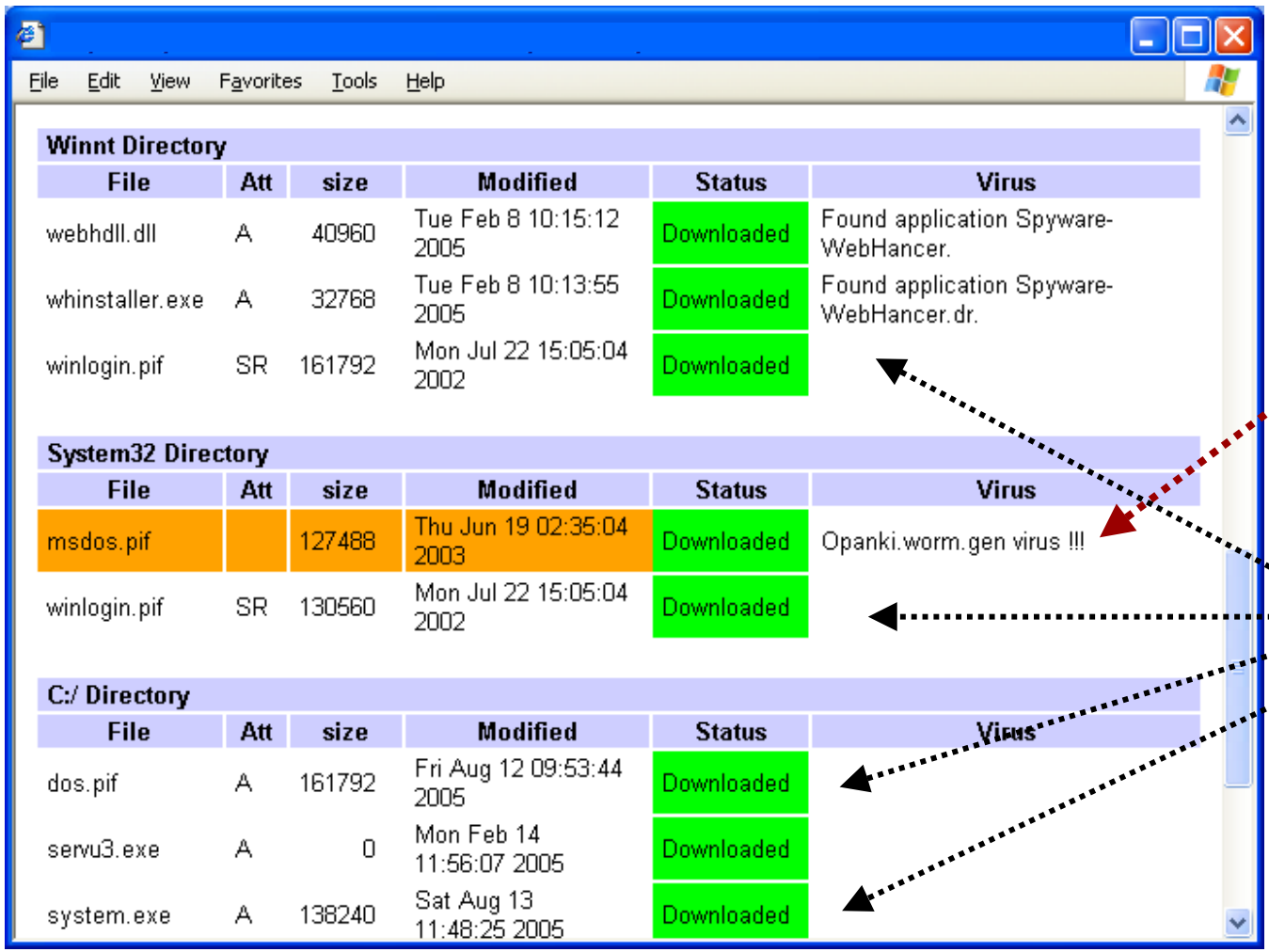
> Full audit can be blocked by Malware's counter-measures.
  - Many bots disable access to administrative shares

> Audit will also be limited if the infected computer is not in domain.
  - Non-corporate computers, etc

> Some Malware infestations force an immediate reboot during infection process, resulting in the system going offline.

Today, Inspector is typically capable of doing full inspections on ~25% of infected computers on our network.

Insight into Bots



File Edit View Favorites Tools Help

Winnt Directory

File	Att	size	Modified	Status	Virus
webhdll.dll	A	40960	Tue Feb 8 10:15:12 2005	Downloaded	Found application Spyware-WebHancer.
whinstaller.exe	A	32768	Tue Feb 8 10:13:55 2005	Downloaded	Found application Spyware-WebHancer.dr.
winlogin.pif	SR	161792	Mon Jul 22 15:05:04 2002	Downloaded	

System32 Directory

File	Att	size	Modified	Status	Virus
msdos.pif		127488	Thu Jun 19 02:35:04 2003	Downloaded	Opanki.worm.gen virus !!!
winlogin.pif	SR	130560	Mon Jul 22 15:05:04 2002	Downloaded	

C:/ Directory

File	Att	size	Modified	Status	Virus
dos.pif	A	161792	Fri Aug 12 09:53:44 2005	Downloaded	
servu3.exe	A	0	Mon Feb 14 11:56:07 2005	Downloaded	
system.exe	A	138240	Sat Aug 13 11:48:25 2005	Downloaded	

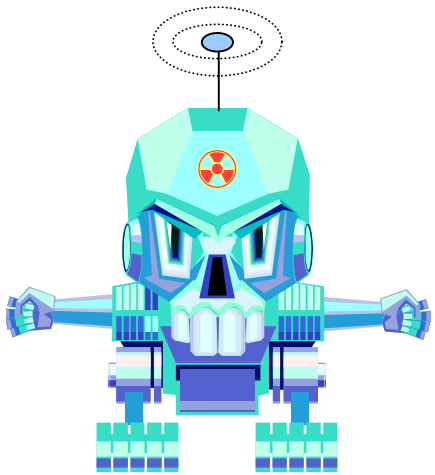
- **AV software was able to detect adware and spyware, as well as a known bot.**

(Aka W32.ALLIM) Bot spread via AIM.

- **But what about the four new bots , varients of Opanki and SDbot (Spybot) found on the same machine?**

What cleanup strategy would you use?

Case Study: Inspector vs Zotob



> August 2005: Zotob (MS05-039 exploiting worm)
  - Whilst the media was focusing on Zotob, using inspector we saw 8 distinct bots (not all Zotob)
  - Some bots were downloading additional software/new versions.
  - Knowing the nature of the outbreak(s) is essential to managing cleanup process.

> During outbreaks, its not uncommon to use ad hoc means of identifying infected systems.
  - Inspector is able to help confirm infections by looking for key infection files.

Benefits of Sample Collection.

> Allows quick delivery to AV vendors

> Facilitates quick identification with tools such as VirusTotal.

> Quick identification speeds research on nature of malware

> Provides samples for testing in our own lab to identify BOT Command and Control servers.

> In the first 18 months of operation, Inspector allowed us to collect an average of 21 new malware samples (undetected by our primary AV vendor) monthly.

- Peak: 66 new malware detections (May 2005).

Why are we using stats from last year?

Inspector and Root Cause Analysis

> Most of our infected systems had one of 8 common vulnerabilities.
  - Inspector helped identify weaknesses in IT processes and procedures
    - Cleanup Processes
    - Patching new computers on the network
  - Continued presence of vulnerabilities has been determined to be an issue with compliance.

> Inspector analysis helped build business case to move from a re-active to pro-active model.
  - Why wait for a worm to find your vulnerable systems?
  - 99% compliance isn't good enough when the other 1% is still a big number.
  - Enforcing security compliance will reduce both the quantity and size of outbreaks.

Conclusion

> Inspector is not worlds greatest forensic tool
  - Simple, speedy
  - Effective - Provided considerable insight into the nature of malware and security process failures in our environment

> Lots of room for improvement
  - Limited to only fully scanning ~25% of infected systems
  - Move from an agent-less to an agent based model (home-grown or commericial)?

> Considerable benefit to automating forensic audits of infected computers
  - Save time and effort during a crises
  - Help provide insights into the nature of an outbreak
  - Help drive change and improvements to policies and procedures.
  - Helps provide the knowledge to reduce both the size and number of outbreaks.

or

-- Last Slide --