ISS – X-Force Professional Security Services

Virtual Machines for Real Malware Capture and Analysis.

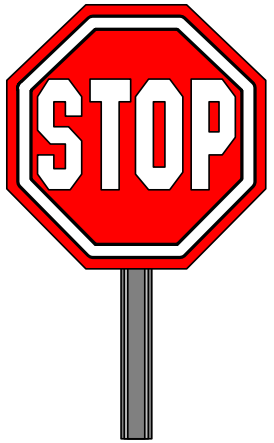
– Martin Overton

– Malware/Anti-Malware SME

Abstract

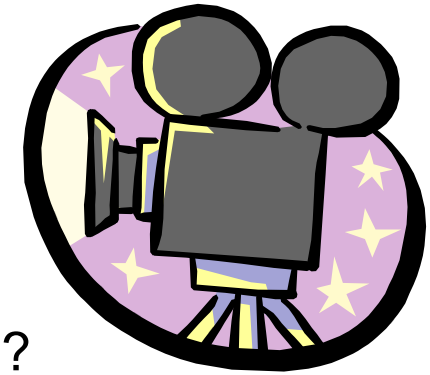
- *Virtual machines are widely used by malcode researchers to analyse new malware or to see what it does without risking a real machine. However, virtual machine aware malware has now appeared which makes using them more problematic.*
- *The beauty of using virtual machines is that they can be easily reset to a 'known clean state' as well as part of virtual networks shared by individual virtual machines. This means that you can simulate the internet to allow analysis of worms, bots and other network borne threats as well as traditional viruses, worms and trojans.*
- *This paper will show how useful virtual machines are to security professionals, using VMware as a working platform. It will also discuss ways to use VMware to not only analyse what a new malware does, but also how to set up virtual machines and networks to capture malware. It will also discuss a selection of known anti-vm malware [including Conficker] and the ways they detect that they are running in a virtual machine.*

Disclaimer



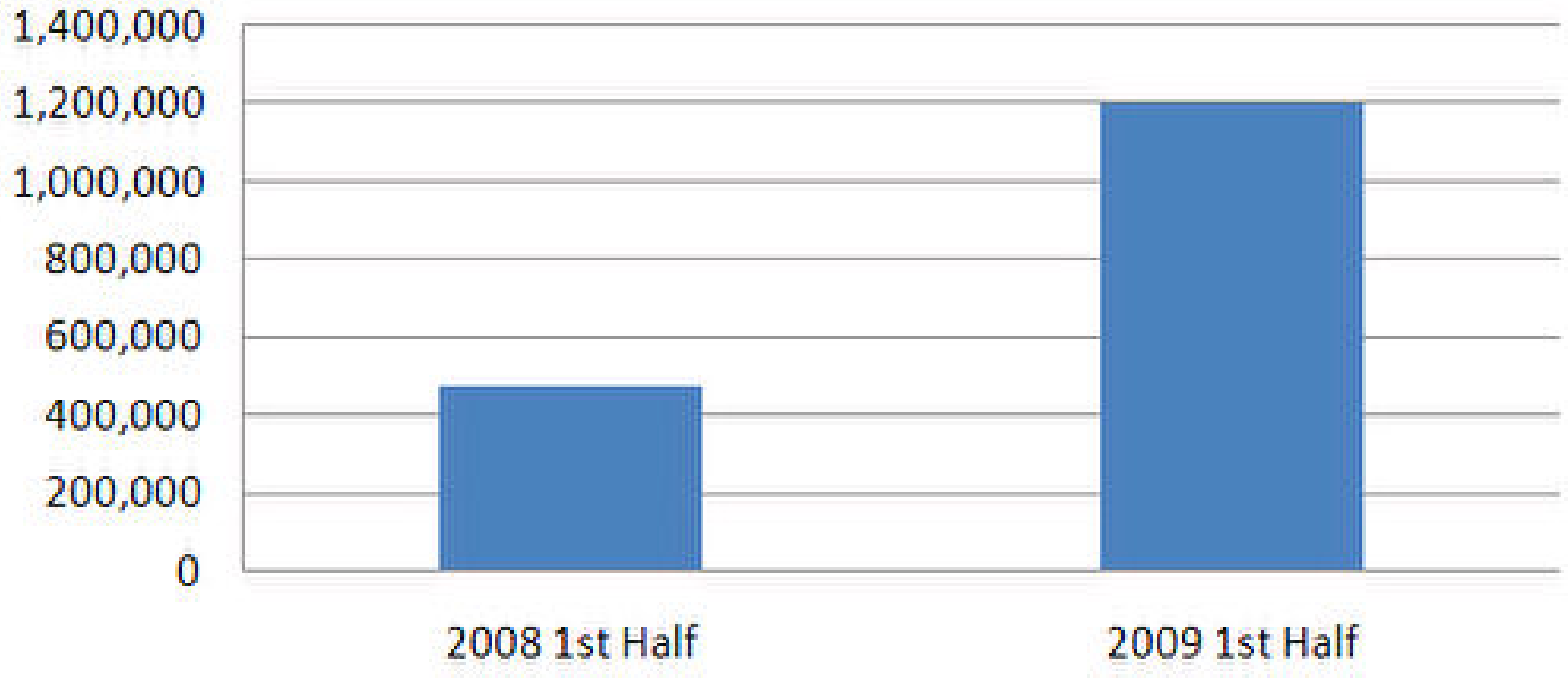
- Products named in this presentation are used as examples only, and should not be taken as any form of endorsement by IBM or ISS.
- All trademarks and copyrights are acknowledged.

Agenda



- What is a Virtual Machine?
  - What Platforms Can You Run VMware On?
  - Guest Operating Systems Supported
  - Benefits & Issues
  - Malware Capture
  - Malware Analysis
- Tools
- Summary
- Conclusions
- Questions

Half Year Malware Growth Comparison

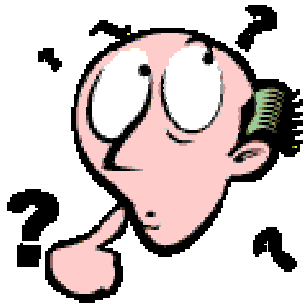


Source: McAfee

What is a Virtual Machine?

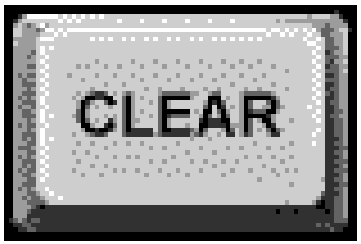
- "*A virtual machine was originally defined by Popek and Goldberg as "an efficient, isolated duplicate of a real machine". Current use includes virtual machines which have no direct correspondence to any real hardware.*"

What is a Virtual Machine?



- For this paper we are going to just focus on system virtual machines; specifically VMware.
- So here is a further definition:
  - ***"System virtual machines (sometimes called hardware virtual machines) allow the sharing of the underlying physical machine resources between different virtual machines, each running its own operating system. The software layer providing the virtualization is called a virtual machine monitor or hypervisor."***

What is a Virtual Machine?



- Several other popular VM offerings fall under this definition, these include:
  - ***Sun's VirtualBox***
  - ***Microsoft VirtualPC and VirtualServer***
  - ***VM from IBM***
  - ***Parallels Workstation and Desktop***
- Definition and prerequisites now completed let me start to cover the use of VMware for malware capture and analysis (both dynamic and static).

What Platforms Can You Run VMware On?

- **Windows**

- **Linux**

- **Mac**

Guest Operating Systems Supported

- **Microsoft Windows – Windows 3.1, 9x, Me,NT, 2K, XP, Vista, Server 2003 (32 & 64 bit) and Server 2008 (32 & 64 bit)**
- **Apple Mac OS X – 10.5 and 10.6 (experimental)**
- **Linux – Red Hat, SUSE, Novell, Mandrake, Ubuntu, Other Linux (32 & 64 bit)**
- **Novell Netware – NetWare 5 and 6**
- **Sun Solaris – 8, 9,and 10**
- **Other – MS-DOS, FreeBSD (32 & 64 bit), Other**

Other VM & Backup Images Supported:

- **The latest versions of Workstation & Fusion also support a number of other Virtual Machine image and backup formats, which can be a useful way to restore an infected or clean system as required, these include:**
  - *Acronis True Image 9 (.tib files)*
  - *StorageCraft ShadowProtect (.spf files)*
  - *Microsoft Virtual PC 7.x and higher (.vmc files)*
  - *Any version of Microsoft Virtual Server (.vmc files)*
  - *Symantec Backup Exec System Recovery (formerly LiveS tate Recovery) 6.5 and 7.0, LiveState Recovery 3.0 and 6.0 (.sv2i files)*
  - *Norton Ghost images 9.x and higher (.sv2i files)*

Benefits for Malware Analysis?

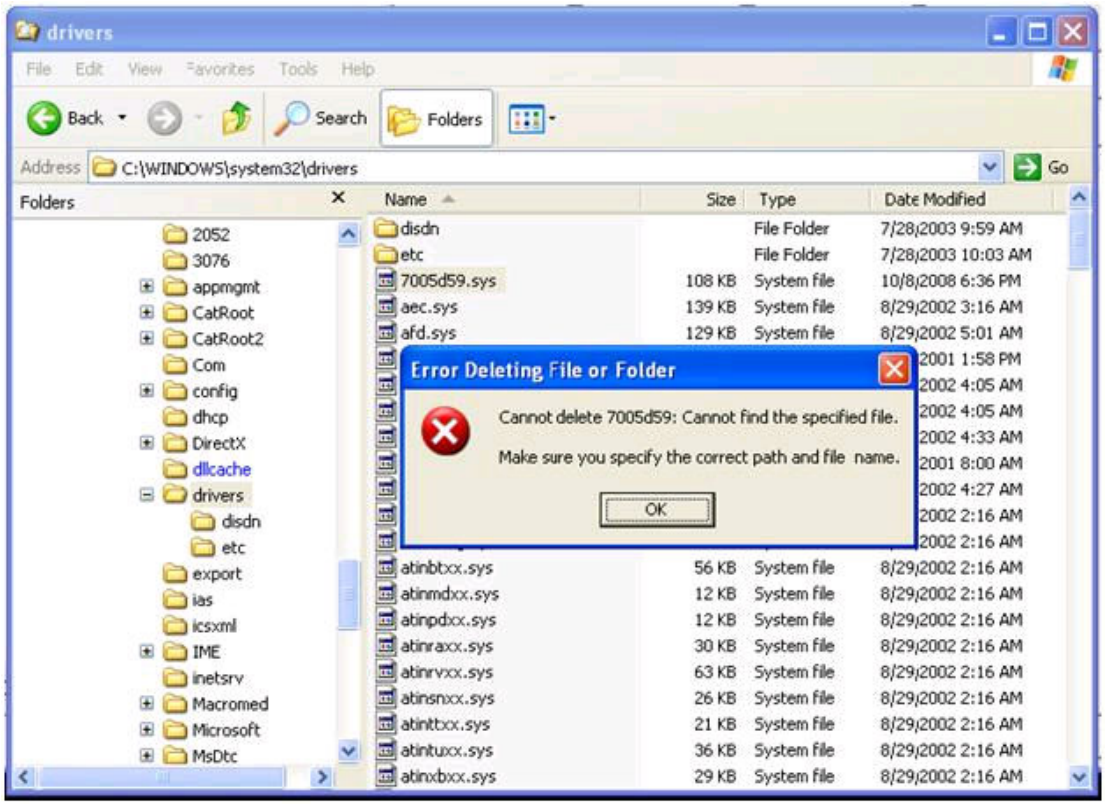
- **Snapshots**
- **Clone**
- **Non-persitence**
- **Virtual Network**
- **Isolation**
- **Mixed VMware Guest Infrastructure**
- **Drag & Drop**
- **Shared Folders**

Issues for Malware Analysis?

- *VM-Aware Malware*
- *How they do it (amongst other methods)*
  - **API**
  - **BUS**
  - **LDT**
  - **IDT**
  - **Registry**
  - **Files/Directories**
  - **Etc, etc.**

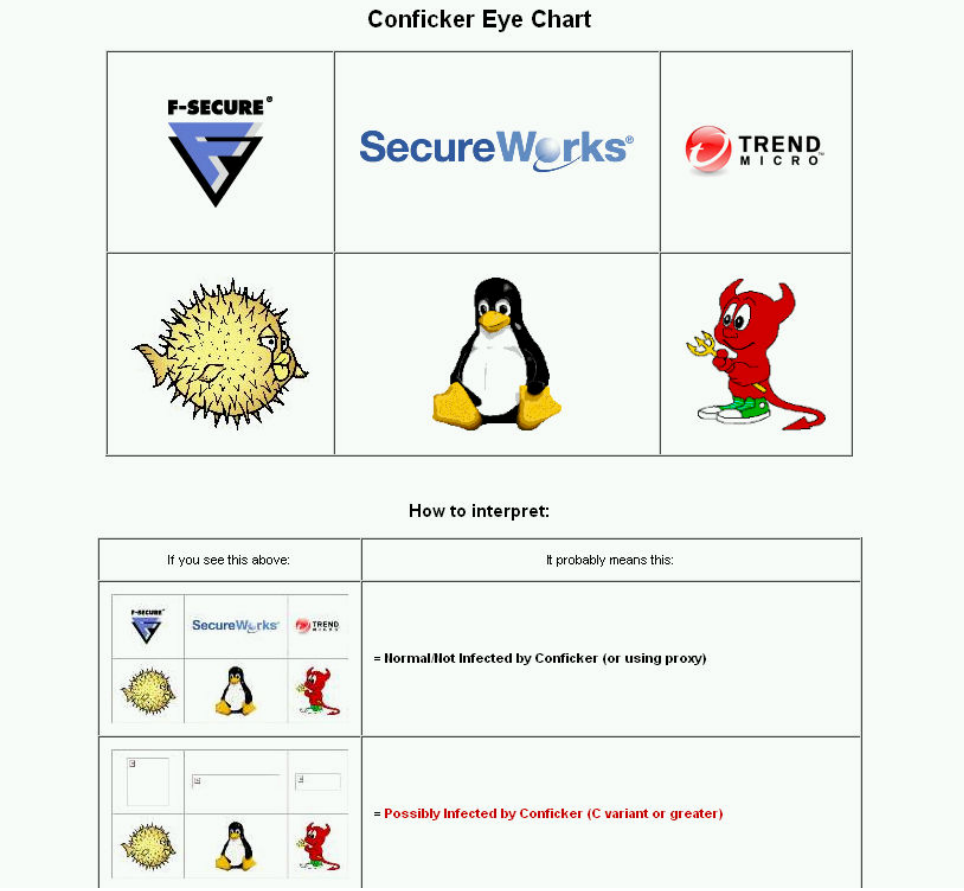
Rustock

- *"Rustock communicates with the PCI Bus Device to get two DWORDs. One DWORD indentifying the vendor and device ID of bridge between PCI Bus to Host and the other DWORD indentifying the device ID of the bridge between PCI Bus and ISA bridge. More than likely the malware uses these vendor and device IDs to detect VMware."*

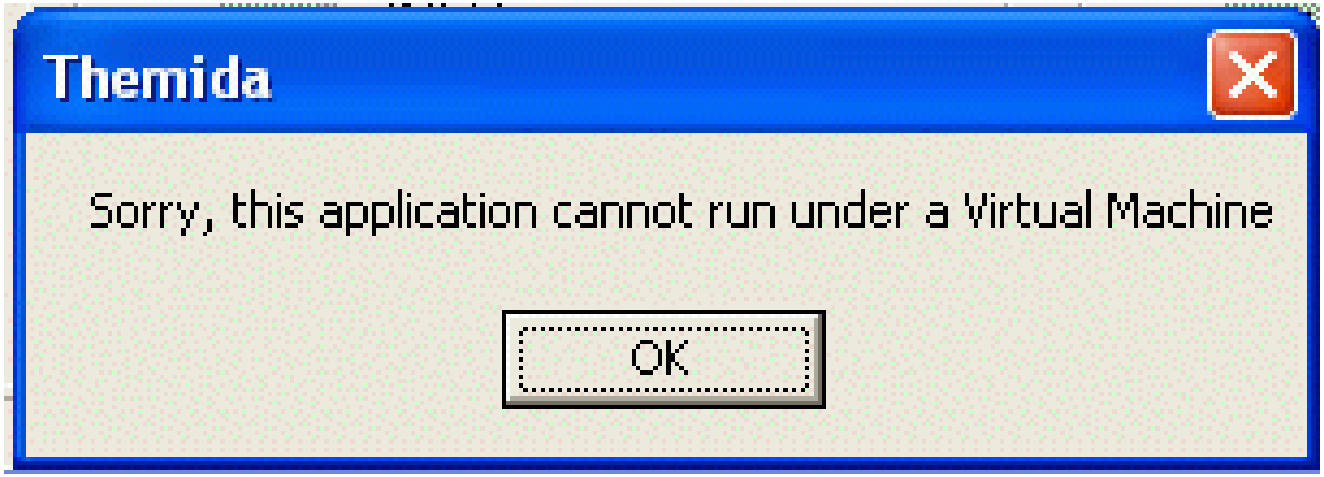


Conficker

- *"During the execution, Conficker calls the SLDT instruction many times. The SLDT instruction stores the Local Descriptor Table in a register that is then compared by Conficker with certain values. This allows Conficker to detect if it's running in a virtual machine – LDT of a native system will be 0x0000 while in VMware (or VirtualPC) LDT will be relocated (for example, in VMware 4 it will often be 0x4058).*
- *If it is 0, the execution continues, otherwise Conficker calls the Sleep function with the value of -1 (0xFFFFFFFF) – this will cause the process to sleep for 29826 hours (so, like forever)."*



Themida

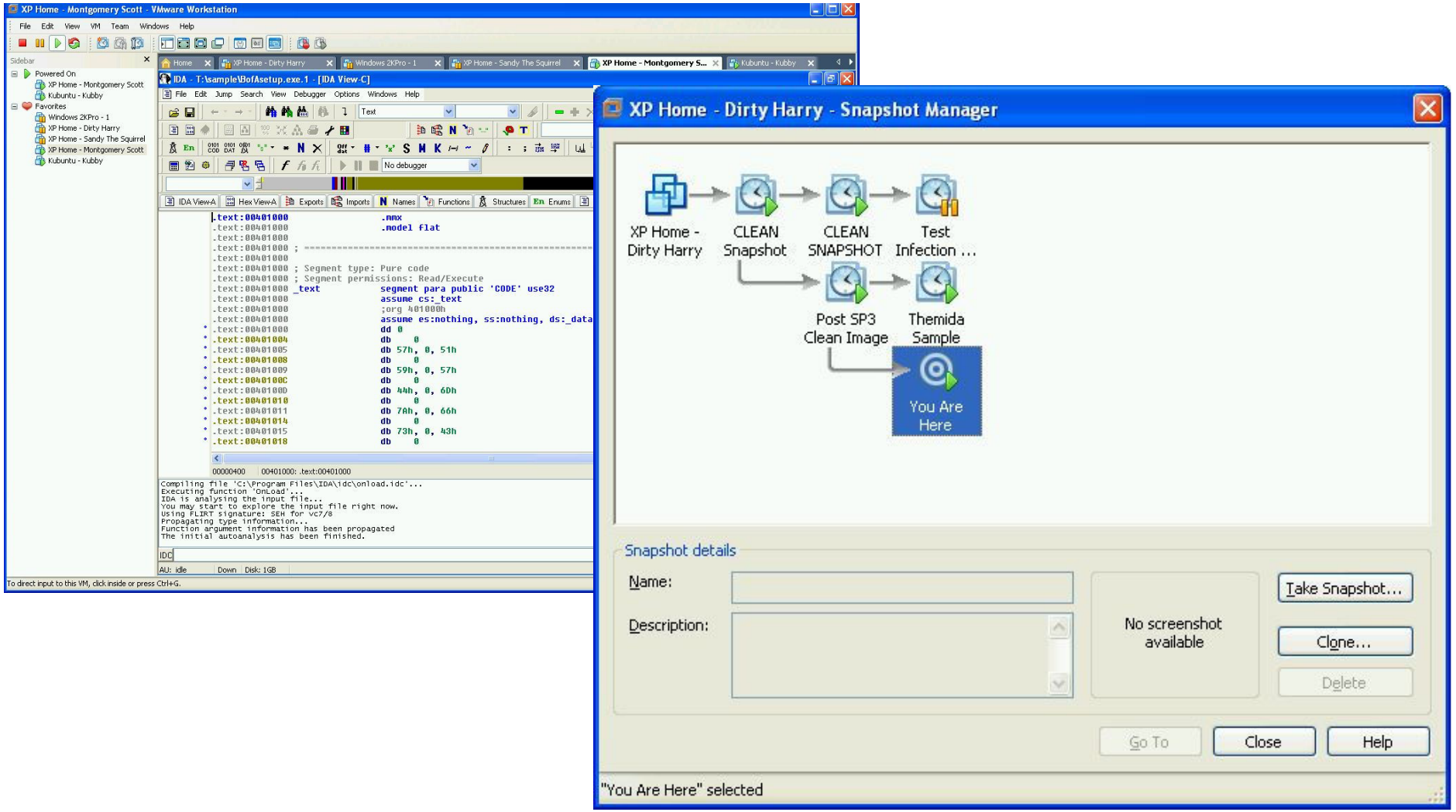


Themida

Malware that just won't run under VMware

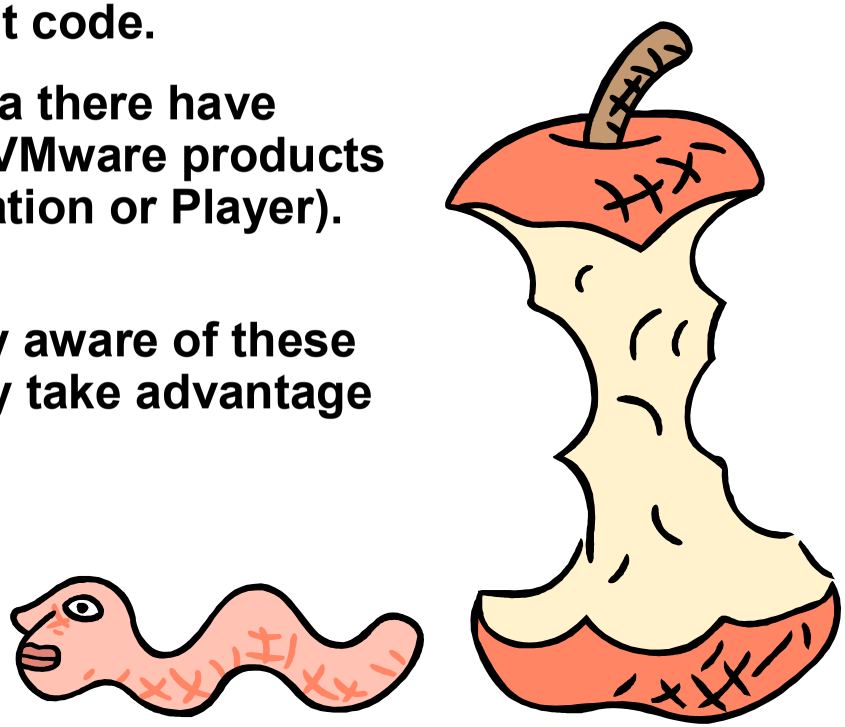
- **CIH**
  - CIH[1] fails to work under VMware but doesn't appear to have any detection routines that it is running inside a virtual machine.
  - There are almost certainly a number of other malware variants that through no obvious method will not run at all, or as designed, under VMware.
  - Why this is the case is unclear, it could be due to unsupported API calls, memory behaviour or other subtle differences between a real machine and the virtual one.
- **Break-Outs**
  - In all the time I've used VMware I have not experienced a malcode escape or breakout. It would be interesting to find out from other researchers if any of them have experienced one? I've certainly not heard of any verified cases.

Maintaining Images/snapshots



Vulnerabilities and Related Attacks

- **As with any application or operating system vulnerabilities are often discovered and often taken advantage of by cyber-criminals.**
- **When using VMware you have to bear in mind that you have another layer to patch and monitor for new and known vulnerabilities and exploit code.**
- **So far this year, according to Secunia there have been fifteen vulnerabilities found in VMware products (all of them, not just Fusion, Workstation or Player). In 2008 they published over 30**
- **The bad guys and girls are obviously aware of these weaknesses and will almost certainly take advantage of them if they can.**

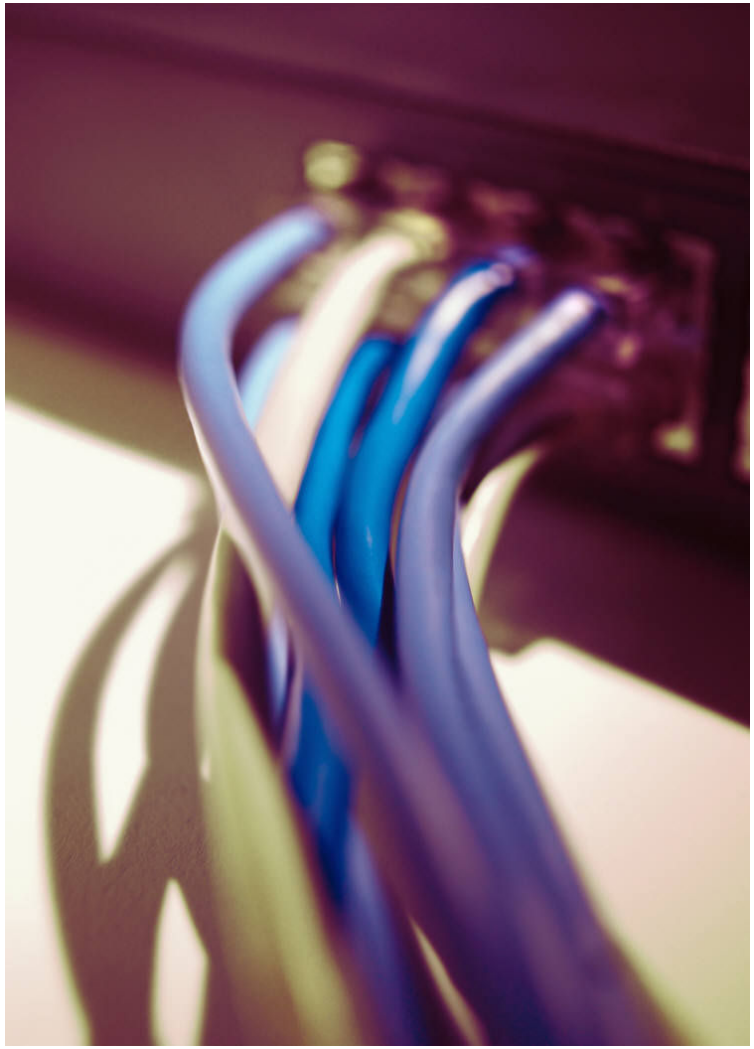


Malware Capture

- **WormCharmer**
  - You can easily create a WormCharmer system using VMware, details on how this works can be found in my VB2003 paper entitled “Worm Charming: Taking SMB Lure to the Next Level”.
- **Honeyd**
  - One of the oldest and most widely respected honeynet tool is Honeyd which is maintained and developed by Niels Provos. Honeyd runs mainly on BSD and Linux although it will also work on Solaris and a Windows port exists.
- **Nepenthes**
  - Another well known and respected tool for capturing malware is Nepenthes, which is somewhat similar to mwcollect. Nepenthes runs mainly on BSD and Linux, although as the source code is available you may be able to compile it for other *NIX flavours.
- **Open and/or Un-patched systems**
  - One of my IBM colleagues (Eric Johansen) used VMware to create a honeynet of open and un-patched windows systems and he documented his findings in a paper for the VB2005 conference, entitled “*Anti-virus in the wild*”.

Malware Analysis

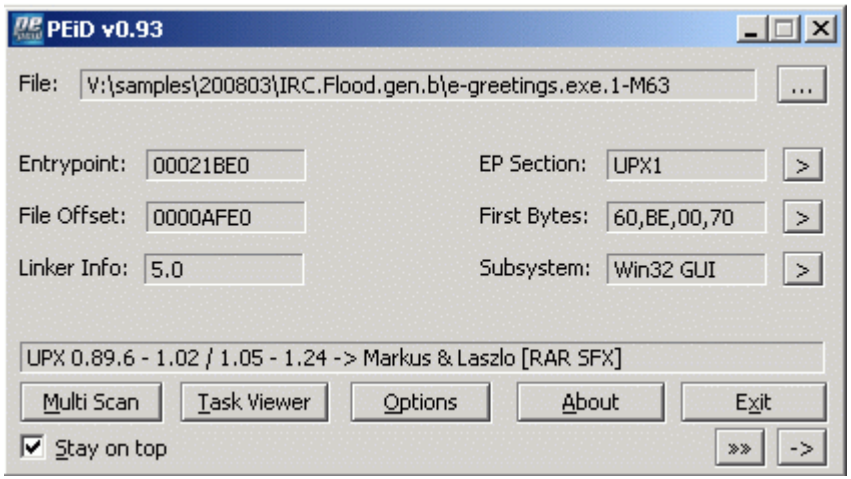
- **Network Configurations**
  - VMware has a virtual 10 port switch inside itself to handle a wide variety of networking configurations. Three of these (virtual switch ports) are mapped by default; these being: VMnet0 (Bridged), VMnet8 (NAT) and VMnet1 (Host-Only).
- **Host only**
- **Bridged**
- **NAT**
- **Custom**

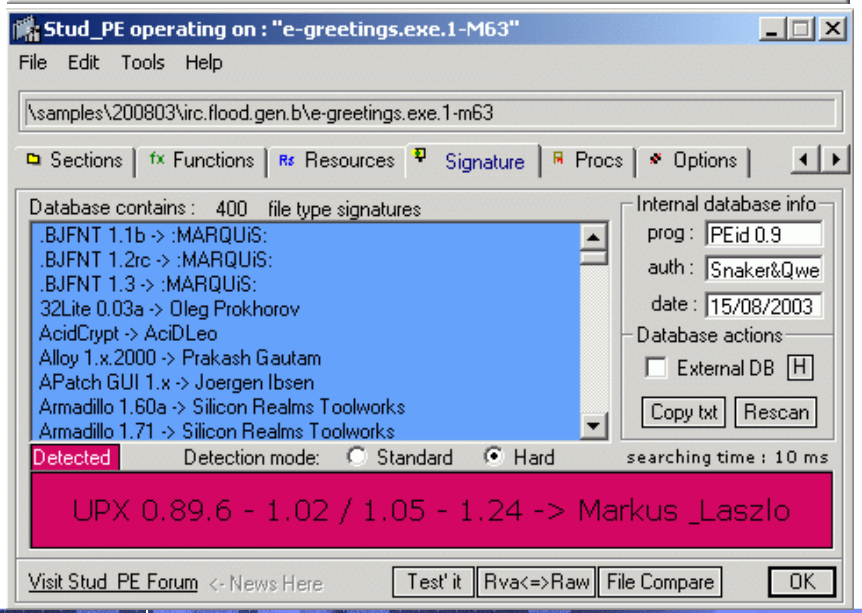


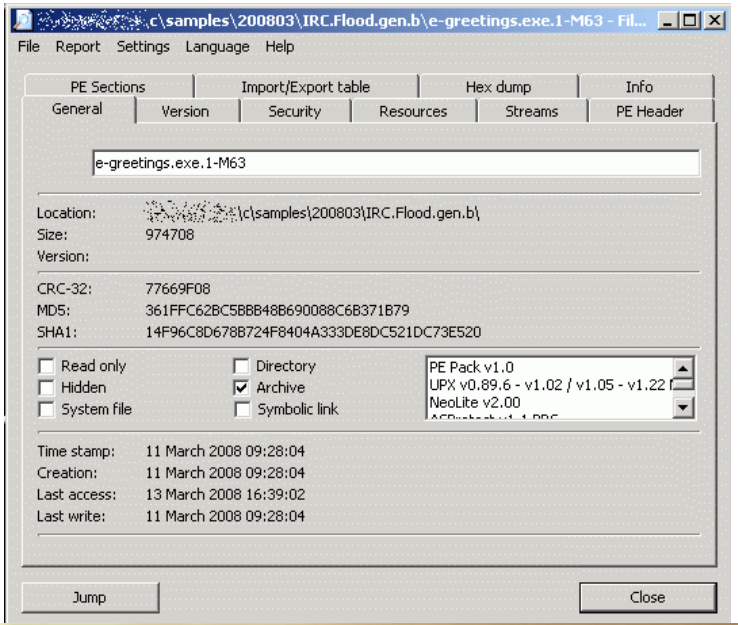
Other Options

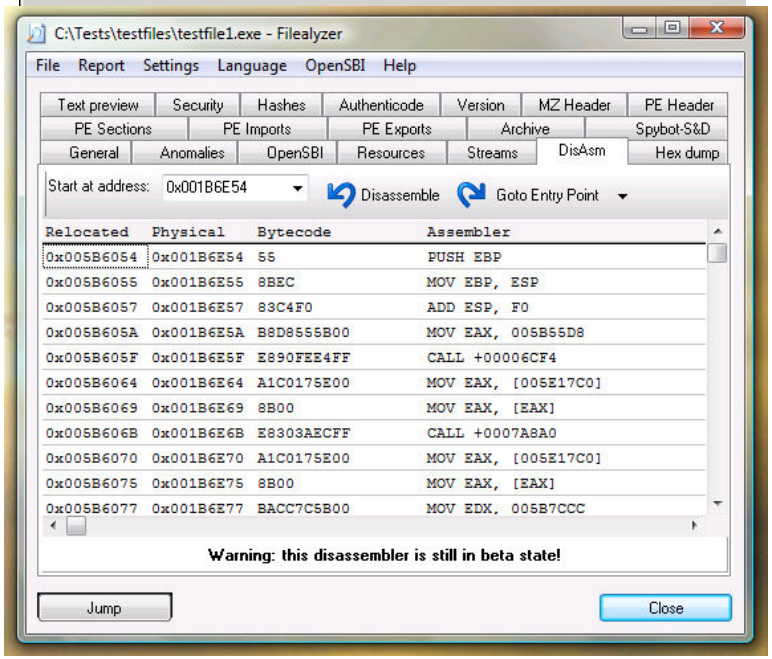
- **VMware Player**
  - VMware Player does not have the ability to create Virtual Machines, only use ones already created by VMware Workstation or other supported products and other supported non-VMware product images (such as Norton Ghost). You can though, modify the configuration of existing Virtual Machines.
- **Mount ISO images**
  - VMware can also directly boot off an ISO image of a CD/DVD ROM. It also has the ability to create Floppy Disk images and boot from those too; could be useful for boot sector infection testing, maybe?
- **VMware Apps**
  - If you use the VMware Player, Workstation, Fusion or the server versions you can use the pre-setup VMware Applications; many are free and kindly donated by vendors, security professionals and other VMware users.

Tools:
Stud_PE, PEiD, FileAlyzer

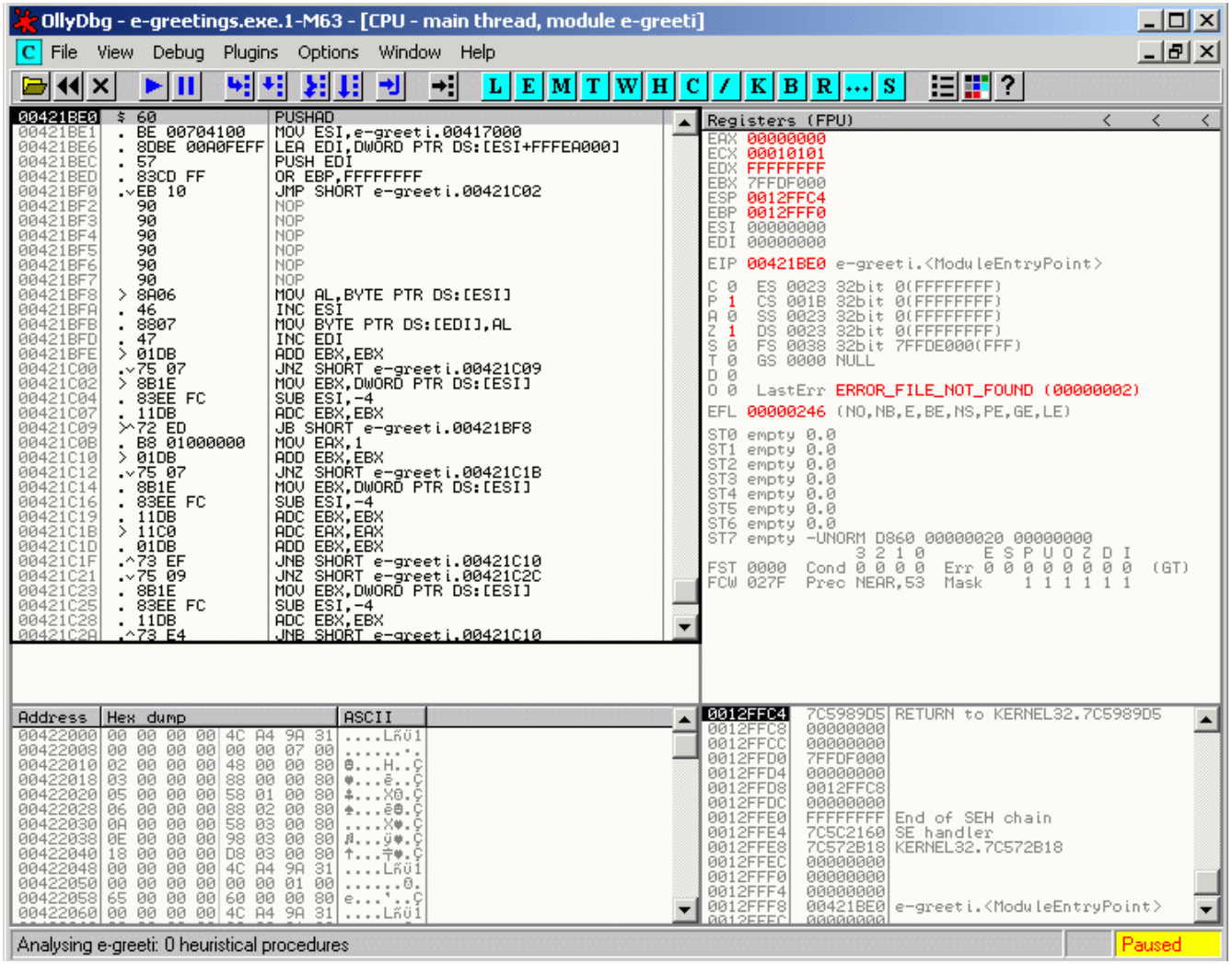




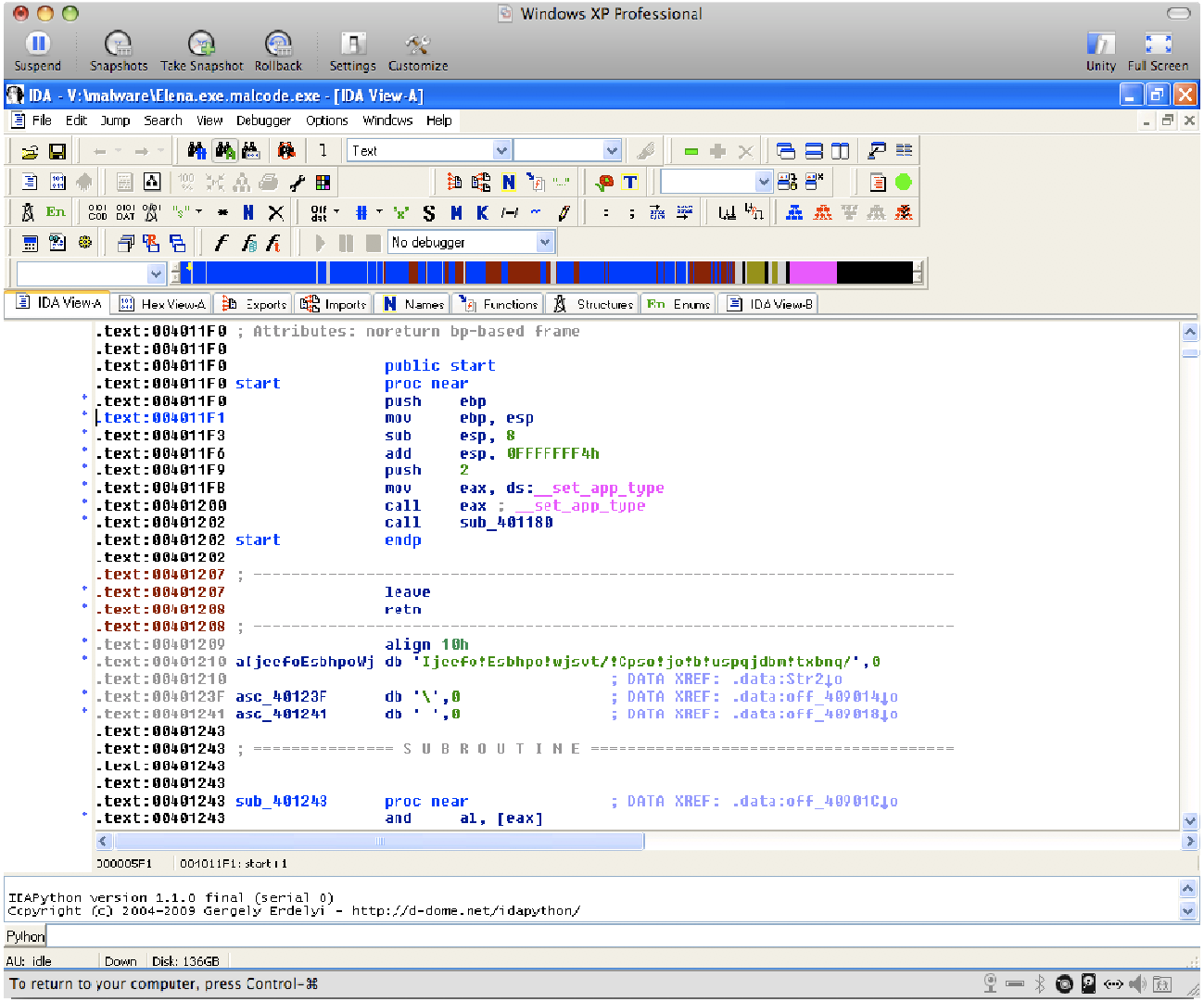




Tools: OllyDbg

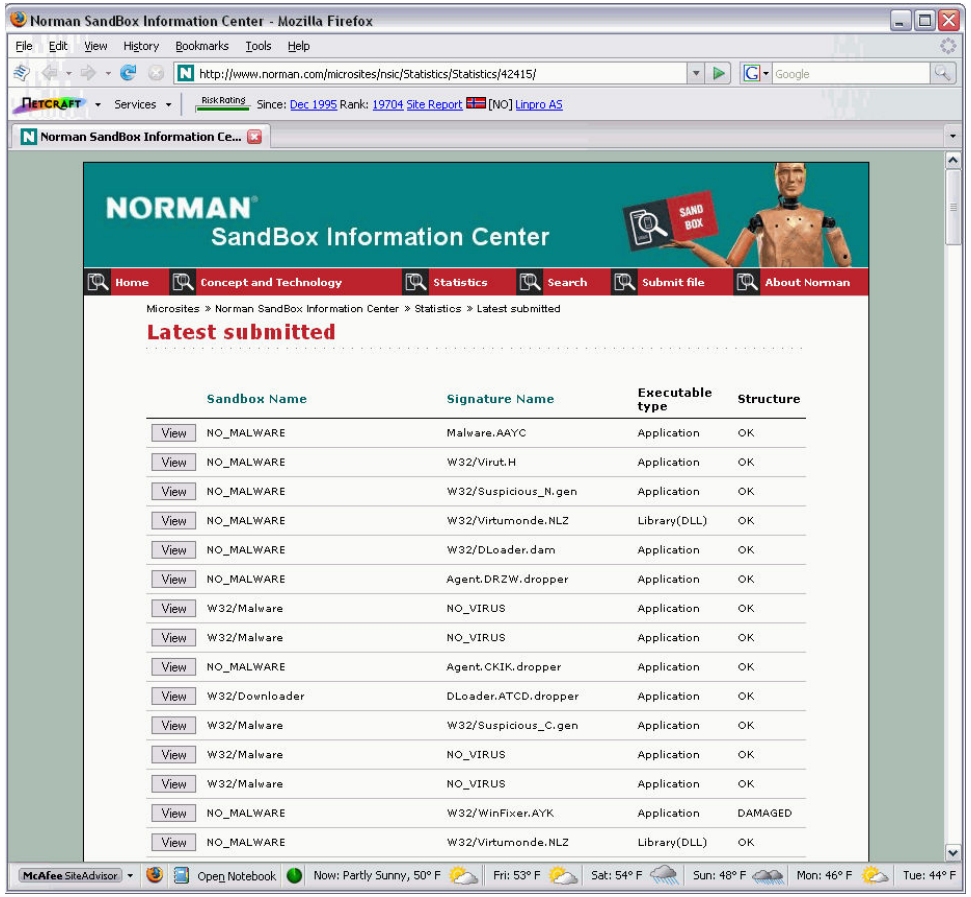


Tools: IDAPro



Tools: Inctrl5

Tools: Sandboxes



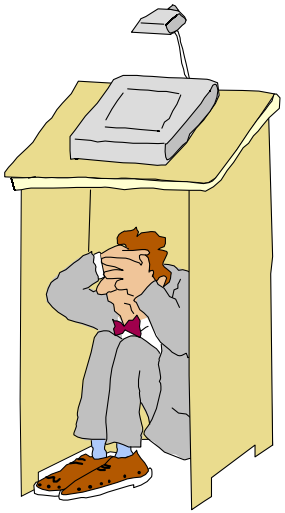
Summary

- So now we've looked at VMware and the features it offers as well as the issues it brings to the capture and analysis table when working with malcode.
- Networking has been covered in reasonable detail, as has managing snapshots and complete images.
- We've also looked at a small selection of tools that are extremely useful when analysing malcode, whether it be statically or dynamically.
- For those of you that would like to dig deeper into the areas I've covered in this paper, then a wealth of material can be found via the links and suggested reading in appendix A.
- So, what conclusions can we draw from the material covered in this paper?

Conclusions

- Hopefully I have shown you that VMware has a place in the toolbox of a malware researcher and security staff too. It also has its place in consolidation of servers in organisations, ISPs, academia and service providers where cost reduction and server utilisation can be crucial to ensure competitive pricing and computing facilities; well, at the moment at least.
- Using VMware can save many companies an otherwise significant investment in hardware that may never be fully realised. Using it allows existing hardware to be fully utilised, or to allow a server farm to be downsized to a smaller number of physical machines.
- The benefits and risks associated with using VMware go beyond those related to malcode, and these risks and benefits need to be acknowledged and factored in to any solution or service that you plan to build or offer.
- If the current trend from malware authors continues, in that they detect that they are inside a virtual machine, emulator or sandbox, and then take no action (instead of turning destructive) , this could be seen as a positive use of such technologies as they would appear to be less likely to become infected.
- However, if the situation changes and malcode authors decide to change the behaviour of their creations to do something destructive or unexpected when they detect that their code is running inside a VM, emulator or sandbox, then it could be a serious blow to the vendors, and to those that base services and offerings based on these technologies.
- At this point it could easily go either way. Only time will tell which way the cyber criminals will eventually go.
- Please do not see this paper as an exhaustive or complete look at Virtual Machines and VMware specifically; to do this real justice would require enough material to fill a large book.

Questions?



Contact details…..

Martin Overton

EMEA Malware/Anti-Malware SME

IBM ISS X-Force – PSS

E-Mail: overtonm@uk.ibm.com

- **Telephone: +44 (0)239 2563442**

All my published papers and articles can be downloaded from:

http://momusings.co.uk/publications.aspx

or

http://momusings.com/papers

