



| ISS – X-Force Professional Security Services

Virtual Machines for Real Malware Capture and Analysis.



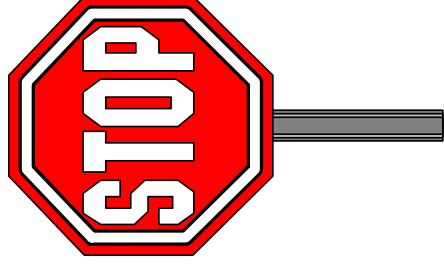
- Martin Overton
- Malware/Anti-Malware SME



Abstract

- *Virtual machines are widely used by malware 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.*

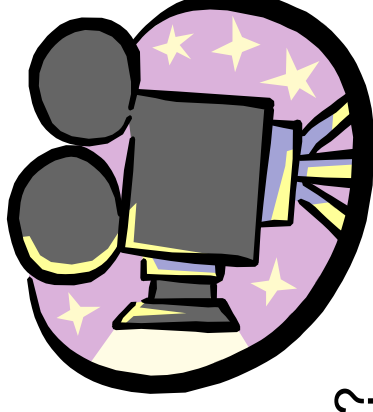
Disclaimer



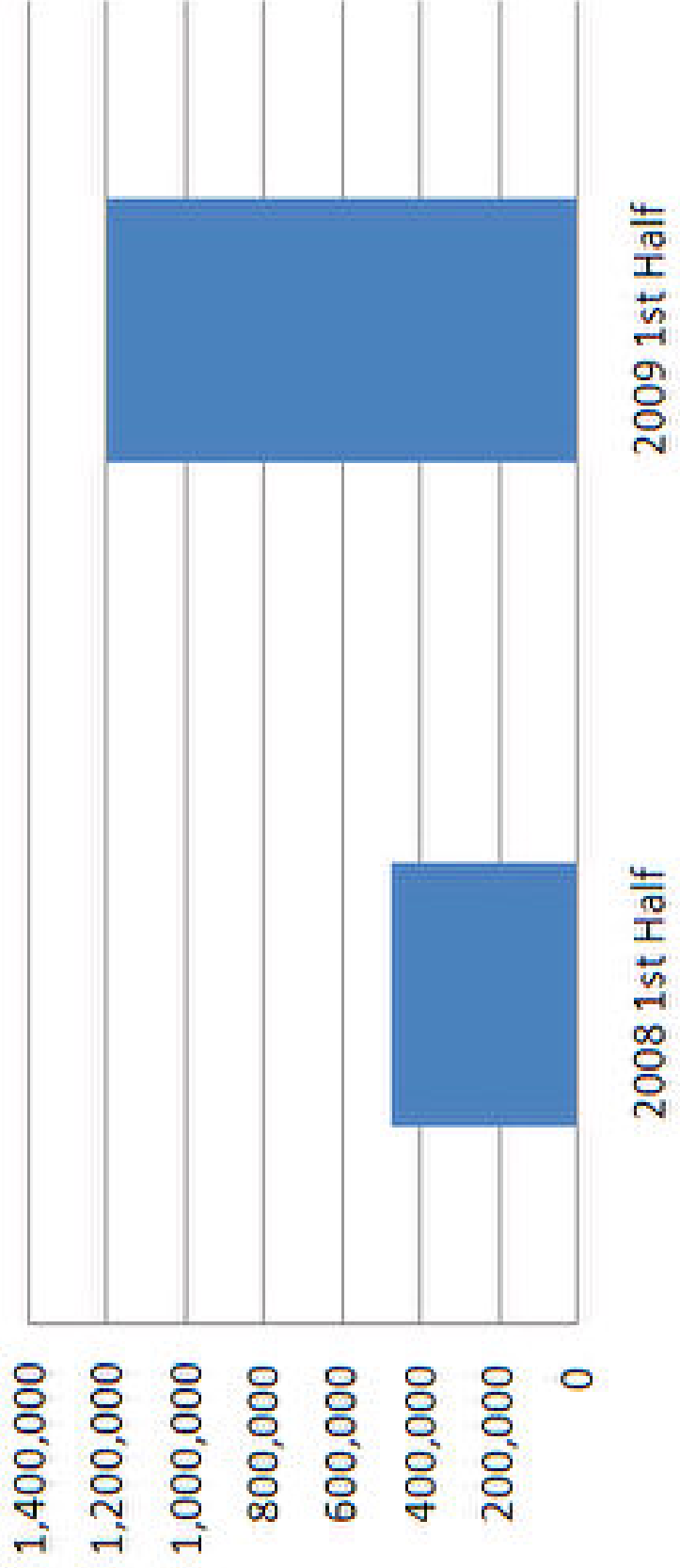
- Products named in this presentation are used as examples only, and should not be taken as any form of endorsement by IBM or ISS.
- All trademarks and copyrights are acknowledged.

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

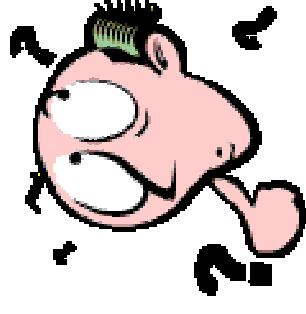


Source: McAfee

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.”*

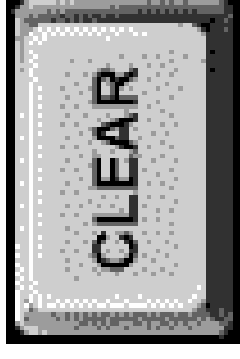




What is a Virtual Machine?

- 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)**

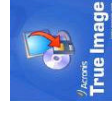
- 
 ■ **Novell Netware – NetWare 5 and 6**

- 
 ■ **Sun Solaris – 8, 9, and 10**

- 
 ■ **Other – MS-DOS, FreeBSD (32 & 64 bit), Other**

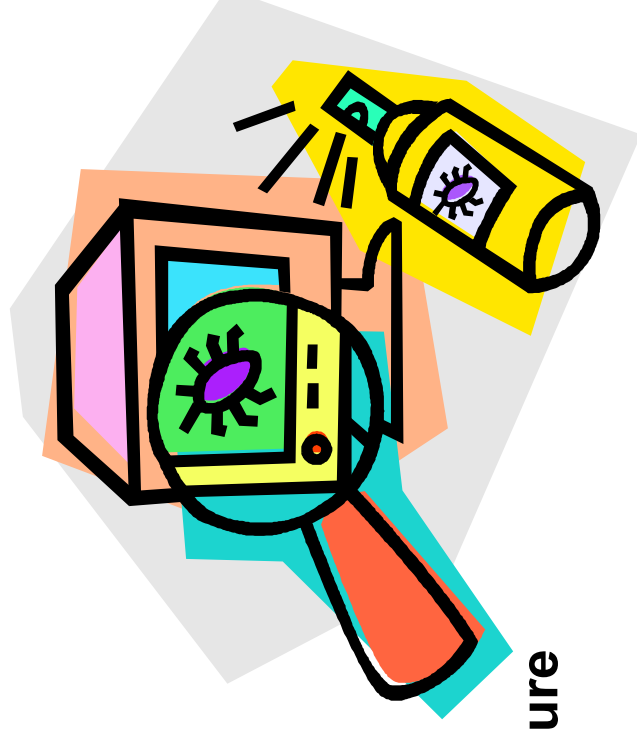
Other VM & Backup Images Supported:

- **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 (.vnc files)*
 - *Any version of Microsoft Virtual Server (.vmc files)*
 - *Symantec Backup Exec System Recovery (formerly LiveState 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-persistence**
- **Virtual Network**
- **Isolation**
- **Mixed VMware Guest Infrastructure**
- **Drag & Drop**
- **Shared Folders**



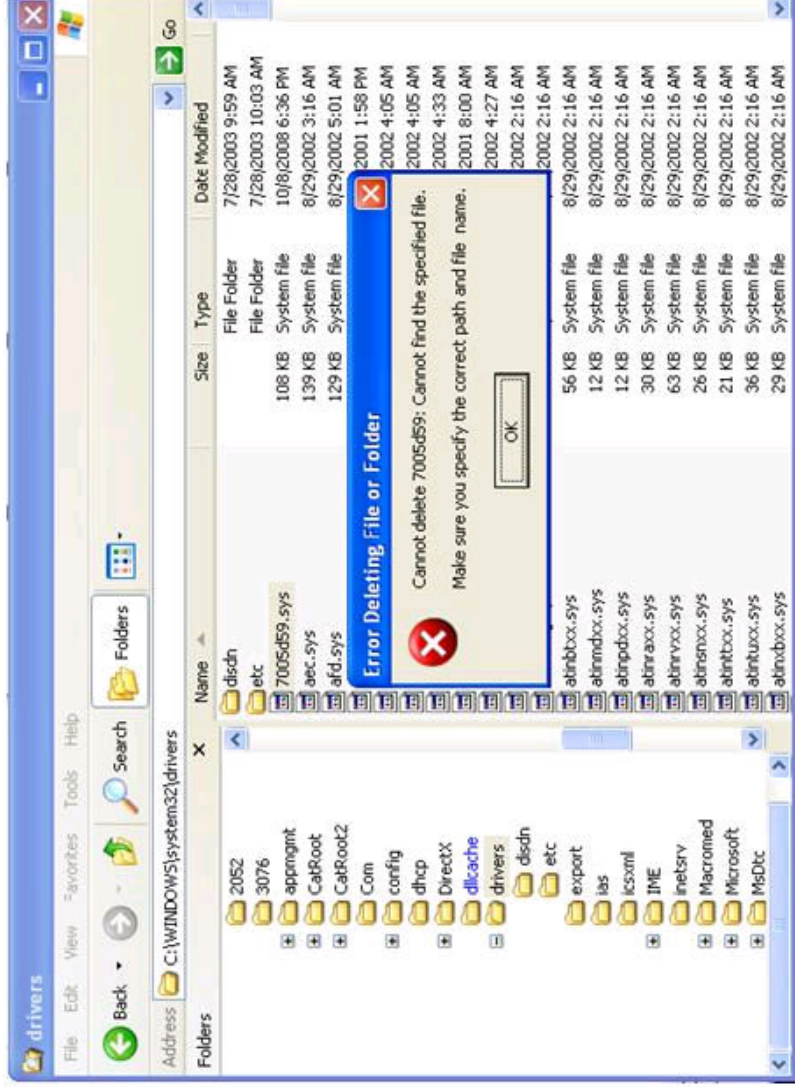
Issues for Malware Analysis?

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



Rustock

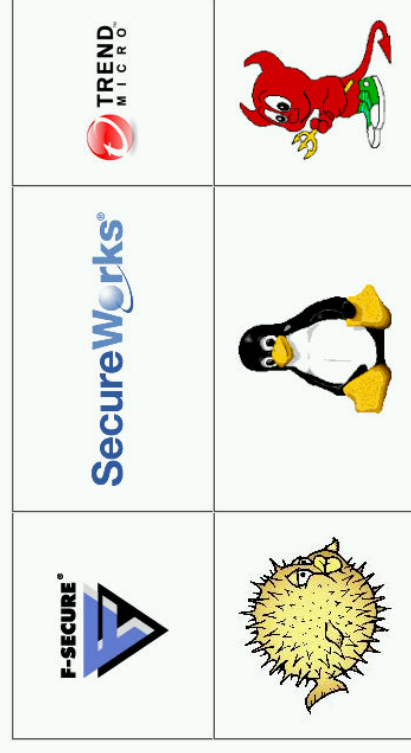
- *“Rustock communicates with the PCI Bus Device to get two DWORDs. One DWORD indentifying the vendor and device ID of bridge between PCI Bus to Host and the other DWORD indentifying the device ID of the bridge between PCI Bus and ISA bridge. More than likely the malware uses these vendor and device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

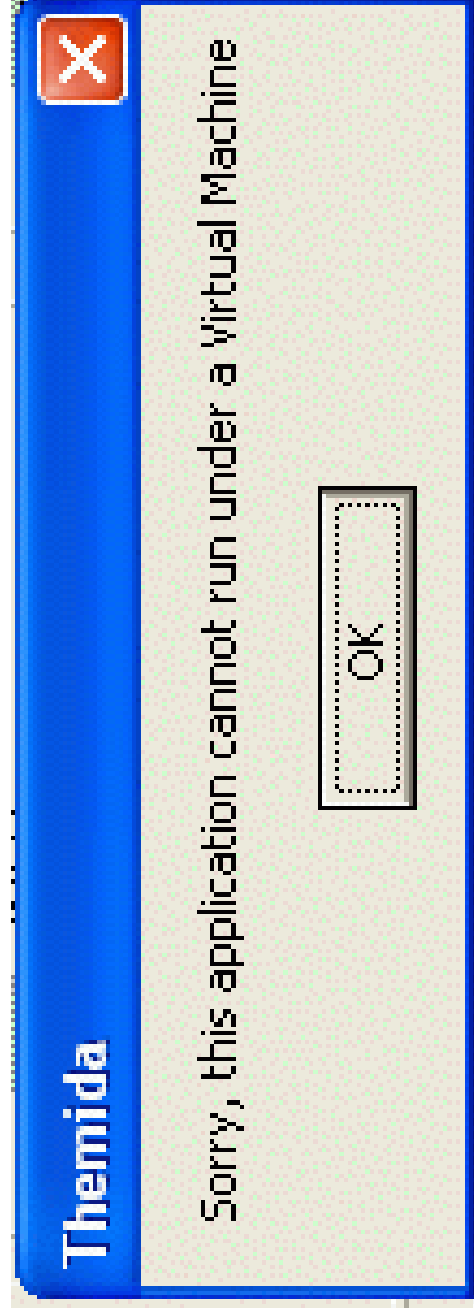
Conficker Eye Chart



How to interpret:

If you see this above:      	It probably means this: = Normal/Not Infected by Conficker (or using proxy)
     	= Possibly Infected by Conficker (C variant or greater)

Themida



Themida



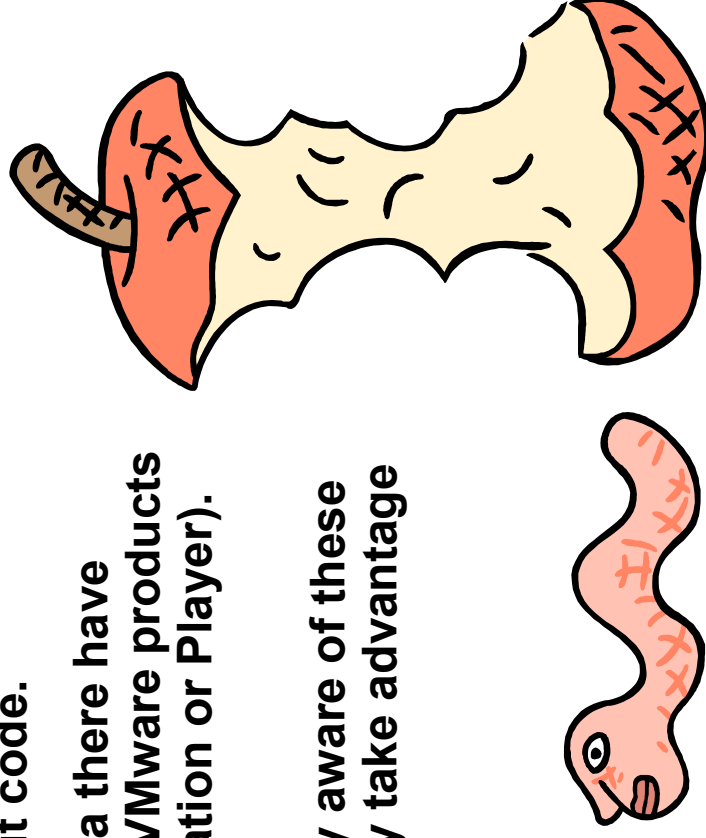
Malware that just won't run under VMware

- **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.



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

File: W:\samples\200803\IRC.Flood.gen.b\e-greetings.exe.1-m63

Endpoint: 00021BE0 EP Section: UPX1

File Offset: 0000AFE0 First Bytes: 60,BE,00,70

Linker Info: 5.0 Subsystem: Win32 GUI

UPX 0.89.6 - 1.02 / 1.05 - 1.24 -> Markus & Laszlo [RAR SFX]

Buttons: Multi Scan, Task Viewer, Options, About, Exit

Checkbox: Stay on top

Stud_PE operating on: "e-greetings.exe.1-m63"

Database contains: 400 file type signatures

- .BIFNT 1.1b -> MARQUIS:
- .BIFNT 1.2rc -> MARQUIS:
- .BIFNT 1.3 -> MARQUIS:
- 32Lite 0.03a -> Oleg Prokhorov
- AcidCrypt -> AcidLeo
- Alloy 1.x.2000 -> Prakash Gautam
- APatch GUI 1.x -> Joergen Ibsen
- Armadillo 1.60a -> Silicon Realms Toolworks
- Armadillo 1.71 -> Silicon Realms Toolworks

Internal database info:
prog: PEID 0.9
auth: [Snaker&Qwe]
date: [15/08/2003]

Database actions:
 External DB [H]
[Copy txt] [Rescan]

Detection mode: Standard Hard
searching time: 10 ms

Detected
UPX 0.89.6 - 1.02 / 1.05 - 1.24 -> Markus_Laszlo

Buttons: Test it, Rvack->Raw, File Compare, OK

File: e-greetings.exe.1-m63

Location: C:\samples\200803\IRC.Flood.gen.b\ (c:\samples\200803\IRC.Flood.gen.b\)

Size: 974708

Version: 77669F08

MDS: 361FFC262C5BB848B690088C66371B79

SHA1: 14F96C8D678B724F8404A333D8DC521DC73E520

Options: Read only, Hidden, System file, Directory, Archive, Symbolic link

PE Pack v1.0
UPX v0.89.6 - v1.02 / v1.05 - v1.22
Neolite v2.00

Time stamp: 11 March 2008 09:28:04
Creation: 11 March 2008 09:28:04
Last access: 13 March 2008 16:39:02
Last write: 11 March 2008 09:28:04

Buttons: Jump, Close

Disassemble

Start at address: 0x001B6E54

Relocated	Physical	Bytecode	Assembler
0x005B6054	0x001B6E54	55	PUSH ESP
0x005B6055	0x001B6E55	8BEC	MOV EBP, ESP
0x005B6057	0x001B6E57	83C4F0	ADD ESP, F0
0x005B605A	0x001B6E5A	B8D855B00	MOV EAX, 005B85D8
0x005B605F	0x001B6E5F	E990FE4FF	CALL +00006CF4
0x005B6064	0x001B6E64	ALC0175E00	MOV EAX, [005E17C0]
0x005B6069	0x001B6E69	8B00	MOV EAX, [EAX]
0x005B606B	0x001B6E6B	E8303AECFF	CALL +0007A8A0
0x005B6070	0x001B6E70	ALC0175E00	MOV EAX, [005E17C0]
0x005B6075	0x001B6E75	8B00	MOV EAX, [EAX]
0x005B6077	0x001B6E77	BACC7C5B00	MOV EDX, 005B7C00

Warning: this disassembler is still in beta state!

Buttons: Jump, Close

Tools: OllyDbg

Registers (FPU)

```

EAX 00000000
ECX 00010101
EDX FFFFFFFF
EBX 7FFDF000
ESP 0012FFC4
EBP 0012FF00
ESI 00000000
EDI 00000000
EIP 00421BE0 e-greet i.<ModuleEntryPoint>
C 0 ES 0023 32bit 0(FFFFFFFF)
P 1 CS 001B 32bit 0(FFFFFFFF)
Z 0 SS 0023 32bit 0(FFFFFFFF)
O 1 DS 0023 32bit 0(FFFFFFFF)
D 0 FS 0038 32bit 7FFDE000(FFF)
T 0 GS 0000 NULL
D 0 LastErr ERROR_FILE_NOT_FOUND (00000002)
EFL 00000246 (NO, NB, E, BE, NS, PE, GE, LE)
ST0 empty 0,0
ST1 empty 0,0
ST2 empty 0,0
ST3 empty 0,0
ST4 empty 0,0
ST5 empty 0,0
ST6 empty 0,0
ST7 empty -UNORM D860 00000020 00000000
FST 0000 Cond 0 0 0 Err 0 0 0 0 0 0 0 0 (GT)
FCW 027F Prec NEHR, S3 Mask 1 1 1 1 1 1
    
```

Assembly Code:

```

00421BE0 $ 60 PUSHAD
00421BE1 BE 00704100 MOV ESI,e-greet.i.00417000
00421BE6 80BE 0080FEFF LEA EDI,DWORD PTR DS:[ESI+FFFEA000]
00421BE7 57 PUSH EDI
00421BED OR EBX,FFFFFFFF
00421BF0 JMP SHORT e-greet.i.00421C02
00421BF2 NOP
00421BF3 NOP
00421BF4 NOP
00421BF5 NOP
00421BF6 NOP
00421BF7 NOP
00421BF8 > 8A06 MOV AL,BYTE PTR DS:[ESI]
00421BF9 INC ESI
00421BFA INC EDI
00421BFB MOV BYTE PTR DS:[EDI],AL
00421BFD INC EDI
00421BFE ADD EBX,EBX
00421C00 JNZ SHORT e-greet.i.00421C09
00421C02 MOV EBX,DWORD PTR DS:[ESI]
00421C04 SUB ESI,-4
00421C07 ADC EBX,EBX
00421C09 JB SHORT e-greet.i.00421BF8
00421C0B MOV EAX,1
00421C0E ADD EBX,EBX
00421C10 > 010B INC EBX
00421C12 > 75 07 JNZ SHORT e-greet.i.00421C1B
00421C14 > 8B1E MOV EBX,DWORD PTR DS:[ESI]
00421C16 > 83EE FC SUB ESI,-4
00421C19 ADC EBX,EBX
00421C1B > 110B INC EBX
00421C1D > 010B INC EBX
00421C1F > 73 EF JNB SHORT e-greet.i.00421C10
00421C21 > 75 09 JNZ SHORT e-greet.i.00421C2C
00421C23 > 8B1E MOV EBX,DWORD PTR DS:[ESI]
00421C25 > 83EE FC SUB ESI,-4
00421C28 > 110B INC EBX
00421C2A > 73 E4 JNB SHORT e-greet.i.00421C10
    
```

Memory Dump:

Address	Hex dump	ASCII
00422000	00 00 00 00 00 4C R4 9A 31LRUI
00422008	00 00 00 00 00 07 00H..C
00422010	03 00 00 00 00 48 00 80	...e..C
00422018	05 00 00 00 00 88 00 80	...X.C
00422020	06 00 00 00 00 58 01 00	...e.C
00422028	06 00 00 00 00 80 02 00	...X.C
00422030	0E 00 00 00 00 58 03 00	...X.C
00422038	0E 00 00 00 00 98 03 00	...X.C
00422040	18 00 00 00 00 08 03 00	...T.C
00422048	00 00 00 00 00 4C R4 9A 31LRUI
00422050	00 00 00 00 00 00 01 000
00422058	65 00 00 00 00 60 00 00C
00422060	00 00 00 00 00 4C R4 9A 31LRUI

Stack:

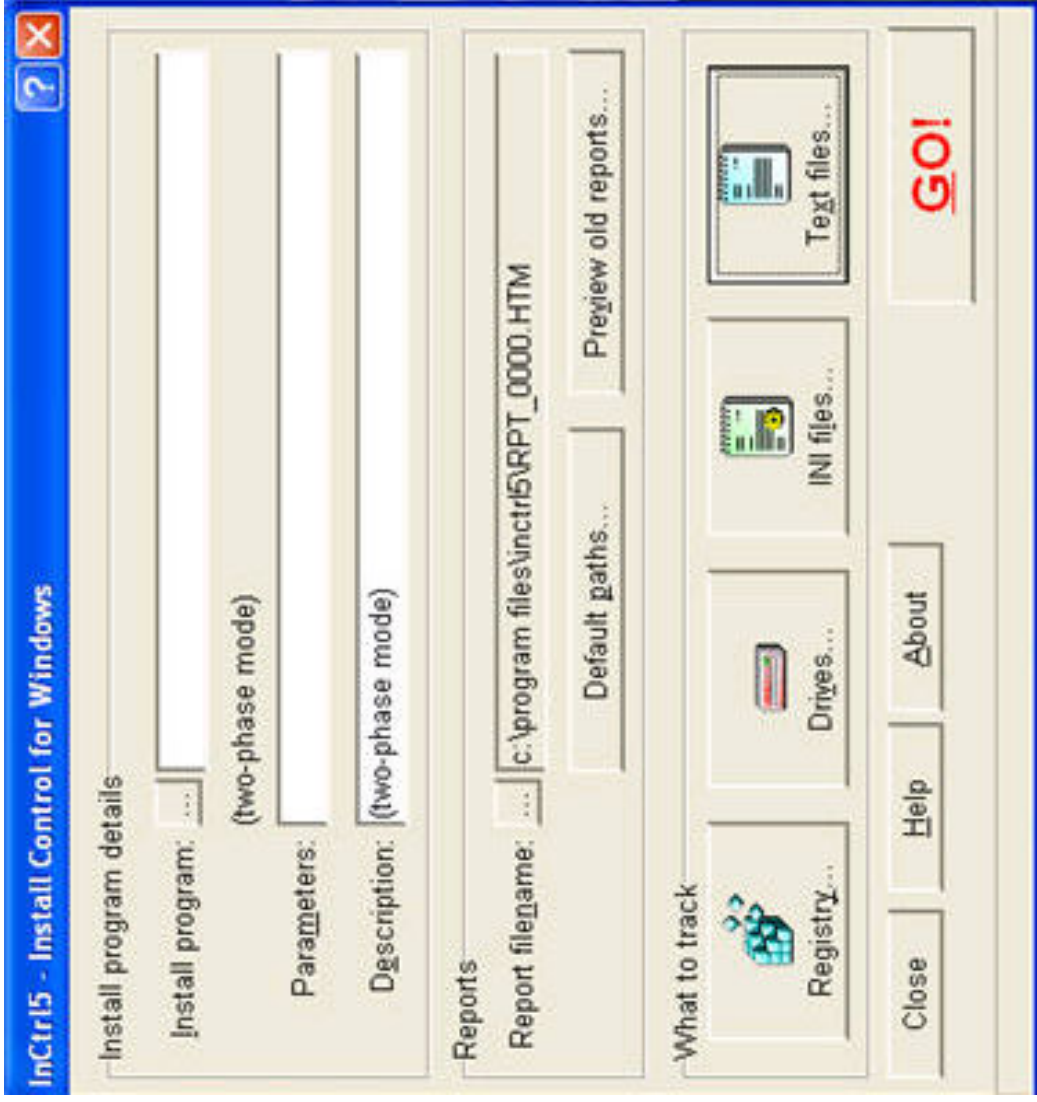
```

7C5989D5 RETURN to KERNEL32.7C5989D5
0012FFC8 00000000
0012FFCC 00000000
0012FFD0 7FFDF000
0012FFD4 00000000
0012FFD8 0012FFC8
0012FFDC 00000000
0012FFE0 FFFFFFFF
0012FFE4 0012FFE4
0012FFE8 7C5C2160 SE handler
0012FFEC 00000000 KERNEL32.7C572B18
0012FFF0 00000000
0012FFF4 00000000
0012FFF8 00421BE0 e-greet i.<ModuleEntryPoint>
0012FE00 00000000
    
```

Analysing e-greet: 0 heuristical procedures

Paused

Tools: Inctrl5



Tools: Sandboxes

Norman Sandbox Information Center - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://www.norman.com/microsites/nsc/statistics/42415/

Services Since: Dec. 1995 Rank: 19704 Site Report [NO] Linux AS

NORMAN SandBox Information Center

Concept and Technology Statistics Search Submit file About Norman

Microsites > Norman Sandbox Information Center > Statistics > Latest submitted

Latest submitted

Sandbox Name	Signature Name	Executable type	Structure
View NO_MALWARE	Malware.AAYC	Application	OK
View NO_MALWARE	W32/Virt-H	Application	OK
View NO_MALWARE	W32/Suspicious_N_gen	Application	OK
View NO_MALWARE	W32/Virtumonde.NLZ	Library(DLL)	OK
View NO_MALWARE	W32/Dloader.dam	Application	OK
View NO_MALWARE	Agent-DR2W_dropper	Application	OK
View W32/Malware	NO_VTRUS	Application	OK
View W32/Malware	NO_VTRUS	Application	OK
View NO_MALWARE	Agent-CKIK-dropper	Application	OK
View W32/Downloader	DLoader.ATCD-dropper	Application	OK
View W32/Malware	W32/Suspicious_C_gen	Application	OK
View W32/Malware	NO_VTRUS	Application	OK
View W32/Malware	NO_VTRUS	Application	OK
View NO_MALWARE	W32/WinFixer.AYK	Application	DAMAGED
View NO_MALWARE	W32/Virtumonde.NLZ	Library(DLL)	OK

CWSandbox Webinterface v2 - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://www.cwsandbox.org/?page=sampledetails

Services Since: Sep. 2006 Rank: 210382 Site Report [DE] Universitaet Mannheim

CWSandbox Webinterface

Home Technical Details Resources Sample Report Licensing Links Submit

Sample Analysis Details

XML (Popup) - TXT (Popup) - HTML - (Popup)

CWSandbox MALWARE ANALYSIS REPORT

Scan Summary

- File Changes
- Registry Changes
- Network Activity
- Technical Details

Submission Details

Date: 04.12.2006 20:51:24

Sandbox Version: 1.86

File Name: d781809c006f96c59675d212680455.exe

Summary Findings

Total Number of Processes: 4

Termination Reason: NormalTermination

Start Time: 00:00:063

Stop Time: 00:00:016

Start Reason: Analysis Target

Scanner Results

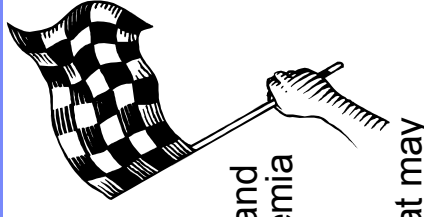
Scan Engine	Version	Signature Version	Result	More Info
ClamAV	0.88.2	2285	OK	
BitDefender	7.0.2492	324601	GenPack.Generic.Sabot.ACG5ZTB	
Avast! Antivirus	2.1.8.64	6.36.1.130	Worm/Sabot.34208.72	

Analysis Highlights

Open Notebook Now: Partly Sunny, 50° F Fri: 53° F Sat: 54° F Sun: 48° F Mon: 46° F Tue: 44° F

Summary

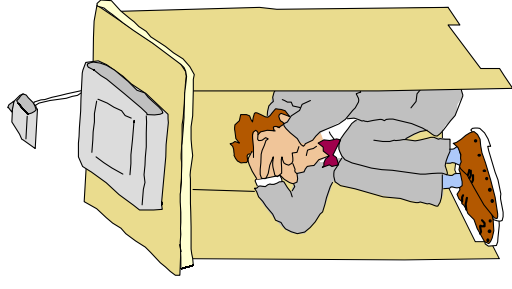
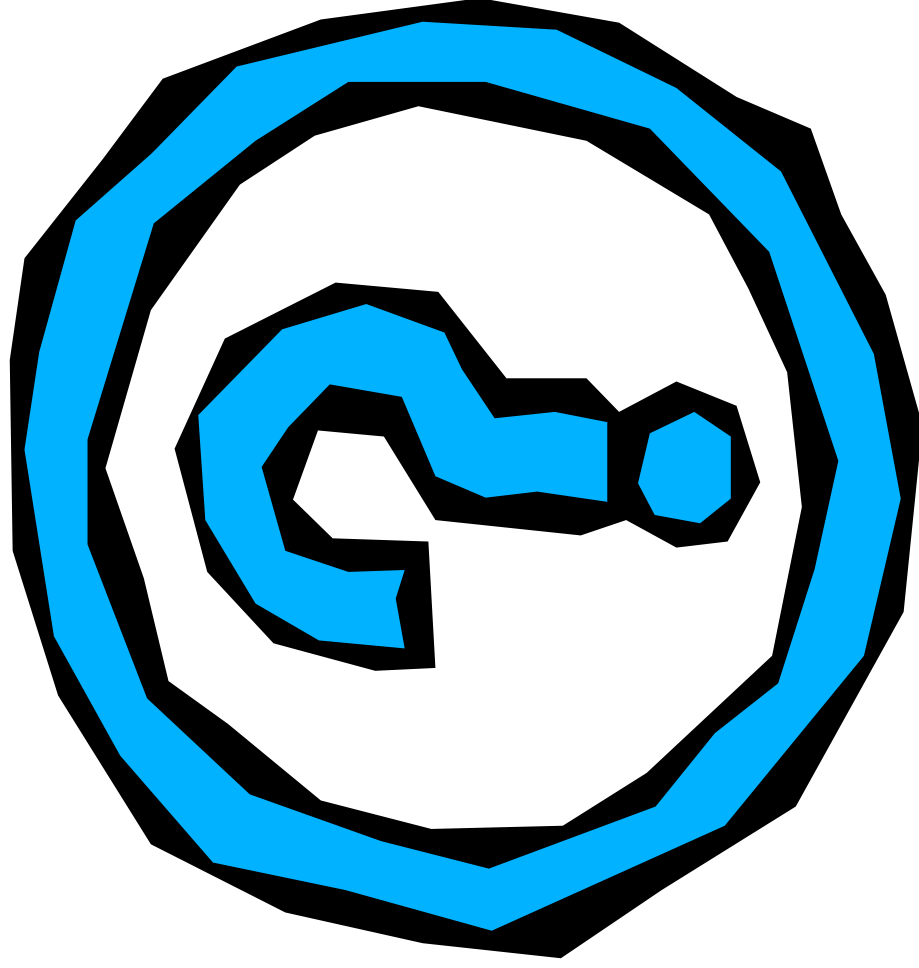
- **So now we've looked at VMware and the features it offers as well as the issues it brings to the capture and analysis table when working with malware.**
- **Networking has been covered in reasonable detail, as has managing snapshots and complete images.**
- **We've also looked at a small selection of tools that are extremely useful when analysing malware, 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 malware, 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 malware 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>

