

Robert Hensing
Software Security Engineer (SWI)
Microsoft Corporation

STRANGE (0-)DAYS

WHOAMI

- ▣ Robert Hensing
(rhensing@microsoft.com)
- ▣ 10 year Microsoft veteran
- ▣ SWI team member
- ▣ Prolific, insanely biased blogger
- ▣ Author of the Stealth chapter in latest Hacking Windows Exposed
- ▣ Vista x64 / Win7 user

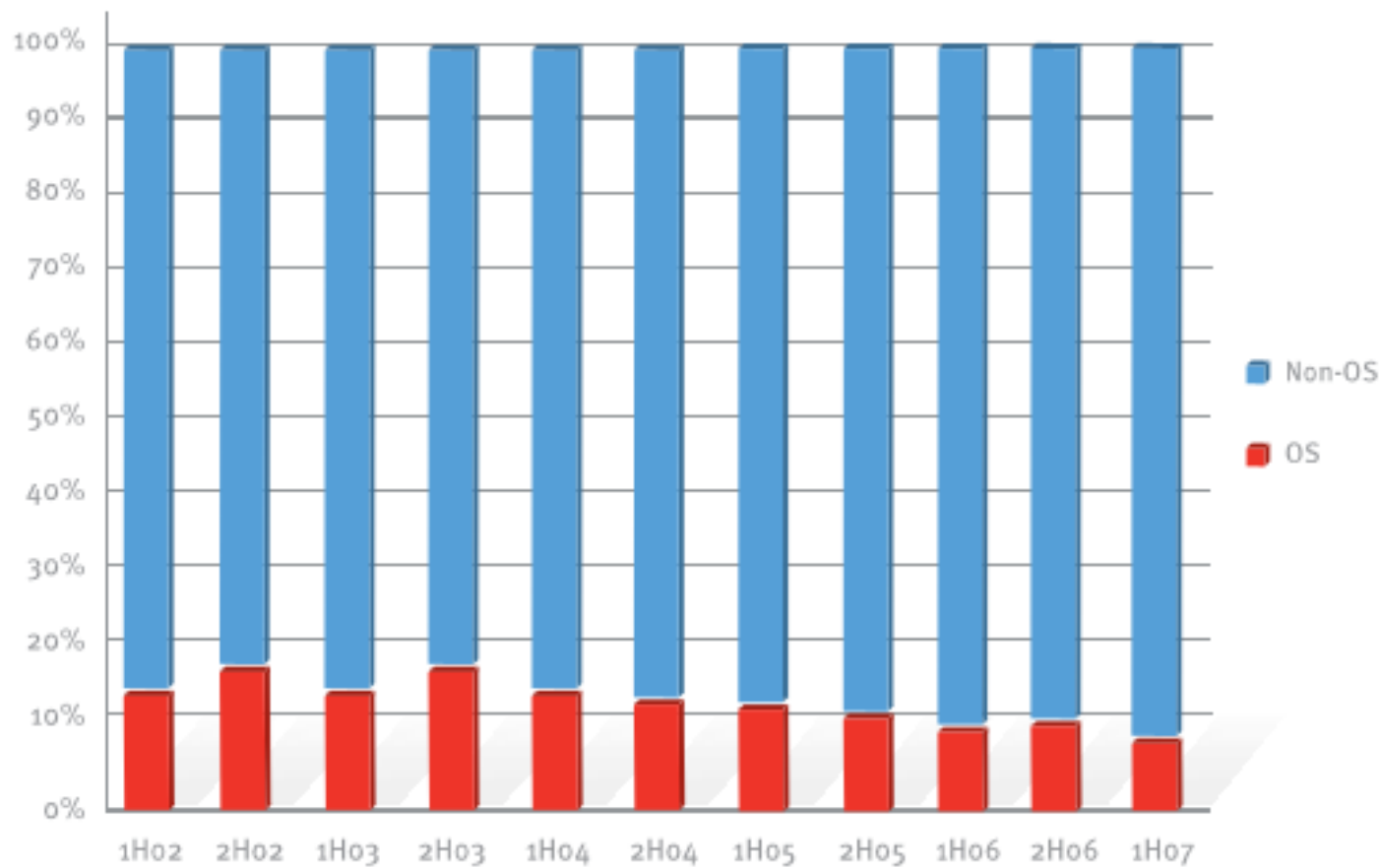
The Changing Threat Environment

An Increased Focus on Application Vulnerabilities

OPERATING SYSTEM VS. NON-OPERATING SYSTEM DISCLOSURES

To break down vulnerabilities into operating system (OS) and non-OS categories, all new vulnerabilities disclosed that affected Windows, Mac OS X, Unix, or the Linux kernel were grouped together into an “Operating System (OS)” category. This data was then used to calculate the percentage of total disclosed vulnerabilities that applied to operating systems. Figure 9 shows that a decreasing percentage of vulnerabilities are from operating systems.

FIGURE 9. OS versus non-OS vulnerabilities



Moving up the stack? Ya don't

- ▣ Microsoft has released 32 bulletins affecting Office 2003 SP2 and lower over the product's life.

- [Office 2003 RTM 11/17/2003](#)

- ▣ 0 bulletins in 2003
- ▣ 0 bulletins in 2004
- ▣ 0 bulletins in 2005
- ▣ 12 bulletins in 2006 ← Umm . . .
- ▣ 13 bulletins in 2007 ← WTF!?
- ▣ 7 bulletins so far in 2008 . . . And it's only March

Case Study

Targeted Attacks Using Microsoft Office Documents

The vulnerability

- ▣ Un-initialized stack variable vulnerability
 - Allocated on stack, not initialized before use
 - Prior stack allocations allow attacker to control the contents of memory backing this variable
 - ▣ Props for creative use of obscure vuln! 😊
- ▣ This led to a controlled arbitrary 4 byte write to memory.
- ▣ Attacker chose to overwrite a return address on the stack.
- ▣ Since it's not an overrun, it bypasses /GS!

Demo

Un-initialized stack variable code execution

How it went down . . .

- ▣ Victim(s) received a targeted e-mail with a malformed Excel document attached
- ▣ When opened the Excel document exploits a vulnerability to cause Excel to run some embedded shellcode
- ▣ Shellcode extracts an embedded XOR'd well formed XLS file and EXE
 - Opens well-formed XLS in Excel
 - Executes the extracted EXE which then installs [a backdoor as a service](#) (no stealth!?)

Microsoft® Malware Protection Center

Threat Research and Response



TrojanDropper:Win32/Malf.gen

Summary

Analysis

Prevention

Recovery

Technical Information

TrojanDropper:Win32/Malf.gen is a generic detection of malware that drops additional malicious files.

While malicious files detected as TrojanDropper:Win32/Malf.gen may vary in their specific behavior, an example of the actions of one such 'variant' that was observed in the wild can be seen below:

Payload

Installs Additional Malware

When executed, this trojan drops the file <system folder>\netmlc.dll, and creates a service to load this DLL. This service has the following characteristics:

Display name (one of the following):

- Removable Storage Service
- Remote Access Manager
- Network Sharing Connection
- Smart Card Supply
- Network Logon Supply

Image path: <system folder>\svchost.exe -k netsvcs
Parameter: <system folder>\netmlc.dll

Note - <system folder> refers to a variable location that is determined by the malware by querying the Operating System. The default installation location for the System folder for Windows 2000 and NT is C:\Winnt\System32; and for XP and Vista is C:\Windows\System32.

The file, <system folder>\netmlc.dll, is detected as [Backdoor:Win32/Ponadr.A](#) by Microsoft AV solutions.

Additional Information

In mid-January 2008, Microsoft received reports from the wild that this specific example of TrojanDropper:Win32/Malf.gen was being installed in targeted attacks via the distribution of a specially crafted, malformed Excel file. The exploit code contained in the file (detected as [Exploit:Win32/Exec.gen](#)) attempts to exploit a vulnerability in Microsoft Office Excel. Please see ['Microsoft Security Advisory \(947563\)- Vulnerability in Microsoft Excel Could Allow Remote Code Execution'](#) for more information.

Search the Encyclopedia

GO

Latest Definition Updates

Windows Defender
Antispyware: v1.29.7920.0

- ▶ 32 bit
- ▶ 64 bit
- ▶ [Information on updating Defender](#)

Microsoft Forefront Client Security
Antivirus: v1.29.7919.0
Antispyware: v1.29.7919.0

- ▶ 32 bit
- ▶ 64 bit
- ▶ [Information on updating FCS](#)

Severity

- High
 Medium
 Low

Glossary

[View the Glossary](#)

Our response . . .

- ▣ Advisory [947563](#) was released 1/15/2008 when Microsoft became aware of a 0-day vulnerability in Excel being used in limited targeted attacks.
- ▣ Some (slightly) good news this time!
 - Office 2003 SP3
 - ▣ [RTM 9/18/2007](#) – Not Affected
 - Office 2007 SP0 & SP1
 - ▣ [RTM 1/27/2007](#) - Not affected
 - MOICE

The Security Bulletin

- ▣ [MS08-014](#) – March 2008
 - Addressed 7 vulnerabilities
 - The CVE-2008-0081 FAQ Section has some interesting information . . .

When this security bulletin was issued, had this vulnerability been publicly disclosed?

Yes. This vulnerability had been publicly disclosed when this security bulletin was originally issued. It has been assigned the Common Vulnerability and Exposure number [CVE-2008-0081](#). This vulnerability was first described in [Microsoft Security Advisory 947563](#).

When this security bulletin was issued, had Microsoft received any reports that this vulnerability was being exploited?

Yes. When this security bulletin was issued, Microsoft had received information that this vulnerability was being exploited.

Demo – Windows XPSP2 + Office 2003 SP2

Spear phishing for fun and profit

Observations on XP

Malicious XLS drops an EXE to %TEMP%

The EXE creates a '.tmp' file in users temp folder and

The malware creates a DLL in system32 and

The binaries are injected into SYSTEM processes

Requires regular user rights

Requires regular user rights

Requires admin rights

Requires admin rights

Windows Vista + Office 2003 SP2

**You're about to get
Own3d, Cancel or
Allow?**

Observations on Vista

Malicious XLS drops an EXE to %TEMP%

Requires regular user rights

The EXE creates a '.tmp' file in users temp folder and

Requires regular user rights

The malware creates a DLL in system32 and

Requires ~~admin~~ rights

The binaries are injected into SYSTEM processes

Requires ~~admin~~ rights

Mitigation Strategies

Reducing the Risk with Windows

Windows XP – Mitigations

▣ Standard User Accounts

- Greatly limits options for maintaining presence and achieving stealth.
- True security boundary

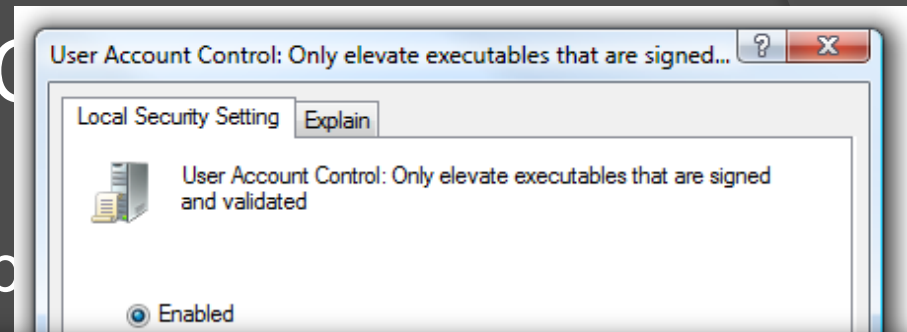
▣ Use Software Restriction Policies to drop the rights of high-risk applications

- DropMyRights.exe
 - ▣ <http://msdn2.microsoft.com/en-us/library/ms972827.aspx>
- Mentioned only for completeness – don't do this.

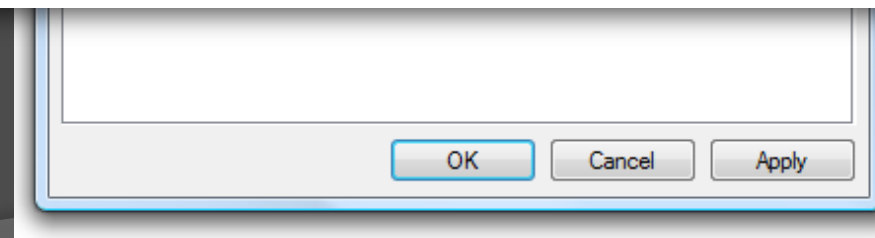
Windows Vista –

▣ Use Vista with UAC

- Default UAC is like
- ▣ Good compromise b



User Account Control: Admin Approval Mode for the Built-in Administrator account	Disabled
User Account Control: Allow UIAccess applications to prompt for elevation without using the secure desktop	Disabled
User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode	Prompt for consent
User Account Control: Behavior of the elevation prompt for standard users	Prompt for credentials
User Account Control: Detect application installations and prompt for elevation	Enabled
User Account Control: Only elevate executables that are signed and validated	Disabled
User Account Control: Only elevate UIAccess applications that are installed in secure locations	Enabled
User Account Control: Run all administrators in Admin Approval Mode	Enabled
User Account Control: Switch to the secure desktop when prompting for elevation	Enabled
User Account Control: Virtualize file and registry write failures to per-user locations	Enabled



Mitigation Strategies

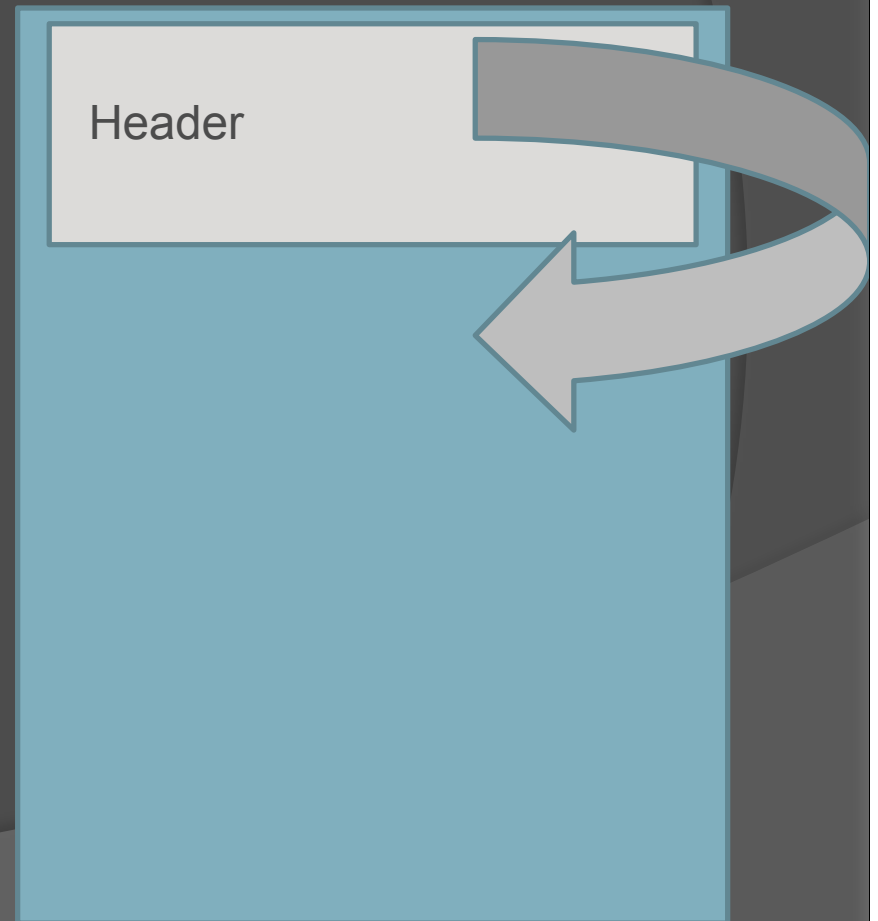
Reducing the Risk with Microsoft Office

A tale of two formats

Binary Office File Format vs. Open XML format

Office 2003 (and lower)

- ❑ OLE Structured Storage outer format
- ❑ File system within a file!
- ❑ Complex file format complete with
 - FAT Table
 - Sectors
 - Streams (like files)
- ❑ Another application specific inner format



Off

□ Sa

□ ZI

□ No

□ Re

WinZip Pro - CanSecWest - Targeted Attacks.zip

File Actions View Jobs Options Help

New Open Favorites Add Extract Encrypt View CheckOut Wizard View Style

Name	Type	Modified	Size	Ratio	Packed	Path
._rels	XML Docum...	1/1/1980 12:00 AM	738	65%	261	._rels\
[Content_Types].xml	XML Docum...	1/1/1980 12:00 AM	14,554	91%	1,270	
app.xml	XML Docum...	1/1/1980 12:00 AM	2,693	61%	1,060	docProps\
colors1.xml	XML Docum...	1/1/1980 12:00 AM	16,863	94%	1,041	ppt\diagrams\
colors2.xml	XML Docum...	1/1/1980 12:00 AM	16,863	94%	1,041	ppt\diagrams\
colors3.xml	XML Docum...	1/1/1980 12:00 AM	16,863	94%	1,041	ppt\diagrams\
colors4.xml	XML Docum...	1/1/1980 12:00 AM	16,863	94%	1,041	ppt\diagrams\
colors5.xml	XML Docum...	1/1/1980 12:00 AM	16,863	94%	1,041	ppt\diagrams\
core.xml	XML Docum...	1/1/1980 12:00 AM	700	48%	363	docProps\
data1.xml	XML Docum...	1/1/1980 12:00 AM	12,124	79%	2,559	ppt\diagrams\
data2.xml	XML Docum...	1/1/1980 12:00 AM	12,299	80%	2,437	ppt\diagrams\
data3.xml	XML Docum...	1/1/1980 12:00 AM	12,124	79%	2,553	ppt\diagrams\
data4.xml	XML Docum...	1/1/1980 12:00 AM	12,299	80%	2,440	ppt\diagrams\
data5.xml	XML Docum...	1/1/1980 12:00 AM	14,323	81%	2,717	ppt\diagrams\
handoutMaster1.xml	XML Docum...	1/1/1980 12:00 AM	4,504	68%	1,462	ppt\handoutMasters\
handoutMaster1.xml.rels	XML Docum...	1/1/1980 12:00 AM	292	36%	187	ppt\handoutMasters_rels\
image1.png	PNG Image	1/1/1980 12:00 AM	9,964	0%	9,964	ppt\media\
image10.png	PNG Image	1/1/1980 12:00 AM	28,983	0%	28,983	ppt\media\
image11.png	PNG Image	1/1/1980 12:00 AM	18,473	0%	18,473	ppt\media\
image2.png	PNG Image	1/1/1980 12:00 AM	18,837	0%	18,837	ppt\media\
image3.png	PNG Image	1/1/1980 12:00 AM	178,210	0%	178,210	ppt\media\
image4.png	PNG Image	1/1/1980 12:00 AM	13,576	0%	13,576	ppt\media\
image5.png	PNG Image	1/1/1980 12:00 AM	29,962	0%	29,962	ppt\media\
image6.png	PNG Image	1/1/1980 12:00 AM	19,897	0%	19,897	ppt\media\
image7.png	PNG Image	1/1/1980 12:00 AM	16,185	0%	16,185	ppt\media\
image8.png	PNG Image	1/1/1980 12:00 AM	25,003	0%	25,003	ppt\media\
image9.png	PNG Image	1/1/1980 12:00 AM	14,070	0%	14,070	ppt\media\
layout1.xml	XML Docum...	1/1/1980 12:00 AM	9,058	82%	1,588	ppt\diagrams\
layout2.xml	XML Docum...	1/1/1980 12:00 AM	7,296	79%	1,507	ppt\diagrams\
layout3.xml	XML Docum...	1/1/1980 12:00 AM	9,058	82%	1,588	ppt\diagrams\

Selected 0 files, 0 bytes Total 192 files, 1,121KB

ing

ver!

EXCEL.EXE:1212 Properties

User: XPSP2OFFICE2003\Admin
 SID: S-1-5-21-2156550803-811028645-1048832425-1003
 Session: 0

Group	Flags
BUILTIN\Administrators	Owner
BUILTIN\Users	Mandatory
Everyone	Mandatory
LOCAL	Mandatory
Logon SID (S-1-5-5-0-36687)	Mandatory
NT AUTHORITY\Authenticated Users	Mandatory
NT AUTHORITY\INTERACTIVE	Mandatory
XPSP2OFFICE2003\Debugger Users	Mandatory
XPSP2OFFICE2003\None	Mandatory

Group SID: Logon SID (S-1-5-5-0-36687)

Privilege	Flags
SeBackupPrivilege	Disabled
SeChangeNotifyPrivilege	Default Enabled
SeCreateGlobalPrivilege	Default Enabled
SeCreatePagefilePrivilege	Disabled
SeDebugPrivilege	Disabled
SeImpersonatePrivilege	Default Enabled
SeIncreaseBasePriorityPrivilege	Disabled
SeIncreaseQuotaPrivilege	Disabled

Permissions

OK Cancel

excelcnv.exe:1104 Properties

User: XPSP2OFFICE2003\Admin
 SID: S-1-5-21-2156550803-811028645-1048832425-1003
 Session: 0

Group	Flags
BUILTIN\Administrators	Deny, Owner
BUILTIN\Users	Mandatory, Restricted
BUILTIN\Users	Mandatory
Everyone	Mandatory, Restricted
Everyone	Mandatory
LOCAL	Mandatory
Logon SID (S-1-5-5-0-36687)	Mandatory, Restricted
Logon SID (S-1-5-5-0-36687)	Mandatory
NT AUTHORITY\Authenticated Users	Mandatory
NT AUTHORITY\INTERACTIVE	Mandatory
NT AUTHORITY\RESTRICTED	Mandatory, Restricted
S-1-5-21-994160850-51221711	Mandatory, Restricted
XPSP2OFFICE2003\Debugger Users	Deny, Mandatory
XPSP2OFFICE2003\None	Deny, Mandatory

Group SID: n/a


Privilege	Flags
SeChangeNotifyPrivilege	Default Enabled

Permissions

OK Cancel

Should be used with File document opening policy.

MOICE – Kid Tested, NSA

National Security Agency  **Central Security Service** Christopher Andrew Lecture

[Home](#) [About NSA](#) [Research](#) [Business](#) [Careers](#) [Public Info](#) [History](#)

Information Assurance  [For Academia](#) [For Industry](#) [For Government](#)
[Products](#) [Services](#) [Awards](#) [Events](#) [Glossary](#) [Links](#)

>>Security Configuration Guides [What's new?](#)







Products

- Security Configuration Guides
 - > All Current Security Guides
 - > Applications
 - > Database Servers
 - > Operating Systems
 - > Routers
 - > Supporting Documents
 - > Switches
 - > VoIP and IP Telephony
 - > Vulnerability Technical Reports
 - > Web Servers and Browsers
 - > Wireless
 - > Archived Security Guides

Overview

NSA initiatives in enhancing software security cover both proprietary and open source software, and we have successfully used both proprietary and open source models in our research activities. NSA's work to enhance the security of software is motivated by one simple consideration: use our resources as efficiently as possible to give NSA's customers the best possible security options in the most widely employed products. The objective of the NSA research program is to develop technologic advances that can be shared with the software development community through a variety of transfer mechanisms. NSA does not favor or promote any specific software product or business model. Rather, NSA is promoting enhanced security.

What's New or Updated

-  [Video Teleconferencing](#) - 748KB
-  [The Microsoft Office Isolated Conversion Environment \(MOICE\) and File Block Functionality with Office 2003](#) - 65KB
-  [A Deployment Guide for the Microsoft Office Isolated Conversion Environment \(MOICE\) and File Block Functionality with Office 2003](#) - 225KB
-  [Internet Protocol version 6 Factsheet](#) - 82KB
-  [Port Security on Cisco Access Switches Factsheet](#) - 82KB
-  [Microsoft® Office Groove® Security Architecture](#) - 768KB
-  [How to Secure a Groove Manager Web Site](#) - 148KB

* To view documents stored as Portable Document Format (PDF) files your local computer must have the [Adobe Acrobat Reader 5.0](#), or later, application or a Web browser plug-in that supports the PDF file format.

Examining last year's file . . .

- ▣ Requires a hex editor + expert knowledge
 - Interesting strings in a stream near the beginning of the malicious files!

0690h:	45 19 45 19	45 19 45 19	02 00 00 00	24 0A 01 00	E.E.E.E.....\$...
06A0h:	0B 00 00 00	00 0A 01 00	63 6D 64 20	2F 63 20 73cmd /c s
06B0h:	74 61 72 74	20 75 70 64	61 74 65 2E	65 78 65 00	tart update.exe.
06C0h:	4D 5A 50 00	02 00 00 00	04 00 0F 00	FF FF 00 00	MZP.....
06D0h:	B8 00 00 00	00 00 00 00	40 00 1A 00	00 00 00 00@.....
06E0h:	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00
06F0h:	00 00 00 00	00 00 00 00	00 00 00 00	00 01 00 00
0700h:	BA 10 00 0E	1F B4 09 CD	21 B8 01 4C	CD 21 90 90!...L!...
0710h:	54 68 69 73	20 70 72 6F	67 72 61 6D	20 6D 75 73	This program mus
0720h:	74 20 62 65	20 72 75 6E	20 75 6E 64	65 72 20 57	t be run under W
0730h:	69 6E 33 32	0D 0A 24 37	00 00 00 00	00 00 00 00	in32..\$7.....
0740h:	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00

- ▣ What could possibly go wrong?

Example file

- ▣ Still exp
- Th wi

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	0123456789ABCDEF
1:FC90h:	33	33	33	33	33	33	33	33	33	33	33	33	33	33	E3	FC	3333333333333333..
1:FCA0h:	22	D3	92	82	29	D2	33	33	33	33	33	33	33	33	33	33	"...).3333333333
1:FCB0h:	33	33	33	33	33	33	0D	33	30	33	CD	CC	3A	33	35	33	333333.303...353
1:FCC0h:	33	33	33	33	33	33	33	33	33	33	32	33	33	33	2D	33	333333333332333-3
1:FCD0h:	33	33	33	33	33	33	33	23	33	33	CD	CC	CC	CC	33	33	33333333#33....33
1:FCE0h:	33	33	CD	CC	CC	CC	33	33	33	33	2E	33	33	33	CC	CC	33....3333.333..
1:FCF0h:	CC	CC	CC	CC	CC	CC	CC	CC	CC	CC	CC	CC	CC	CC	CC	CC
1:FD00h:	CC	CC	CC	CC	CC	CC	CC	CC	CC	CC	CC	CC	CC	CC	CC	CC
1:FD10h:	CC	CC	CC	CC	CC	CC	CC	CC	CC	CC	CC	CC	CC	CC	CC	CC
1:FD20h:	CC	CC	CC	CC	CC	CC	CC	CC	CC	CC	CC	CC	CC	CC	CC	CC
1:FD30h:	CC	CC	CC	CC	CC	CC	CC	CC	CC	CC	CC	CC	CC	CC	CC	CC
1:FD40h:	CC	CC	CC	CC	CC	CC	CC	CC	CC	CC	CC	CC	CC	CC	CC	CC
1:FD50h:	CC	CC	CC	CC	CC	CC	CC	CC	CC	CC	CC	CC	CC	CC	CC	CC
1:FD60h:	CC	CC	CC	CC	CC	CC	CC	CC	CC	CC	CC	CC	CC	CC	CC	CC
1:FD70h:	CC	CC	CC	CC	CC	CC	CC	CC	CC	CC	CC	CC	CC	CC	CC	CC
1:FD80h:	CC	CC	CC	CC	CC	CC	CC	CC	CC	CC	CC	CC	CC	CC	CC	CC
1:FD90h:	CC	CC	CC	CC	CC	CC	CC	CC	CC	CC	CC	CC	CC	CC	CC	CC
1:FDA0h:	CC	CC	CC	CC	CC	CC	CC	CC	CC	CC	CC	CC	CC	CC	CC	CC
1:FDB0h:	CC	CC	CC	CC	CC	CC	CC	CC	CC	CC	CC	CC	CC	CC	CC	CC
1:FDC0h:	CC	CC	CC	CC	CC	CC	CC	CC	CC	CC	CC	CC	CC	CC	CC	CC
1:FDD0h:	CC	CC	CC	CC	CC	CC	CC	CC	CC	CC	CC	CC	CC	CC	CC	CC
1:FDE0h:	CC	CC	CC	CC	CC	CC	CC	CC	CC	CC	CC	CC	CC	CC	CC	CC
1:PDF0h:	CC	CC	CC	CC	CC	CC	CC	CC	CC	CC	CC	CC	CC	CC	CC	CC
1:FE00h:	CC	CC	CC	CC	CC	CC	CC	CC	CC	CC	CC	CC	CC	CC	CC	CC
1:FE10h:	CC	CC	CC	CC	CC	CC	CC	CC	CC	CC	CC	CC	CC	CC	CC	CC
1:FE20h:	CC	CC	CC	CC	CC	CC	CC	CC	CC	CC	CC	CC	CC	CC	CC	CC
1:FE30h:	CC	CC	CC	CC	CC	CC	CC	CC	CC	CC	CC	CC	CC	CC	CC	CC
1:FE40h:	CC	CC	CC	CC	CC	CC	CC	CC	CC	CC	CC	CC	CC	CC	CC	CC
1:FE50h:	CC	CC	CC	CC	CC	CC	CC	CC	CC	CC	CC	CC	CC	CC	CC	CC
1:FE60h:	CC	CC	CC	CC	CC	CC	CC	CC	CC	CC	CC	CC	CC	CC	CC	CC
1:FE70h:	CC	CC	CC	CC	CC	CC	CC	CC	CC	CC	CC	CC	CC	CC	CC	CC
1:FE80h:	CC	CC	CC	CC	CC	CC	CC	CC	CC	CC	CC	CC	CC	CC	CC	CC
1:FE90h:	CC	CC	CC	CC	CC	CC	CC	CC	CC	CC	CC	CC	CC	CC	3A	3B;
1:FEA0h:	23	33	33	35	36	33	8B	2C	FE	34	F2	F3	33	33	35	30	#33563.,.4..3350
1:FEB0h:	33	33	D2	33	31	33	83	37	F2	33	31	33	33	33	D1	33	33.313.7.31333.3
1:FEC0h:	33	33	6F	33	43	33	36	33	33	72	57	5E	5A	5D	13	13	33o3C3633rW^Z]..
1:FED0h:	13	13	13	13	13	13	13	13	13	13	13	13	13	13	13	13
1:FEE0h:	13	13	13	13	13	13	13	13	13	13	13	13	13	13	13	13
1:FEF0h:	13	13	13	13	13	13	13	13	13	13	13	13	13	13	13	13
1:FF00h:	13	13	13	13	13	13	13	13	13	13	13	13	13	13	13	13
1:FF10h:	13	13	13	13	13	13	13	13	13	13	13	13	13	13	13	13

re
w

Better Together

File Block

MOICE

Standard User / UAC

UAC "Dark Roast"

Demo – Excel 0-day vs. MOICE

0-Day Fail

Soooo . . . that's it?!

**Where do we go from
here?**

Be On The Lookout

- Increasingly sophisticated social engineering attacks involving attachments!
 - ⌘ Unexpected documents delivered via spoofed emails
- Suspicious application 'crashes'
 - ⌘ Always look for 'Office Watson' when Office crashes
 - Did you see it in my demonstration?
 - ⌘ Check for an audit trail
 - Even Log data (or lack thereof)
 - ⌘ When investigating suspicious Office documents – always grab them from the original e-mail (save the e-mail message as a .MSG file via File->Save as)

Advice

- Keep up to date on security updates!
 - ⌘ This applies to non-Microsoft applications as well. 😊
- Reduce your risk (mitigation strategies)
 - ⌘ Educate employees about targeted attacks
 - ⌘ Use Windows with standard user accounts
- Office 2003 & 2007
 - ⌘ If on Office 2003 - Deploy 2003 SP3 *immediately*
 - ⌘ Read the Office Security Guide
 - ⌘ Evaluate and Deploy MOICE + File Block
- Corporate Policy
 - ⌘ Require S/MIME signed emails?
 - ⌘ Deploy SenderID to reject spoofed emails at the edge?

Give us your 0-day

- ▣ 0-day is the spice of life!
- ▣ Please e-mail all 0-day to:
 - secure@microsoft.com
 - Cc: rhensing@microsoft.com
 - 😊

EOF

Appendix

Links

- Microsoft Office Isolated Conversion Environment (MOICE)
<http://support.microsoft.com/kb/935865>
- Plan Block File Format Settings in Office 2007
<http://technet2.microsoft.com/Office/en-us/library/fe3f431c-8d7a-45c8-954f-1268f3b533161033.mspx>
- Structured Storage File Format Specification
<http://aafassociation.org/html/specs/aafcontainerspec-v1.0.1.pdf>
- Office 2007 Open XML File Format
<http://msdn2.microsoft.com/en-us/library/aa338205.asp>

Links

- NSA Security Configuration Guides
<http://www.nsa.gov/snac/>
- Spear Phishing
http://www.microsoft.com/athome/security/email/spear_phishing.mspix
- Security Intelligence Report (Jan – June 2007)
<http://www.microsoft.com/security/portal/SIR.aspx>
- Results of Implementing the SDL
http://msdn2.microsoft.com/en-us/library/ms995349.aspx#sdl2_topic4
- David LeBlanc's Blog
http://blogs.msdn.com/david_leblanc/default.aspx

Links

- Restricted Tokens
[http://msdn2.microsoft.com/en-us/library/aa379316\(VS.85\).aspx](http://msdn2.microsoft.com/en-us/library/aa379316(VS.85).aspx)
- Practical Sandboxing Part 1
http://blogs.msdn.com/david_leblanc/archive/2007/07/27/practical-windows-sandboxing-part-1.aspx
- Practical Sandboxing Part 2
http://blogs.msdn.com/david_leblanc/archive/2007/07/30/practical-windows-sandboxing-part-2.aspx
- Practical Sandboxing Part 3
http://blogs.msdn.com/david_leblanc/archive/

Microsoft[®]

Your potential. Our passion.[™]

© 2007 Microsoft Corporation. All rights reserved. Microsoft, Windows, Windows Vista and other product names are or may be registered trademarks and/or trademarks in the U.S. and/or other countries.

The information herein is for informational purposes only and represents the current view of Microsoft Corporation as of the date of this presentation. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information provided after the date of this presentation.

Microsoft Confidential

MICROSOFT MAKES NO WARRANTIES, EXPRESS, IMPLIED OR STATUTORY, AS TO THE INFORMATION IN THIS PRESENTATION.