

Application of Win32 Executable File Infectors on Intel Itanium and AMD Opteron Based Win64 Systems

Oleg Petrovsky and Shali Hsieh
Computer Associates International Inc.
1 Computer Associates Plaza, Islandia, NY 11749,
USA

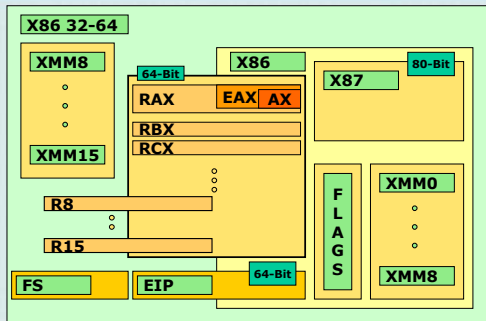
64-bit computing

- Legacy 64 bit platforms
- Benefits of 64-bit processors
- Increased integer dynamic range
- Much larger addressable memory space
- Benefits to database, scientific and cryptography applications

AMD Opteron 64

- Inbuilt 128-bit bus DDR memory controller with memory bandwidth speed up to 5.3GB/s.
- Use of hyper transport protocol, "glueless" architecture.
- Available in up to 8 way configuration with the clock speeds of 1.4 GHz, 1.6 GHz and 1.8 GHz .
- Reuses already familiar 32-bit x86 instruction set and extends it to support 64-bit operands, registers and memory pointers.

AMD64 Programming Model



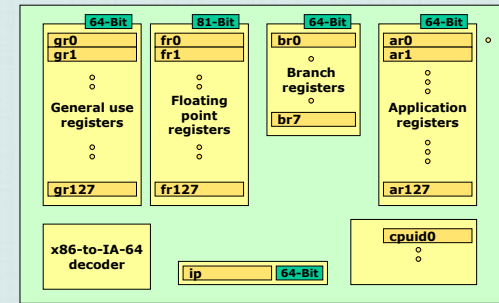
AMD64: Programming model

- Extends general use registers to 64-bit, adds additional eight general purpose 64-bit registers.
- Reuses x86 instruction set.
- Runs 32-bit code without emulation or translation to a native instruction set.
- Minimizes learning curve.

Intel Itanium 64

- 64 bit Itanium line of processors is being developed by Intel
- Itanium - 800 MHz, no on die L3 cache, Itanium 2 - 1GHz, 3MB L3 on die, Itanium 2003 (Madison) - 1.5 GHz, 6MB L3 on die cache, 410M transistors, largest integration on a single silicon crystal today.
- Itanium line of processors utilizes more efficient and robust than legacy x86 instruction set architecture
- Itanium has to use x86-to-IA-64 decoder a specifically tailored to x86 on chip emulator
- EPIC instruction set architecture

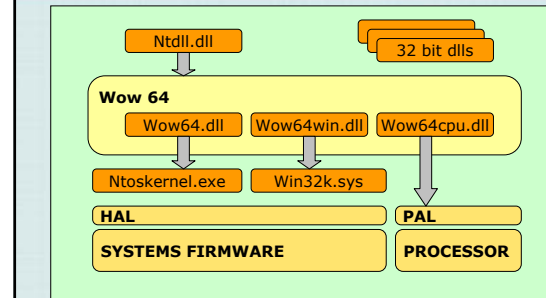
IA64 Programming model



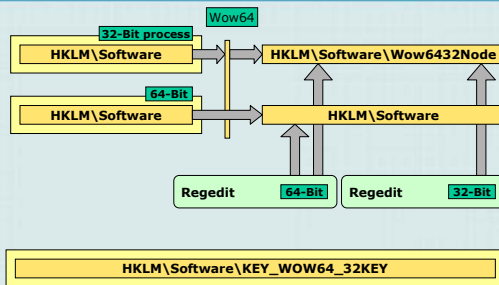
32-bit application support

- Windows on Windows 64 (WoW64), an abstraction layer between 64 bit executing environment and 32 bit processes.
- Wow64 consists of Wow64.dll, Wow64win.dll, Wow64cpu.dll
- Wow64 intercepts and emulates system calls made by 32 bit applications in user mode
- Wow64 prevents files and registry collisions
- 32 and 64 bit dlls are stored separately, 32 bit application can only load 32 bit dlls as well as 64 bit application can only load 64 bit dlls.

32-bit application support (cont.)



Registry Redirector



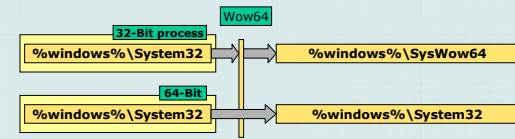
Registry Reflector

- Wow64 synchronizes certain registry keys to allow 64 and 32 bit programs connectivity through COM
- Registry keys which are affected:
 - HKLM\Software\Classes
 - HKLM\Software\Microsoft\COM3,
 - HKLM\Software\Microsoft\OLE,
 - HKLM\Software\Microsoft\EventSystem
 - HKLM\Software\Microsoft\RPC
- During the synchronization the keys information may be modified to reflect differences between 64 and 32 bit environments

File System Redirector

- Most of the file names of 64 bit Windows dlls are identical to their 32 bit implementation
- Wow64 redirects %windows%\system32 to %windows%\syswow64 for 32 bit applications
- File system redirection mechanism separates 64 and 32 bit dlls for the use by 64 and 32 bit applications respectively

File System Redirector (cont.)



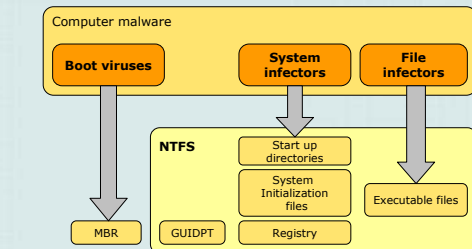
Interprocess communications

- Name object such as mutexes, semaphores and file handles can be shared between 64 and 32 processes
- Handles to windows can be shared (HWND)
- RPC calls can be issued from 32 bit process to 64 bit and vice versa
- COM local services can be shared
- CreateProcess and ShellExecute can launch 64 bit or 32 bit processes from within either 64 or 32 bit process

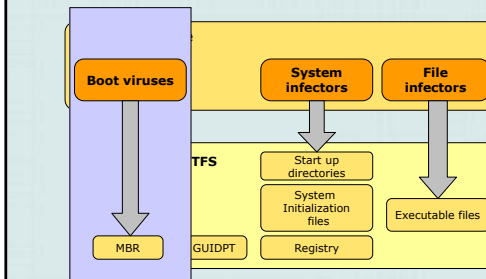
PE vs. PE+

Machine signature	+0x0	'P','E','\0','\0'	+0x0	Machine signature
Machine signature	+0x4	0x14C0x200	+0x4	Machine signature
Optional header size	+0x14	0xE0 0xF0	+0x14	Optional header size
Optional header signature	+0x18	0x10B0x20B	+0x18	Optional header signature
Base of data	+0x30		+0x30	Image Base
Image Base	+0x34			
Size of stack reserve	+0x60		+0x60	Size of stack reserve
Size of stack commit	+0x64			
Size of heap reserve	+0x68		+0x68	Size of stack commit
Size of heap commit	+0x6C			
Loader flags	+0x70		+0x70	Size of heap reserve
			+0x78	Size of heap commit
			+0x80	Loader flags

Virus Threats on Windows 64



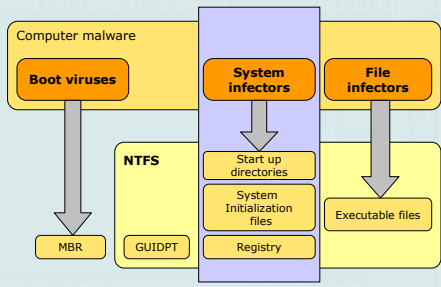
MBR Infection



MBR Infection

- GPT disk have a protective MBR sitting in the sector 0 preceding the GPT partition
- The GPT disk will appear as an MBR disk with possibly unrecognized partition instead of being appearing as unformatted
- The MBR is not used during the boot process of the Windows system
- MBR viruses will not be able to propagate since the viral code will not be loaded and run during the GPT boot

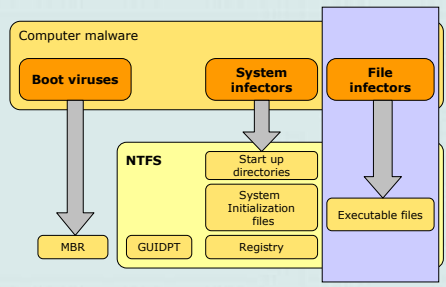
System Infection



System Infection (Trojan/Worm)

- Copying itself to a designated location
- Applying changes to the system registry run keys settings
- Inserting references to its code inside win.ini or system.ini files
- Copying itself in to the system startup folders
- Modifying or substituting a program, that runs on every boot by the OS, to run the malicious code
- Change associations to a known file types
- Install itself as a NT service

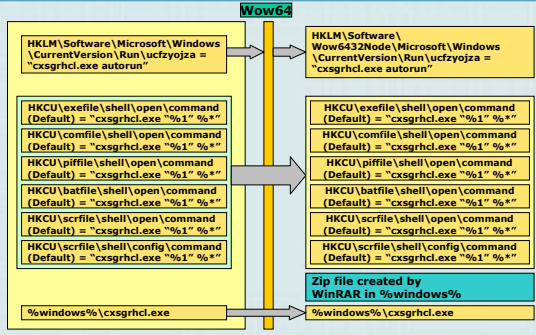
File Infection



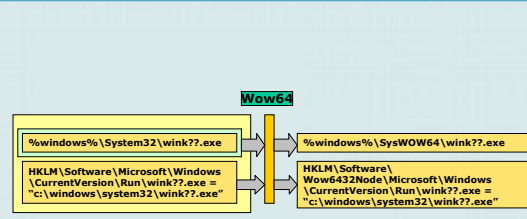
File Infection (Cont.)

- Attaching viral code to the beginning of the executable image, original PE file is not modified.
- Overwriting an original file, the original code is not preserved.
- Overwriting an original code preserving the original code in a file stream
- Modifying the PE+ header of an original file to point to viral code embedded in the file.
- Using entry point obfuscation methods.

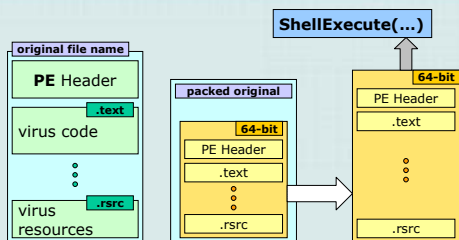
Win32.Swen.A



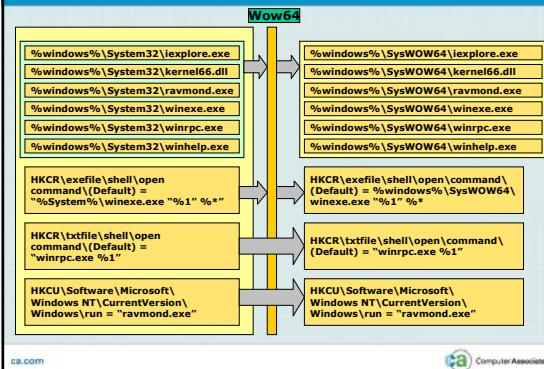
Win32.Klez.H



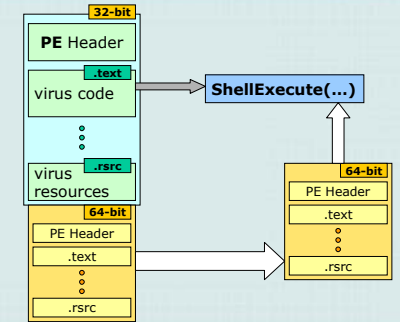
Win32.Klez.H File Infection



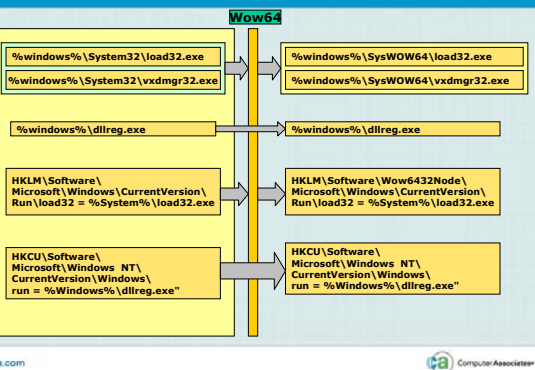
Win32.Lovgate.J



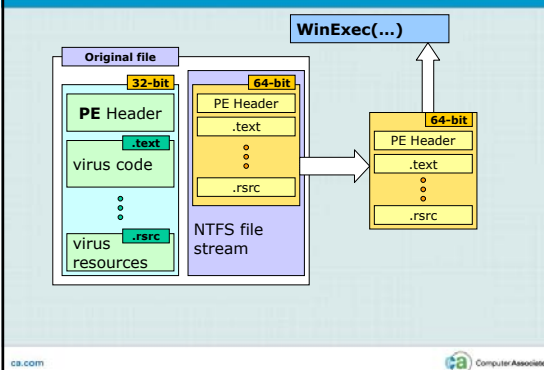
Win32.Lovgate.J File Infection



Win32.Dumaru.A



Win32.Dumaru.A File Infection



Win32.Valla.2048

- Search for .EXE extension
- Check PE signature
- Add a new section named "XOR"
- The virus doesn't work on 64-bit Windows. In order to determine kernel32.dll memory address the virus code assumes kernel32.ExitProcess() address to be on the stack location 0x1c when called.
- The virus doesn't infect 64-bit executables, the virus code assumes the size of an optional PE header to be 0xe0 bytes long. The virus misses a location of a section table.

Conclusion

- Wow64 provides Win32 execution environment for 32 bit applications on 64-bit Windows.
- Wow64 registry redirection mechanism affects HKLM\Software tree. 32-bit programs registered in the run keys under HKLM\Software registry tree will not run during boot.
- Registry reflection mechanism will synchronize per machine copy of HKEY_CLASSES_ROOT located in HKLM\Software\Classes tree between 64 and 32-bit registry views. File extension association information affects both 64 and 32 bit registry views.

Conclusion (cont.)

- 32-bit processes can launch 64-bit applications using ShellExecute() or CreateProcess() functions.
- Viruses which assume optional header size to be 0xe0 will most probably not infect or will corrupt PE+ executables on infection
- Viruses which insert themselves into hosts PE+ structure by means of adding a new section or by means of injecting its code inside already existing sections will not work due to the 64 and 32-bit code mix-up.
- Most of the 32 bit AV software shouldn't have any problems dealing with 32 bit infections on 64-bit Windows.

Conclusion (cont.)

- The existing security vulnerability will carry over to the 64-bit Windows system. Exploiting security vulnerabilities usually requires specific memory address and the exploitable memory address will most likely be different between 32-bit and 64-bit Windows.

End of Presentation

- Questions?

Computer Associates
Virus Information Center
www.ca.com/virusinfo