

# 'Enhanced' Virus Protection

**Costin G. Raiu**

**Head of R&D, Kaspersky Lab, Romania**  
**<costin.raiu@kaspersky.ro>**

# *“Enhanced”?*

*"AMD Athlon 64 CPU Feature:*

- HyperTransport technology*
- Cool'n'Quiet technology*
- **Enhanced Virus Protection** for Microsoft Windows XP SP2"*

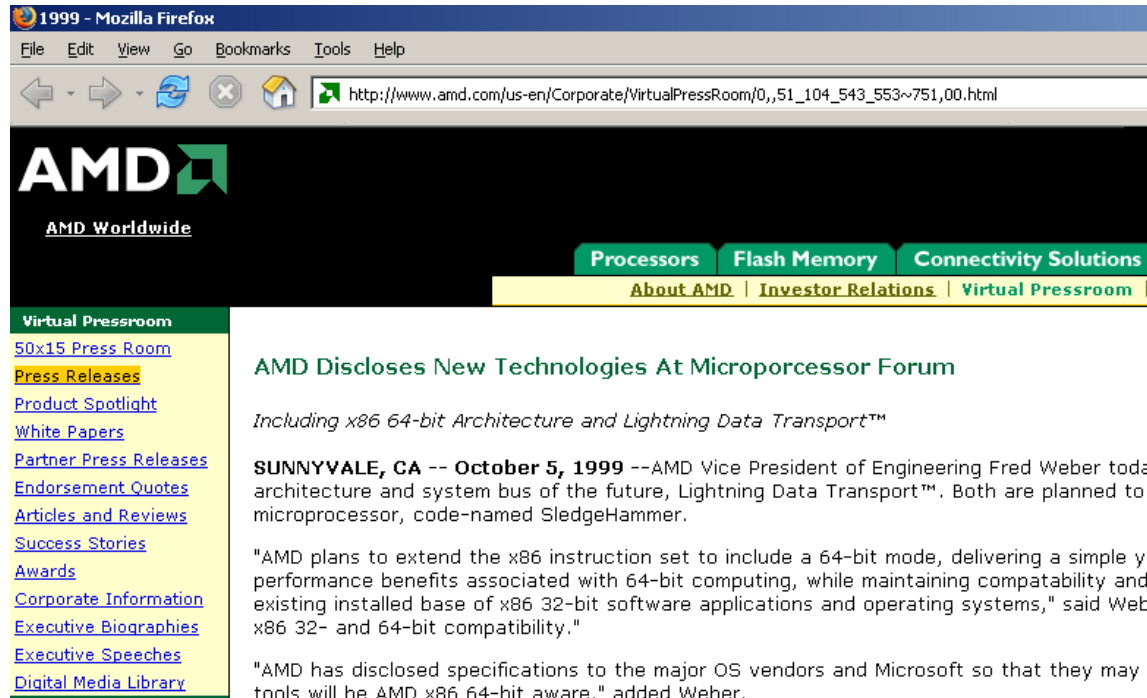
(a snippet from an AMD64 commercial)

# The AMD64 Marketing Campaign

- AMD, Intel put antivirus tech into chips  
[http://news.zdnet.com/2100-1009\\_22-5137832.html?tag=nl](http://news.zdnet.com/2100-1009_22-5137832.html?tag=nl)
- Holland Bans AMD's 'Virus Protection' Campaign  
<http://it.slashdot.org/it/04/12/29/0034228.shtml?tid=142&tid=172>
- AMD's "Enhanced Virus Protection" Radio Ads Banned in The Netherlands.  
<http://www.xbitlabs.com/news/other/display/20041227094638.html>
- AMD stopped from advertising NX flag as anti-virus cure  
<http://www.theinquirer.net/?article=20352>
- Reclame Code Commissie: radiospots Athlon 64 misleidend (dutch)  
<http://www.tweakers.net/nieuws/35463>

# October 5, 1999

## “AMD Discloses New Technologies At *Microprocessor Forum*”



1999 - Mozilla Firefox

File Edit View Go Bookmarks Tools Help

http://www.amd.com/us-en/Corporate/VirtualPressRoom/0,,51\_104\_543\_553~751,00.html

**AMD**  
AMD Worldwide

Processors Flash Memory Connectivity Solutions

About AMD | Investor Relations | Virtual Pressroom

Virtual Pressroom

- [50x15 Press Room](#)
- [Press Releases](#)
- [Product Spotlight](#)
- [White Papers](#)
- [Partner Press Releases](#)
- [Endorsement Quotes](#)
- [Articles and Reviews](#)
- [Success Stories](#)
- [Awards](#)
- [Corporate Information](#)
- [Executive Biographies](#)
- [Executive Speeches](#)
- [Digital Media Library](#)

### AMD Discloses New Technologies At Microprocessor Forum

*Including x86 64-bit Architecture and Lightning Data Transport™*

**SUNNYVALE, CA -- October 5, 1999** --AMD Vice President of Engineering Fred Weber today architecture and system bus of the future, Lightning Data Transport™. Both are planned to b microprocessor, code-named SledgeHammer.

"AMD plans to extend the x86 instruction set to include a 64-bit mode, delivering a simple yet performance benefits associated with 64-bit computing, while maintaining compatability and existing installed base of x86 32-bit software applications and operating systems," said Webe x86 32- and 64-bit compatibility."

"AMD has disclosed specifications to the major OS vendors and Microsoft so that they may er tools will be AMD x86 64-bit aware," added Weber.

# The new technologies

- AMD64 (also known as “x64”) is a full 64-bit computing architecture with several notable enhancements over x86-32
- The CPU can run in a native 64-bit mode with 32-bit and 16-bit VM’s, but also in a native 32-bit mode with 16-bit VM’s, as well as the “old” 16-bit real mode
- This allows compatibility with existing 32 bit operating systems, but also with 32-bit applications running from a 64-bit operating system
- The AMD64 architecture supports the new PAE memory addressing mode, as well as a new *Non-Executable* (NX) property for the memory pages

# Why is AMD64 important?

- The AMD64 architecture is an affordable way of getting the power of 64-bit computing into a desktop computer
- It is better (for the vast majority of users) than Intel's Itanium 2 architecture because it includes full hardware support for the x86-32 instruction execution
- It is already widely available on the market; Intel has a compatible platform called EM64T, built into the latest Pentium 4's (as of Feb 2004)
- The choice of native operating systems for the AMD64 / x64/ EM64T architecture is wide: Windows XP / 2003, Linux (Fedora, Debian, SuSE, etc...), FreeBSD, Solaris 10...

# 64-bit malware, 32-bit malware

- Fact: the AMD64 is most likely to become the dominant PC 64-bit architecture
- As it happens with every popular system, it will eventually become a target for malicious software
- At the same time, while the users are still running older 32-bit applications, x64 operating systems will also suffer from 32-bit malicious software
- The vast majority of new malware we receive is (still) 32-bit viruses/trojans/backdoors
- In the beginning, operating systems for x64 will mostly suffer (or not?) from 32-bit malicious software

# To summarize

# *x64*

- 64-bit computing on the x64 platform is affordable and backwards-compatible
- The CPUs can also be used with 32-bit operating systems!
- Only 64-bit-aware operating systems can use the full potential of the architecture
- The extended memory address space of 1TB for the recent AMD64's and 64GB for recent Pentium IV's with EM64T opens up new possibilities for data intensive applications (eg. Databases)
- These machines are fast – it takes about 8 seconds to boot Windows XP Professional x64 on a regular AMD64 3200+754



# AMD64 vs Intel's EM64T

- EM64T supports the CMPXCHNG16B instruction in 64-bits, while current AMD64 CPUs do not
- Then, SYSCALL and SYSRET in 32-bits are supported by AMD64 but they are not supported by early EM64T models
- Additionally, SYSENTER and SYSEXIT in 64-bits are supported by EM64T but not by AMD64.
- Finally, LAHF and SAHF in 64 bits are only supported by early AMD64 models
- The “NX” bit vs the “XD” bit

# The NX bit

- Without doubt, the most interesting security feature available in the x64 architecture (and Intel's recent EM64 machines) is the Non-Executable (NX) bit
- The NX bit (63<sup>rd</sup> bit in the TT entries) can be set in the memory page translation tables to prevent code execution in the stack or from data pages
- The NX bit feature needs to be enabled by the OS by setting bit 11 the EFER – it is disabled by default in the CPU
- The NX bit method is not limited to the x64's 64-bit operating mode; it can also be used by PAE-aware 32-bit operating systems

# The NX bit, continued

- The NX bit is used by XP (Win32) SP2 if available (but not by Windows 2000, or older 9x'es)
- The NX bit is used by all x64 versions of Windows (XP Professional, 2003 Server)
- It can be enabled/disabled for specific programs, or it can be enabled/disabled system wide
- Recent Linux kernels are also NX-aware on both 32 and 64 bit x86
- The NX bit is enabled by default on Windows (XP SP2, x64) and Linux, if available

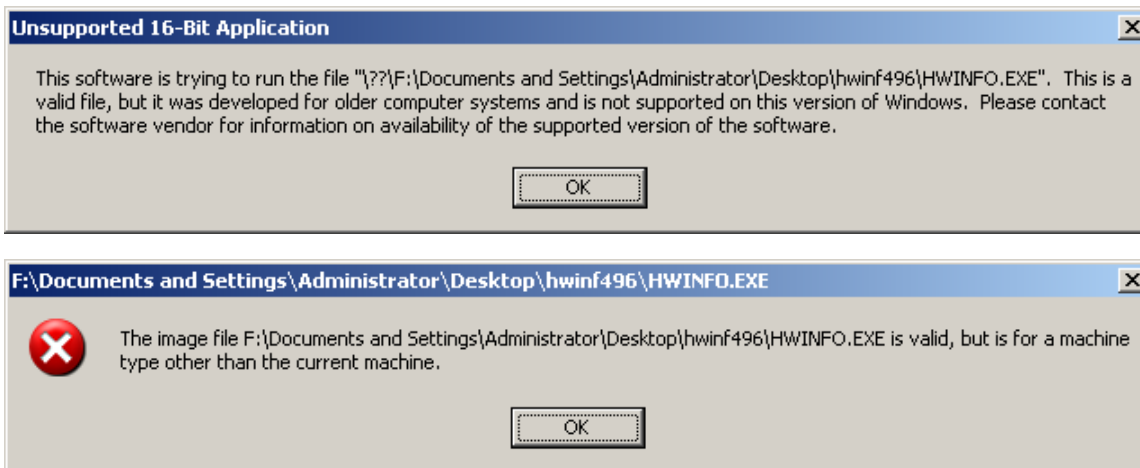
# Windows x64

- To take advantage of all the new features of the x64 computing platform (read: larger memory, more registers), a 64-bit operating system is required
- Windows XP Professional x64 bit Edition supports 32 and 64-bit applications; it does not run 16 bit applications though (bye bye older MSDOS apps!)
- 32-bit applications run via WOW64
- The system files and the drivers are all 64-bit native code
- 32-bit drivers can't work in these OSes

# Windows *x64*, continued

- The %system% folder is called “system32” ☺
- The WOW64 system folder is called “syswow64”
- In addition to “Program Files” there is a “Program Files (x86)” folder where older 32 bit applications get installed
- The API 32-to-64 translation is done by two important DLL's:
  - Wow64.dll – core emulation and thunks for kernel
  - Wow64Win.dll – thunks for Win32k.sys entry-points

# Running 16 bit code / tools in Windows *x64* – bad luck!



# NX protection, Windows, Linux



```
Jun 7 18:34:40 localhost kernel: simple[6594]: segfault at 0000000005008e0  
rip 0000000005008e0 rsp 00007fffffff9a8 error 15
```

# A special “feature”

- Has been discovered by Yury Mashevsky, KL Moscow
- NTDLL.dll: `_LdrpCheckNXCompatibility@4`
- ...further calling `_LdrpCheckNxIncompatibleDllSection@4`



# NTDLL.dll in x64 Windows

```
7DA3CC37 6A 08          push      8
7DA3CC39 68 BC CB A3 7D  push      offset a_aspack
7DA3CC3E 56             push      esi
7DA3CC3F E8 1C 1E 05 00  call     strncmp
7DA3CC44 8B D8          mov       ebx, eax
7DA3CC46 83 C4 0C       add       esp, 0Ch
7DA3CC49 85 DB          test      ebx, ebx
7DA3CC4B 74 29          jz        short loc_7DA3CC76
7DA3CC4D 6A 06          push     6
7DA3CC4F 68 C4 CB A3 7D  push     offset a_pcle
7DA3CC54 56             push     esi
7DA3CC55 E8 06 1E 05 00  call     strncmp
7DA3CC5A 8B D8          mov       ebx, eax
7DA3CC5C 83 C4 0C       add       esp, 0Ch
7DA3CC5F 85 DB          test      ebx, ebx
7DA3CC61 74 13          jz        short loc_7DA3CC76
7DA3CC63 6A 08          push     8
7DA3CC65 68 CC CB A3 7D  push     offset a_sforce
7DA3CC6A 56             push     esi
7DA3CC6B E8 F0 1D 05 00  call     strncmp
```

- ...checking if one of the sections in the PE file is named “.aspack”, “.pcle” or “.sforce”

# A special “feature”, continued

- If any of the sections in the PE file is called “.aspack”, “.pcle” or “.sforce”, NTDLL calls `ZwSetInformationProcess` with a certain set of flags
- This results in disabling the NX (DEP) protection for the `_entire_process`
- All 32-bit programs packed by ASPack do not benefit from the hardware DEP in Windows, even if enabled and enforced by the system!
- Same is true about applications protected by StarForce, or those with “.pcle” sections

## 32-bit threats in x64 Windows

32-bit viruses in *x64* Windows:

- Win32/Xorala.A
- Win32/Funlove.4099
- Win32/Parite.B

32-bit rootkits:

- Win32/HackDef
- Win32/NTRootKit.040
  - Win32/Hider.C

# Win32/Xorala

- Simple direct action parasitic infector
- First reported ItW in July 2003
- Still out there (Smallpot)
- When run on Win x64 it gracefully crashes:

```
00413008 E8 00 00 00 00      call    $+5
0041300D 5F                      pop     edi
0041300E 81 EF 0D 00 00+       sub     edi, 0Dh
00413014 8B 87 D0 05 00+       mov     eax, [edi+5D0h]
0041301A 89 87 CC 05 00+       mov     [edi+5CCh], eax
00413020 8B 74 24 1C           mov     esi, [esp+1Ch]
00413024 81 E6 00 F0 FF+       and     esi, 0FFFFFF00h
0041302A
0041302A                      loc_41302A:
0041302A 66 81 3E 4D 5A       cmp     word ptr [esi], 5A4Dh
0041302F 74 08                jz     short loc_413039
00413031 81 EE 00 10 00+       sub     esi, 1000h
00413037 EB F1                jmp     short loc_41302A
```

## Win32/Xorala - continued

- In the WOW64 system, kernel32.dll has a special structure
- The first section starts at 0x7DBE0000 but the image is based at 0x7DBD0000
- There is a gap between the end of the header and the first segment, which is non-allocated memory
- Access to the memory pages between the end of the PE header and the first section causes an exception

# Win32/Funlove.4099

- Funlove uses a tricky method to receive control during system start; it registers itself as a service; “Flcss.exe” in the Windows System directory
- It attaches itself to the end of the last section of the PE files, which usually is a *DATA* section
- NX pops in and prevents its execution
- Even if the last section is marked executable, Funlove expects the ExitThread handler from stack to point to certain addresses
- Compares the ExitThread handle to 0xBFF00000, 0x77F00000 and 0x77E00000

# Win32/Parite.B

- It is a parasitic virus composed of a dropper written in assembler and the main virus body in C, ~176K
- When executed, the dropper creates the main virus body in the Windows temp directory and attempts to inject the 32-bit DLL file into the “Explorer.exe” process
- Of course, this fails – Explorer is a 64-bit native application

# Win32/HackDef

- It is an open source rootkit with lots of features
- It is based on a 32 bit driver ☺
- ...which of course doesn't load in Windows x64
- HackDef is effective per-process, via API hooking; but the stealth is visible from other 32 bit processes or any 64 bit process



# Win32/Hider.C

- It is a simple rootkit which patches the Windows API to perform stealthing operations
- Hider.C tries to execute code from a data segment (antidebugging)



# 32-bit viruses on x64 Windows

- The more complex and tricky, the less likely to still be able to run on x64
- A good degree of protection exists between the 32-bit and 64-bit OS layers
- It is of course, open to new, targeted 32-bit and 64-bit code attacks
- The NX protection is disabled by the OS transparently in some cases, leaving the system vulnerable to BOF attacks
- The x64 Windows platform is indeed more secure against 32-bit viruses
- *Enhanced Virus Protection? Yes.*

Thanks!

<costin.raiu@kaspersky.ro>