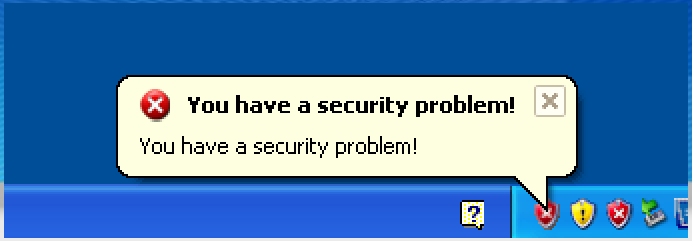
# Recent Rogueware



You have a security problem!

You have a security problem!

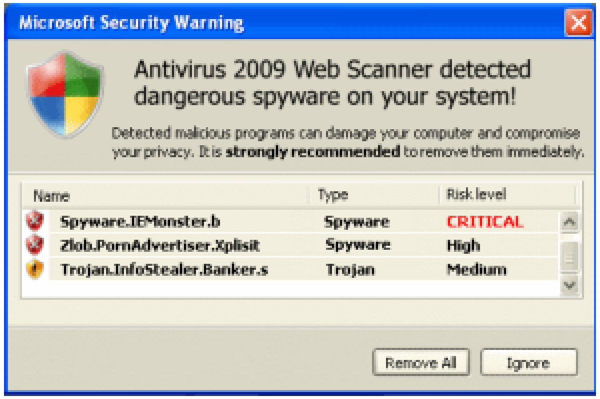
Kurt Baumgartner

PC Tools ThreatFire Research

Virus Bulletin 2008

# Recent Rogueware

- Rogueware?
- Obfuscation Methods and Vundo Behaviors
- Survey Multiple Recent Rogueware
- MonaRonaDona Hoax
- Recent Binder and Downloader Components and Behavioral Challenges
- What Now?



Antivirus 2009 Web Scanner detected dangerous spyware on your system!

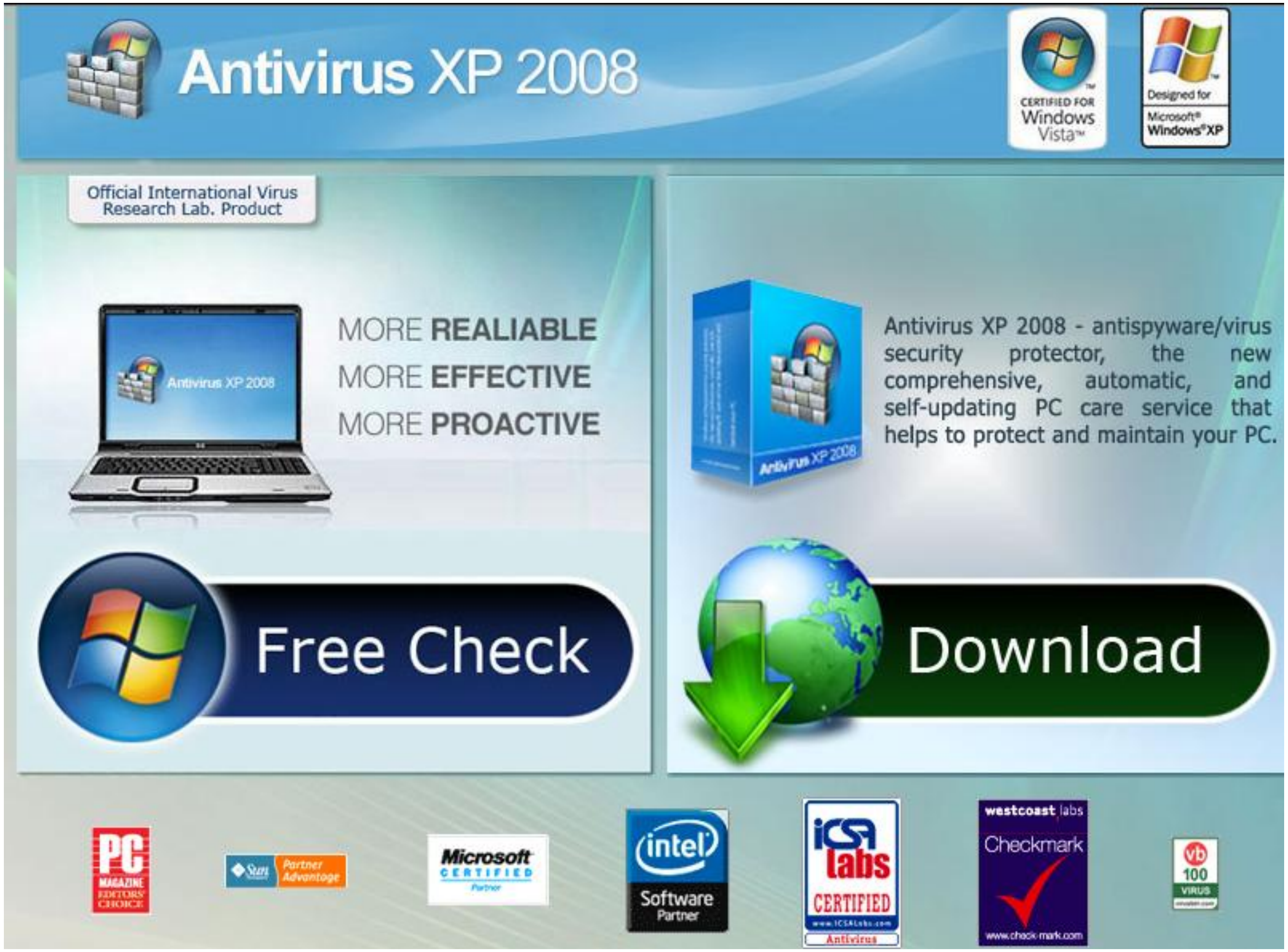
Detected malicious programs can damage your computer and compromise your privacy. It is **strongly recommended** to remove them immediately.

| Name | Type | Risk level |
|---|---|---|
| Spyware.IEMonster.b | Spyware | CRITICAL |
| Zlob.PornAdvertiser.Xplisit | Spyware | High |
| Trojan.InfoStealer.Banker.s | Trojan | Medium |

# Rogueware?

- Sometimes clumsy descriptions found on sites and blogs.
- Substantial definitions exist on well known sites like castlecops, spywarewarrior, and many others
- My definition: Rogueware-based schemes coerce computer users to pay for removal of nonexistent malware. **Rogueware are select software components used in these schemes to aid in coercion.**

# Rogueware Certifed



Antivirus XP 2008

Official International Virus Research Lab. Product

MORE **REALIABLE**
MORE **EFFECTIVE**
MORE **PROACTIVE**

Antivirus XP 2008 - antispyware/virus security protector, the new comprehensive, automatic, and self-updating PC care service that helps to protect and maintain your PC.

CERTIFIED FOR Windows Vista
Designed for Microsoft® Windows®XP
Antivirus XP 2008
Antivirus XP 2008
Free Check
Download
PC MAGAZINE EDITORS' CHOICE
Sun Partner Advantage
Microsoft CERTIFIED Partner
intel Software Partner
ICSA labs CERTIFIED www.ICSALabs.com Antivirus
westcoast labs Checkmark www.check-mark.com
vb 100 VIRUS

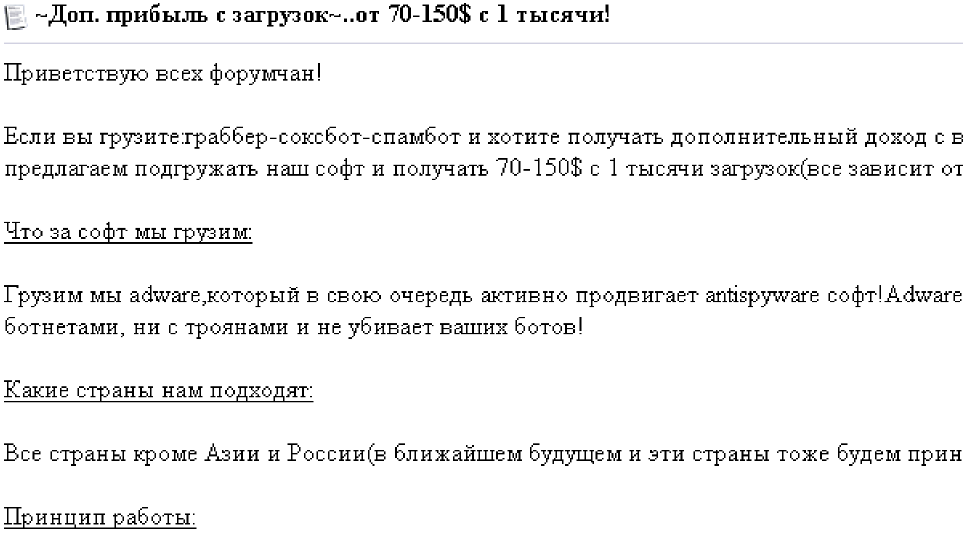
# Rogueware?

- Recent active and prevalent examples over the past couple of weeks
  - AntiVirus2008 and 2009
  - MultyCodecUpdr.7.2068.exe and its “promom [illegible] which then drops sav components
  - pdf sploit -> 0xf9.exe -> AntiVirus2008, other adware

- not-so-recent MonaRonaDona and Unigray Antivirus

# Rogueware?

- Shameless re branding, shuffling of domains, redistribution, shock messaging
- Towards the end of last year, high level of active distribution channels and offers:



**~Доп. прибыль с загрузок~..от 70-150$ с 1 тысячи!**

Приветствую всех форумчан!

Если вы грузите:граббер-соксбот-спамбот и хотите получать дополнительный доход с в
предлагаем подгружать наш софт и получать 70-150$ с 1 тысячи загрузок(все зависит от

Что за софт мы грузим:

Грузим мы adware,который в свою очередь активно продвигает antispyware софт!Adware
ботнетами, ни с троянами и не убивает ваших ботов!

Какие страны нам подходят:

Все страны кроме Азии и России(в ближайшем будущем и эти страны тоже будем прин

Принцип работы:

# Rogueware?

~ Extras. Profit from downloads ~ .. from 70-150 $ c 1 thousand!

If you load: grabber-soksbot-spambot and would like to receive additional income from your downloads, we offer our software and get 70-150 $ 1 to thousands of downloads (all depends on the country).

As for software, we control:

adware, which in turn actively promotes antispyware software! Adware does not conflict with either the botnetami, or trojan, and does not kill your bots!

# Survey Multiple Fakealerts - Intro

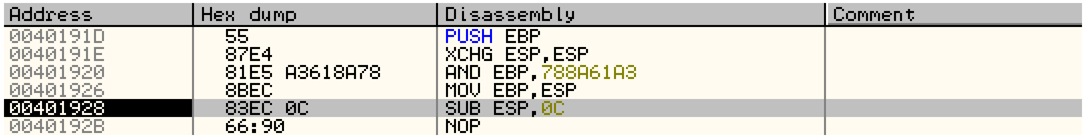
- Vundo obfuscation, behavior, commodity client side exploits
- Codec distribution, often via spammed links – MultyCodecUpgr.7.20680.exe
- P2P distribution and crack sites – binding keygen schemes, most active downloads
- Shuffling web sites and domains
- Common component behaviors – Shell_NotifyIcon

# Vundo's Blatantly Intrusive Behavior

- Vundo's prevalence seems to be on a steep downward slope towards the end of this year
- Vundo loaders and dll's have maintained multiple layers of obfuscation, calls to random antiquated API's, polymorphism
- Vundo distributors most commonly implemented commodity exploits to download and execute components that dropped a randomly named dll and loaded it into its own process, then the loaded dll made copies of itself that it injected first into winlogon, then globally into explorer and other processes
- Process check – ad-aware, winlogon, explorer, other AV's

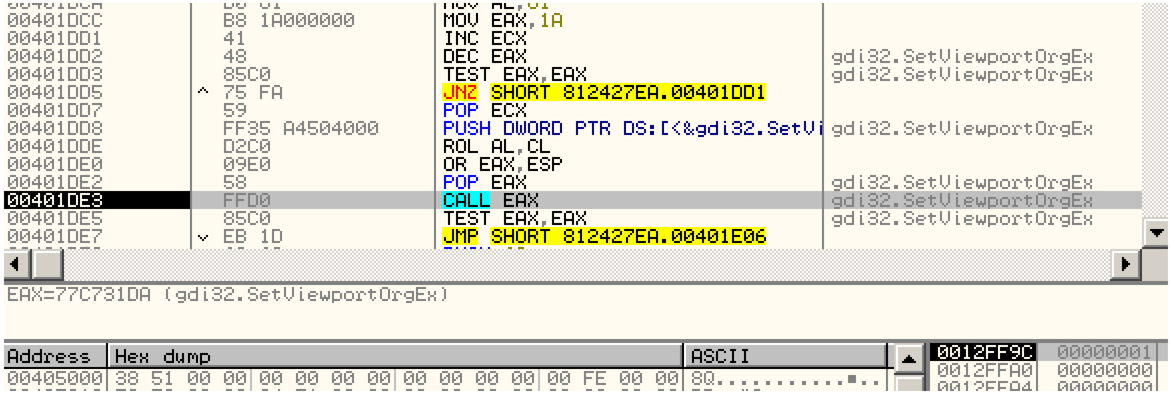
# Vundo's Blatantly Intrusive Behavior

- Anti-RE Obfuscation
  - Anti-RE: perverted code beyond recognition, i.e. prologues where normal “push ebp...move ebp,esp” is mangled



```
Address    Hex dump          Disassembly          Comment
0040191D     55              PUSH EBP
0040191E     87E4            XCHG ESP,ESP
00401920     81E5 A3618A78   AND EBP,788A61A3
00401926     8BEC            MOV EBP,ESP
00401928     83EC 0C         SUB ESP,0C
0040192B     66:90           NOP
```

  - Anti-emulation: calling antiquated api's with “impossible” parameters to generate predictable values – this is not compiler “optimization”



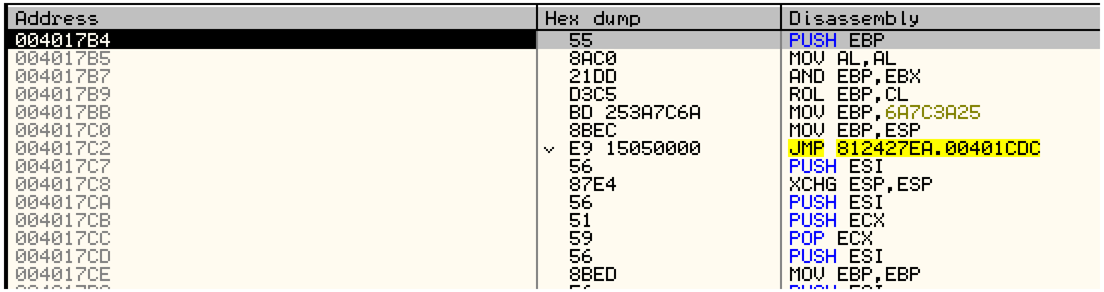
```
00401DCA     B0 01           MOV AL,01
00401DCC     B8 1A000000     MOV EAX,1A
00401DD1     41              INC ECX
00401DD2     48              DEC EAX                          gdi32.SetViewportOrgEx
00401DD3     85C0            TEST EAX,EAX                     gdi32.SetViewportOrgEx
00401DD5   ^ 75 FA           JNZ SHORT 812427EA.00401DD1
00401DD7     59              POP ECX
00401DD8     FF35 A4504000   PUSH DWORD PTR DS:[<&gdi32.SetVi gdi32.SetViewportOrgEx
00401DDE     D2C0            ROL AL,CL
00401DE0     09E0            OR EAX,ESP
00401DE2     58              POP EAX                          gdi32.SetViewportOrgEx
00401DE3     FFD0            CALL EAX                         gdi32.SetViewportOrgEx
00401DE5     85C0            TEST EAX,EAX                     gdi32.SetViewportOrgEx
00401DE7   v EB 1D           JMP SHORT 812427EA.00401E06

EAX=77C731DA (gdi32.SetViewportOrgEx)

Address  Hex dump                                         ASCII               0012FF9C   00000001
00405000 38 51 00 00|00 00 00 00|00 00 00 00|00 FE 00 00|8Q..........■..      0012FFA0   00000000
                                                                             0012FFA4   00000000
```

# Vundo's Blatantly Intrusive Behavior

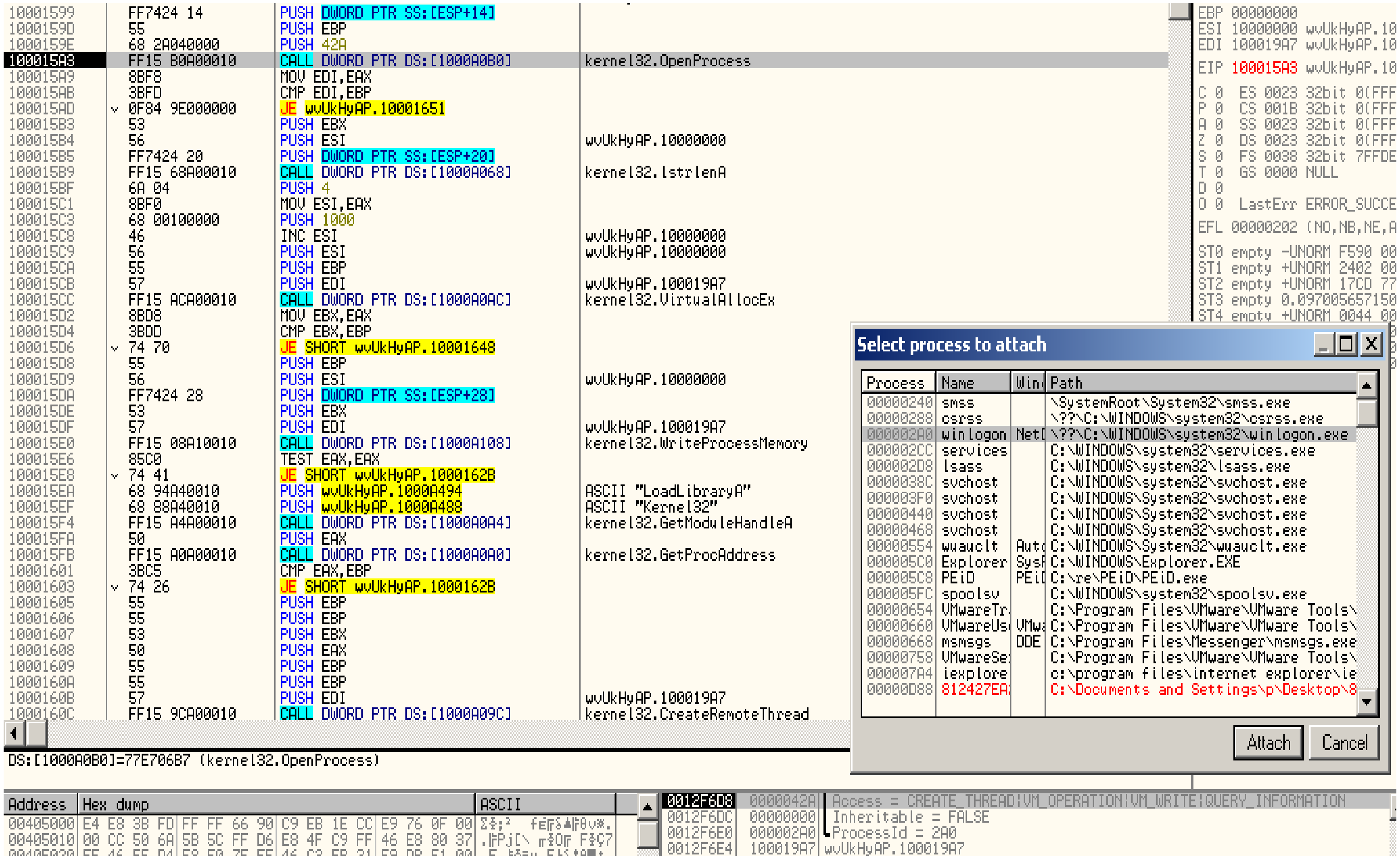
- Garbage assembly level instructions, loops and jmp flows: i.e. implement ridiculous custom GetProcAddress with multiple levels of needless instructions



```
Address     Hex dump       Disassembly
004017B4      55           PUSH EBP
004017B5      8AC0         MOV AL,AL
004017B7      21DD         AND EBP,EBX
004017B9      D3C5         ROL EBP,CL
004017BB      BD 253A7C6A  MOV EBP,6A7C3A25
004017C0      8BEC         MOV EBP,ESP
004017C2    v E9 15050000  JMP 812427EA.00401CDC
004017C7      56           PUSH ESI
004017C8      87E4         XCHG ESP,ESP
004017CA      56           PUSH ESI
004017CB      51           PUSH ECX
004017CC      59           POP ECX
004017CD      56           PUSH ESI
004017CE      8BED         MOV EBP,EBP
```

# Vundo's Blatantly Intrusive Behavior

- Definitive Vundo loader winlogon injection



```
10001599   FF7424 14       PUSH DWORD PTR SS:[ESP+14]
1000159D   55              PUSH EBP
1000159E   68 2A040000     PUSH 42A
100015A3   FF15 B0A00010   CALL DWORD PTR DS:[1000A0B0]        kernel32.OpenProcess
100015A9   8BF8            MOV EDI,EAX
100015AB   3BFD            CMP EDI,EBP
100015AD v 0F84 9E000000   JE wvUkHyAP.10001651
100015B3   53              PUSH EBX
100015B4   56              PUSH ESI                            wvUkHyAP.10000000
100015B5   FF7424 20       PUSH DWORD PTR SS:[ESP+20]
100015B9   FF15 68A00010   CALL DWORD PTR DS:[1000A068]        kernel32.lstrlenA
100015BF   6A 04           PUSH 4
100015C1   8BF0            MOV ESI,EAX
100015C3   68 00100000     PUSH 1000
100015C8   46              INC ESI                             wvUkHyAP.10000000
100015C9   56              PUSH ESI                            wvUkHyAP.10000000
100015CA   55              PUSH EBP
100015CB   57              PUSH EDI                            wvUkHyAP.100019A7
100015CC   FF15 ACA00010   CALL DWORD PTR DS:[1000A0AC]        kernel32.VirtualAllocEx
100015D2   8BD8            MOV EBX,EAX
100015D4   3BDD            CMP EBX,EBP
100015D6 v 74 70           JE SHORT wvUkHyAP.10001648
100015D8   55              PUSH EBP
100015D9   56              PUSH ESI                            wvUkHyAP.10000000
100015DA   FF7424 28       PUSH DWORD PTR SS:[ESP+28]
100015DE   53              PUSH EBX
100015DF   57              PUSH EDI                            wvUkHyAP.100019A7
100015E0   FF15 08A10010   CALL DWORD PTR DS:[1000A108]        kernel32.WriteProcessMemory
100015E6   85C0            TEST EAX,EAX
100015E8 v 74 41           JE SHORT wvUkHyAP.1000162B
100015EA   68 94A40010     PUSH wvUkHyAP.1000A494              ASCII "LoadLibraryA"
100015EF   68 88A40010     PUSH wvUkHyAP.1000A488              ASCII "Kernel32"
100015F4   FF15 A4A00010   CALL DWORD PTR DS:[1000A0A4]        kernel32.GetModuleHandleA
100015FA   50              PUSH EAX
100015FB   FF15 A0A00010   CALL DWORD PTR DS:[1000A0A0]        kernel32.GetProcAddress
10001601   3BC5            CMP EAX,EBP
10001603 v 74 26           JE SHORT wvUkHyAP.1000162B
10001605   55              PUSH EBP
10001606   55              PUSH EBP
10001607   53              PUSH EBX
10001608   50              PUSH EAX
10001609   55              PUSH EBP
1000160A   55              PUSH EBP
1000160B   57              PUSH EDI                            wvUkHyAP.100019A7
1000160C   FF15 9CA00010   CALL DWORD PTR DS:[1000A09C]        kernel32.CreateRemoteThread

DS:[1000A0B0]=77E706B7 (kernel32.OpenProcess)
```

```
EBP 00000000
ESI 10000000 wvUkHyAP.10
EDI 100019A7 wvUkHyAP.10

EIP 100015A3 wvUkHyAP.10

C 0  ES 0023 32bit 0(FFF
P 0  CS 001B 32bit 0(FFF
A 0  SS 0023 32bit 0(FFF
Z 0  DS 0023 32bit 0(FFF
S 0  FS 0038 32bit 7FFDE
T 0  GS 0000 NULL
D 0
O 0  LastErr ERROR_SUCCE

EFL 00000202 (NO,NB,NE,A

ST0 empty -UNORM F590 00
ST1 empty +UNORM 2402 00
ST2 empty +UNORM 17CD 77
ST3 empty 0.097005657150
ST4 empty +UNORM 0044 00
```

**Select process to attach**

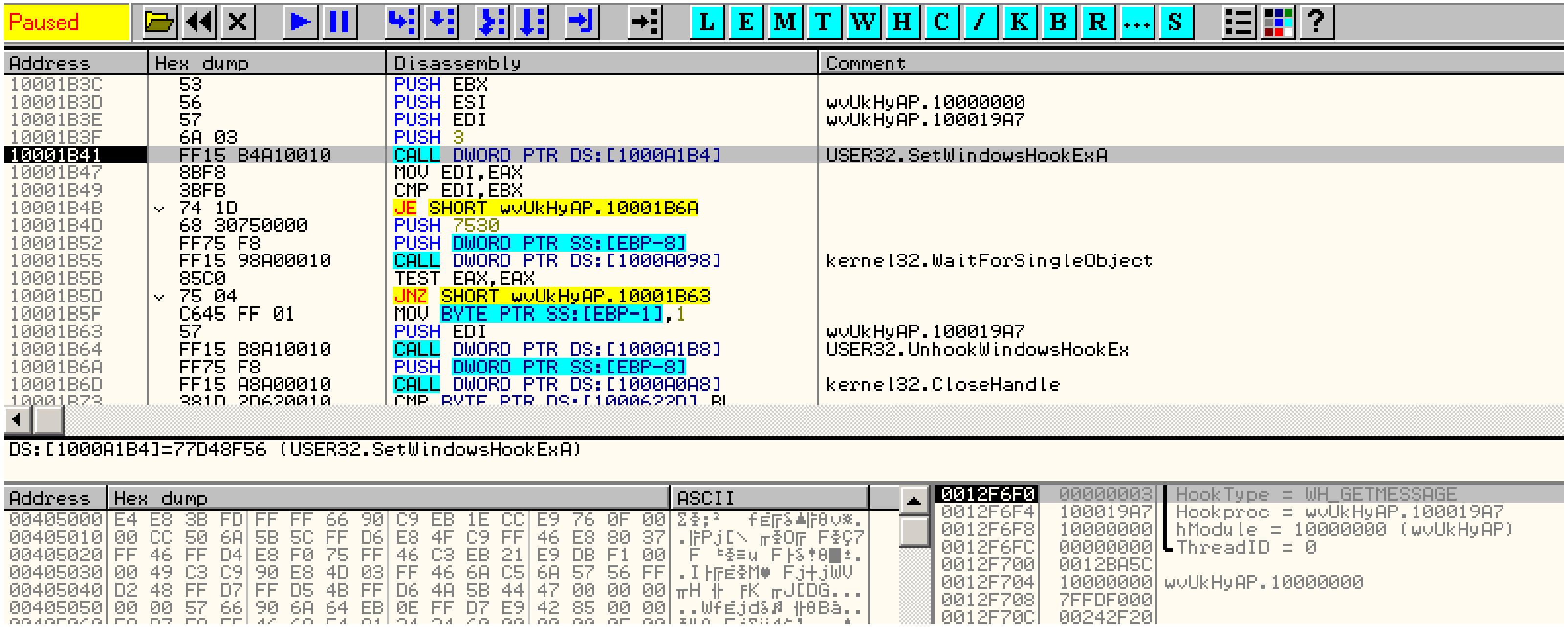
```
Process   Name      Win  Path
00000240  smss           \SystemRoot\System32\smss.exe
00000288  csrss          \??\C:\WINDOWS\system32\csrss.exe
000002A0  winlogon  Net  \??\C:\WINDOWS\system32\winlogon.exe
000002CC  services       C:\WINDOWS\system32\services.exe
000002D8  lsass          C:\WINDOWS\system32\lsass.exe
0000038C  svchost        C:\WINDOWS\system32\svchost.exe
000003F0  svchost        C:\WINDOWS\System32\svchost.exe
00000440  svchost        C:\WINDOWS\System32\svchost.exe
00000468  svchost        C:\WINDOWS\System32\svchost.exe
00000554  wuauclt   Aut  C:\WINDOWS\System32\wuauclt.exe
000005C0  Explorer  SysF C:\WINDOWS\Explorer.EXE
000005C8  PEiD      PEiI C:\re\PEiD\PEiD.exe
000005FC  spoolsv        C:\WINDOWS\system32\spoolsv.exe
00000654  VMwareTr.      C:\Program Files\VMware\VMware Tools\
00000660  VMwareUs  VMwa C:\Program Files\VMware\VMware Tools\
00000668  msmsgs    DDE  C:\Program Files\Messenger\msmsgs.exe
00000758  VMwareSe       C:\Program Files\VMware\VMware Tools\
000007A4  iexplore       c:\program files\internet explorer\ie
00000D88  812427EA       C:\Documents and Settings\p\Desktop\8
```

```
Address   Hex dump                                          ASCII
00405000  E4 E8 3B FD FF FF 66 90 C9 EB 1E CC E9 76 0F 00  Σ╪;²  fɛ╔╞▲╟θv☼.
00405010  00 CC 50 6A 5B 5C FF D6 E8 4F C9 FF 46 E8 80 37  .╟Pj[\ ╓Φ0╔ FΦÇ7
```

```
0012F6D8  0000042A  Access = CREATE_THREAD|VM_OPERATION|VM_WRITE|QUERY_INFORMATION
0012F6DC  00000000  Inheritable = FALSE
0012F6E0  000002A0  ProcessId = 2A0
0012F6E4  100019A7  wvUkHyAP.100019A7
```

# Vundo's Blatently Intrusive Behavior

- Definitive SetWindowsHook WH_GETMESSAGE injection, from this injection, ads displayed, trayalert



```
Address   Hex dump          Disassembly                          Comment
10001B3C    53              PUSH EBX
10001B3D    56              PUSH ESI                             wvUkHyAP.10000000
10001B3E    57              PUSH EDI                             wvUkHyAP.100019A7
10001B3F    6A 03           PUSH 3
10001B41    FF15 B4A10010   CALL DWORD PTR DS:[1000A1B4]         USER32.SetWindowsHookExA
10001B47    8BF8            MOV EDI,EAX
10001B49    3BFB            CMP EDI,EBX
10001B4B  v 74 1D           JE SHORT wvUkHyAP.10001B6A
10001B4D    68 30750000     PUSH 7530
10001B52    FF75 F8         PUSH DWORD PTR SS:[EBP-8]
10001B55    FF15 98A00010   CALL DWORD PTR DS:[1000A098]         kernel32.WaitForSingleObject
10001B5B    85C0            TEST EAX,EAX
10001B5D  v 75 04           JNZ SHORT wvUkHyAP.10001B63
10001B5F    C645 FF 01      MOV BYTE PTR SS:[EBP-1],1
10001B63    57              PUSH EDI                             wvUkHyAP.100019A7
10001B64    FF15 B8A10010   CALL DWORD PTR DS:[1000A1B8]         USER32.UnhookWindowsHookEx
10001B6A    FF75 F8         PUSH DWORD PTR SS:[EBP-8]
10001B6D    FF15 A8A00010   CALL DWORD PTR DS:[1000A0A8]         kernel32.CloseHandle
10001B73    381D 2D620010   CMP BYTE PTR DS:[1000622D],BL

DS:[1000A1B4]=77D48F56 (USER32.SetWindowsHookExA)
```

```
Address   Hex dump                                         ASCII
00405000  E4 E8 3B FD FF FF 66 90 C9 EB 1E CC E9 76 0F 00  Σ‡;²  ƒ╔╒§▲╟θv☼.
00405010  00 CC 50 6A 5B 5C FF D6 E8 4F C9 FF 46 E8 80 37  .╠Pj[\ ╓‡O╔ F‡Ç7
00405020  FF 46 FF D4 E8 F0 75 FF 46 C3 EB 21 E9 DB F1 00   F ╘‡≡u F├δ!Θ█±.
00405030  00 49 C3 C9 90 E8 4D 03 FF 46 6A C5 6A 57 56 FF  .I├╔É‡M♥ Fj┼jWV
00405040  D2 48 FF D7 FF D5 4B FF D6 4A 5B 44 47 00 00 00  ╥H ╫ ╒K ╓J[DG...
00405050  00 00 57 66 90 6A 64 EB 0E FF D7 E9 42 85 00 00  ..WfÉjdδ♫ ╫ΘBà..
```

```
0012F6F0  00000003  ┌HookType = WH_GETMESSAGE
0012F6F4  100019A7  │Hookproc = wvUkHyAP.100019A7
0012F6F8  10000000  │hModule = 10000000 (wvUkHyAP)
0012F6FC  00000000  └ThreadID = 0
0012F700  0012BA5C
0012F704  10000000  wvUkHyAP.10000000
0012F708  7FFDF000
0012F70C  00242F20
```

# Codec Distribution

- Zcodec.1140.exe -> 5491.exe -> sav.exe, etc
- 5491.exe is a simple self extracting compressed archive, no packing involved, drops sav.exe in %progfiles%\AV2008
- No injections, no system tampering -- clearly “malicious” behavior?

# MonaRonaDona Hoax - Intro

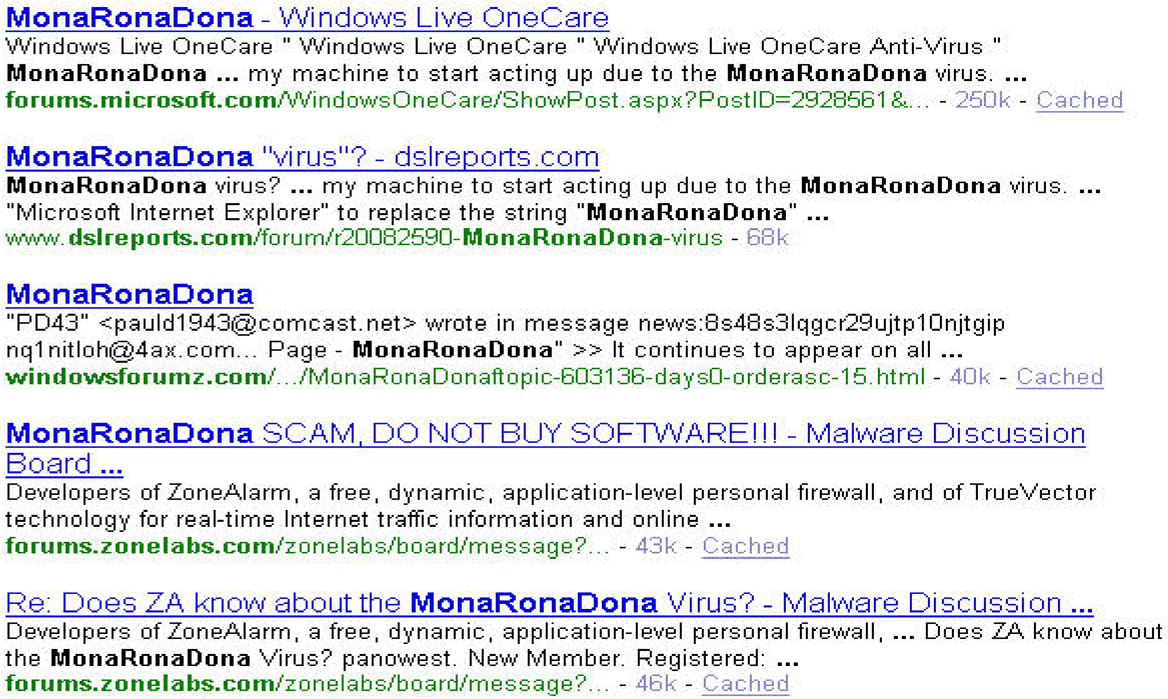
- Bumbling rogueware scheme – early 2008
- “Virus” bound to version of "Registrycleaner2008"
- Hoax postings and content regarding this “virus”
- “Virus”?
- Fraudulent postings about unigray antivirus scanner and its user base, google/search engine top results

# MonaRonaDona Hoax -- Planning

- Create AV product that performs no beneficial activity
- Attempt to establish reputation and price point by comparison between it and legitimate solutions
- Write phony “virus”
- Create confusion and chatter about it on popular forums
- Wait for $$$ -- you will wait a long time
- This does not work

# MonaRonaDona Hoax – Hoax postings

- Create forum chatter and search engine hits:



**MonaRonaDona** - Windows Live OneCare
Windows Live OneCare " Windows Live OneCare " Windows Live OneCare Anti-Virus "
**MonaRonaDona ...** my machine to start acting up due to the **MonaRonaDona** virus. **...**
**forums.microsoft.com**/WindowsOneCare/ShowPost.aspx?PostID=2928561&... - 250k - Cached

**MonaRonaDona** "virus"? - dslreports.com
**MonaRonaDona** virus? **...** my machine to start acting up due to the **MonaRonaDona** virus. **...**
"Microsoft Internet Explorer" to replace the string "**MonaRonaDona**" **...**
www.**dslreports.com**/forum/r20082590-**MonaRonaDona**-virus - 68k

**MonaRonaDona**
"PD43" <pauld1943@comcast.net> wrote in message news:8s48s3lqgcr29ujtp10njtgip
nq1nitloh@4ax.com... Page - **MonaRonaDona**" >> It continues to appear on all **...**
**windowsforumz.com**/.../MonaRonaDonaftopic-603136-days0-orderasc-15.html - 40k - Cached

**MonaRonaDona** SCAM, DO NOT BUY SOFTWARE!!! - Malware Discussion Board **...**
Developers of ZoneAlarm, a free, dynamic, application-level personal firewall, and of TrueVector
technology for real-time Internet traffic information and online **...**
**forums.zonelabs.com**/zonelabs/board/message?... - 43k - Cached

Re: Does ZA know about the **MonaRonaDona** Virus? - Malware Discussion **...**
Developers of ZoneAlarm, a free, dynamic, application-level personal firewall, **...** Does ZA know about
the **MonaRonaDona** Virus? panowest. New Member. Registered: **...**
**forums.zonelabs.com**/zonelabs/board/message?... - 46k - Cached

# MonaRonaDona Hoax – “Virus”

- Svcspool.exe dropped to All Users StartMenu Startup by RegistryCleaner2008.exe
- Really a “virus”? No – no replication code. IE WindowBar manipulation, Task Manager disabled by dropper. Some amount of hiding, obfuscation
- “Top virus list”

# Downloader Components – Intro

- Malicious examples – 0xf9.exe, av2009install.exe
- Static characteristics
- Behavioral characteristics
- Downloading sav.exe
- Groups continue to use exploits to deliver downloaders, do testers know that?

# Downloaders

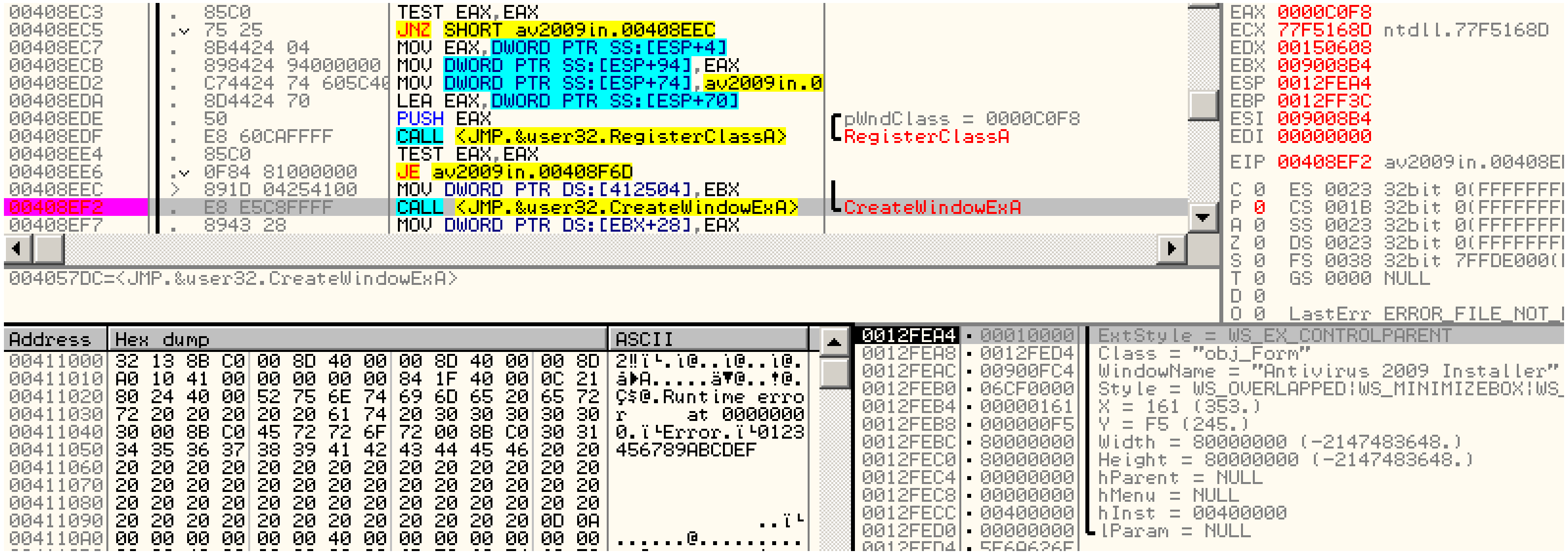
- Difficult for behavioral solutions to assess without using more hardcoded data – closer to signature based technologies

av2009install.exe

- AV2009 UPX packed compiled Delphi executable
  - Simple and straightforward, like any other app...CreateWindow, InternetOpen, InternetOpenUrl, CreateProcess
  - Creating a dependence on static characteristics of file, connection endpoints,etc
  - InternetOpenUrl connects with http://securedownloads6.com/download/av_2009.exe

# Downloaders

- Simple CreateWindowEx for installer box, nothing obfuscated or injected here...



```
00408EC3  .   85C0            TEST EAX,EAX
00408EC5  .v  75 25           JNZ SHORT av2009in.00408EEC
00408EC7  .   8B4424 04       MOV EAX,DWORD PTR SS:[ESP+4]
00408ECB  .   898424 94000000 MOV DWORD PTR SS:[ESP+94],EAX
00408ED2  .   C74424 74 605C40 MOV DWORD PTR SS:[ESP+74],av2009in.0
00408EDA  .   8D4424 70       LEA EAX,DWORD PTR SS:[ESP+70]
00408EDE  .   50              PUSH EAX                                  [pWndClass = 0000C0F8
00408EDF  .   E8 60CAFFFF     CALL <JMP.&user32.RegisterClassA>         [RegisterClassA
00408EE4  .   85C0            TEST EAX,EAX
00408EE6  .v  0F84 81000000   JE av2009in.00408F6D
00408EEC  >   891D 04254100   MOV DWORD PTR DS:[412504],EBX
00408EF2  .   E8 E5C8FFFF     CALL <JMP.&user32.CreateWindowExA>        [CreateWindowExA
00408EF7  .   8943 28         MOV DWORD PTR DS:[EBX+28],EAX

004057DC=<JMP.&user32.CreateWindowExA>
```

```
EAX 0000C0F8
ECX 77F5168D ntdll.77F5168D
EDX 00150608
EBX 009008B4
ESP 0012FEA4
EBP 0012FF3C
ESI 009008B4
EDI 00000000

EIP 00408EF2 av2009in.00408EI

C 0  ES 0023 32bit 0(FFFFFFFI
P 0  CS 001B 32bit 0(FFFFFFFI
A 0  SS 0023 32bit 0(FFFFFFFI
Z 0  DS 0023 32bit 0(FFFFFFFI
S 0  FS 0038 32bit 7FFDE000(I
T 0  GS 0000 NULL
D 0
O 0  LastErr ERROR_FILE_NOT_I
```

```
Address  Hex dump                                         ASCII
00411000 32 13 8B C0 00 8D 40 00 00 8D 40 00 00 8D 40 00 2‼ï└.ì@..ì@..ì@.
00411010 A0 10 41 00 00 00 00 00 84 1F 40 00 0C 21 40 00 á▶A.....ä▼@..!@.
00411020 80 24 40 00 52 75 6E 74 69 6D 65 20 65 72 72 6F Ç$@.Runtime erro
00411030 72 20 20 20 20 20 61 74 20 30 30 30 30 30 30 30 r     at 0000000
00411040 30 00 8B C0 45 72 72 6F 72 00 8B C0 30 31 32 33 0.ï└Error.ï└0123
00411050 34 35 36 37 38 39 41 42 43 44 45 46 20 20 20 20 456789ABCDEF
00411060 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
00411070 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
00411080 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
00411090 20 20 20 20 20 20 20 20 20 20 20 20 0D 0A 8B C0             ..ï└
004110A0 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 ......@.........
```

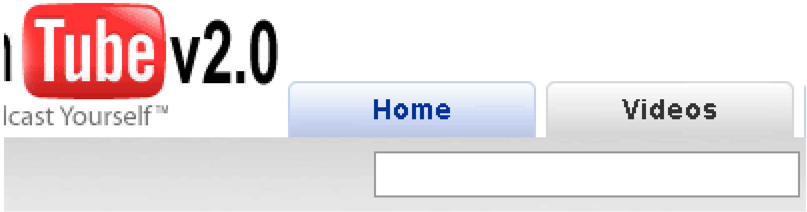
```
0012FEA4 . 00010000 ExtStyle = WS_EX_CONTROLPARENT
0012FEA8 . 0012FED4 Class = "obj_Form"
0012FEAC . 00900FC4 WindowName = "Antivirus 2009 Installer"
0012FEB0 . 06CF0000 Style = WS_OVERLAPPED|WS_MINIMIZEBOX|WS_
0012FEB4 . 00000161 X = 161 (353.)
0012FEB8 . 000000F5 Y = F5 (245.)
0012FEBC . 80000000 Width = 80000000 (-2147483648.)
0012FEC0 . 80000000 Height = 80000000 (-2147483648.)
0012FEC4 . 00000000 hParent = NULL
0012FEC8 . 00000000 hMenu = NULL
0012FECC . 00400000 hInst = 00400000
0012FED0 . 00000000 lParam = NULL
0012FED4 . 5F6A626F
```

# Downloaders

- Adobe exploit kits – Dancho Danchev's blog, Secure Computing
- 0xf9.exe is generally a ~20k upx packed Visual Basic compiled executable, standard part of a kit being reused
  - Names? “Downloader.MisleadApp”, Trojan-Downloader.Win32.VB.hww,Trojan-Downloader.Win32.VB.hyc
  - Trivial unpacking with upx, simple inspection of underlying code with Basic Decompiler
  - Straightforward download and setup of msadv.exe or mssadv_sp.exe in “Program Files\Microsoft Security Adviser”

# Recent Components -- MultyCodec

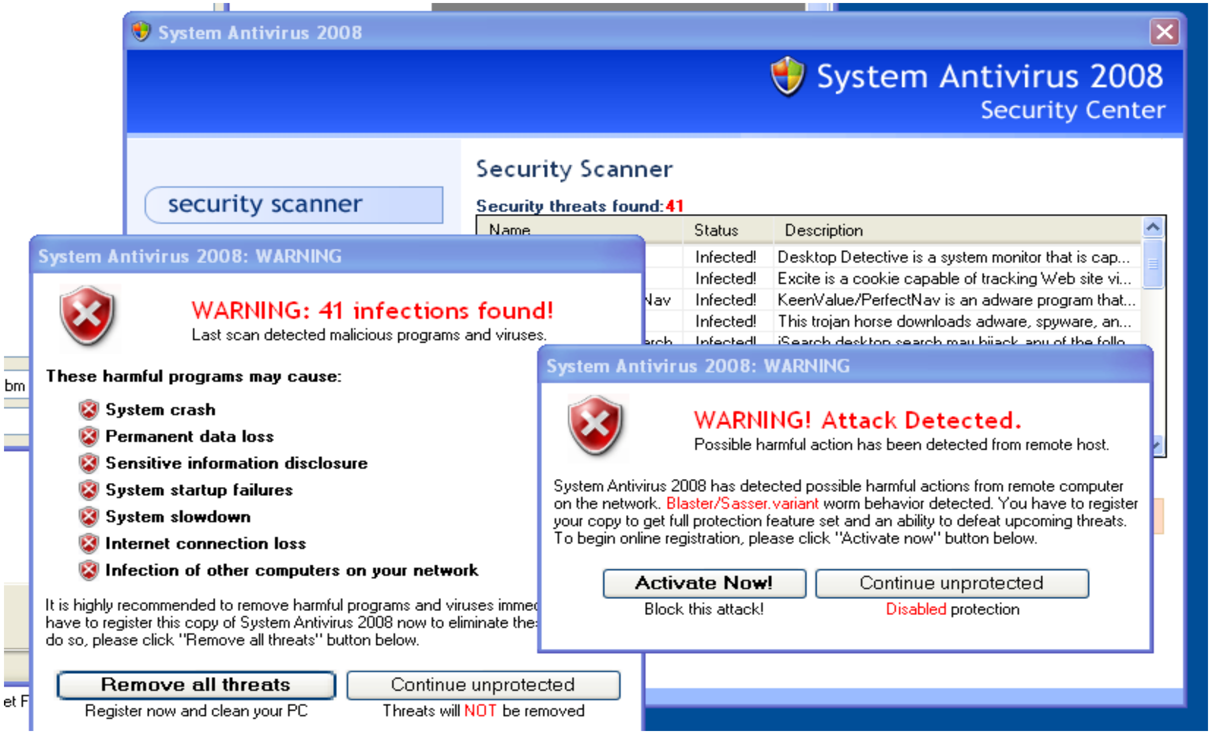
- Multiple components delivered via phony video codec



- MultyCodec.7.20680.exe drops c..exe, calls CreateProcess on the file, phones home
  - Based on http responses, “promomodule” carries out 'trayalert', 'winalert', 'excelalert', etc
  - Changing behaviors from b..exe based on response – spoils automated analysis
  - Shell_NotifyIcon call based on 'trayalert'...”you have a security problem'

# Recent Components -- AntiVirus 2008

- Misleading scan results



Security Scanner

Security threats found: 41

| Name | Status | Description |
|---|---|---|
| | Infected! | Desktop Detective is a system monitor that is cap... |
| | Infected! | Excite is a cookie capable of tracking Web site vi... |
| Nav | Infected! | KeenValue/PerfectNav is an adware program that... |
| | Infected! | This trojan horse downloads adware, spyware, an... |
| arch | Infected! | iSearch desktop search may hijack any of the follo |

WARNING: 41 infections found!

Last scan detected malicious programs and viruses.

These harmful programs may cause:

- System crash
- Permanent data loss
- Sensitive information disclosure
- System startup failures
- System slowdown
- Internet connection loss
- Infection of other computers on your network

It is highly recommended to remove harmful programs and viruses immed
have to register this copy of System Antivirus 2008 now to eliminate the
do so, please click "Remove all threats" button below.

Register now and clean your PC

Threats will NOT be removed

WARNING! Attack Detected.

Possible harmful action has been detected from remote host.

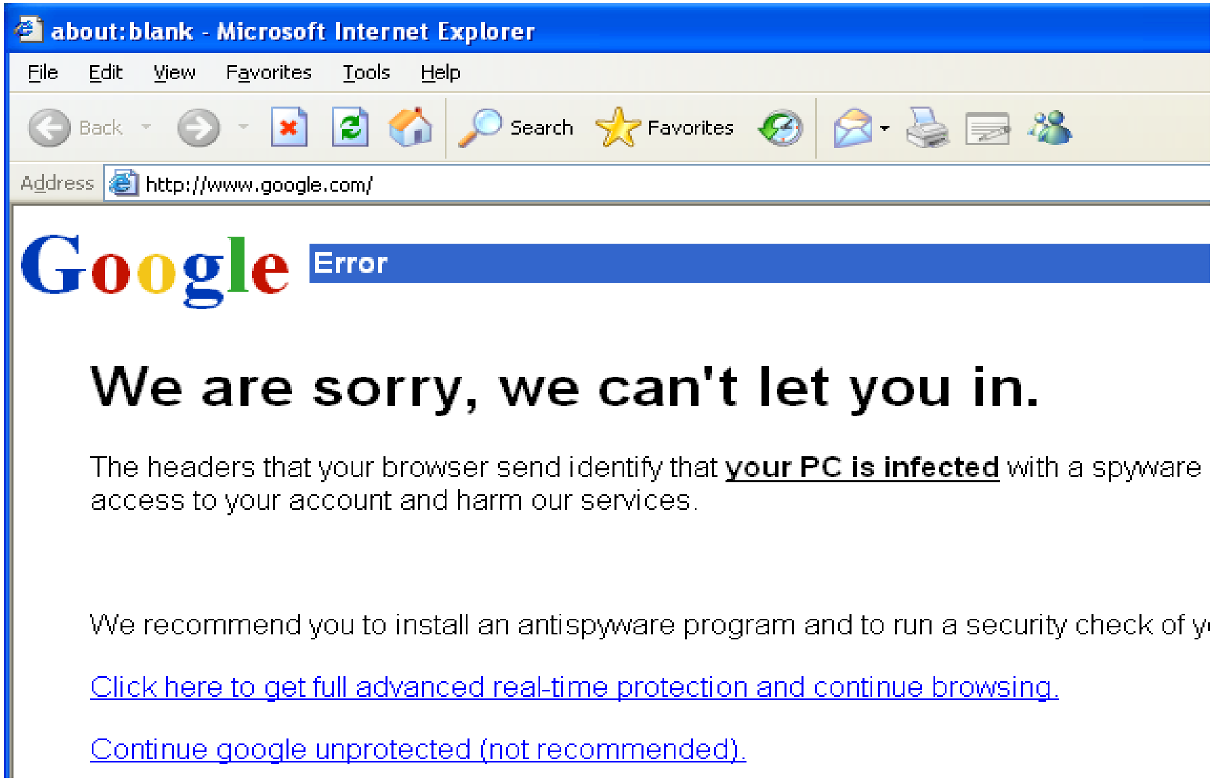
System Antivirus 2008 has detected possible harmful actions from remote computer on the network. Blaster/Sasser.variant worm behavior detected. You have to register your copy to get full protection feature set and an ability to defeat upcoming threats. To begin online registration, please click "Activate now" button below.

Block this attack!

Disabled protection

# Recent Components -- AntiVirus 2008

- Misleading browser redirection



We are sorry, we can't let you in.

The headers that your browser send identify that **your PC is infected** with a spyware access to your account and harm our services.

We recommend you to install an antispyware program and to run a security check of y

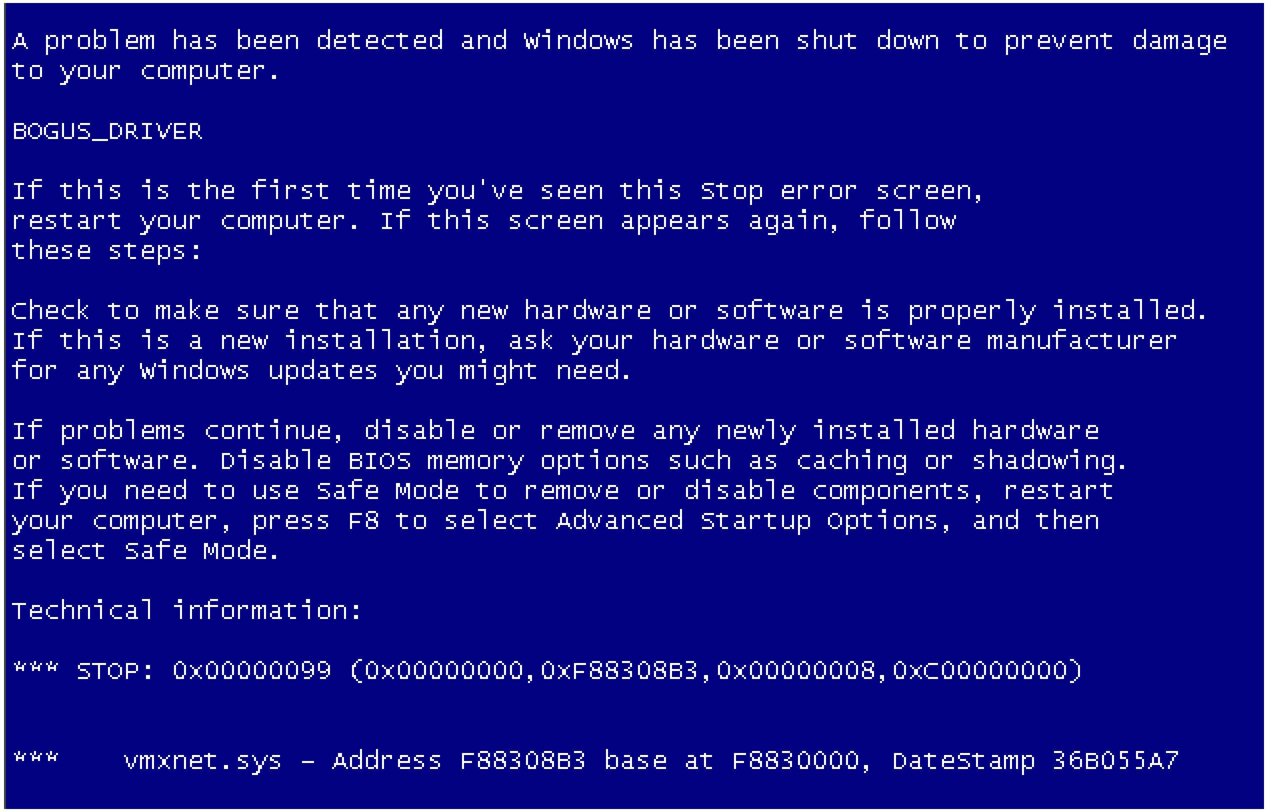
Click here to get full advanced real-time protection and continue browsing.

Continue google unprotected (not recommended).

# Microsoft Legal Efforts

- On Monday, Microsoft/State of Wash Atty General Office lawsuit filed against “John Doe”, maker of AV2008, Winfixer, etc
- CAN-SPAM enforced against some Spam Kings, ineffective against global spam industry. See inbox/bulk.
- Behavioral based products – will they have to hybridize, or will they just continue as another layer?

# Questions?



```
A problem has been detected and Windows has been shut down to prevent damage
to your computer.

BOGUS_DRIVER

If this is the first time you've seen this Stop error screen,
restart your computer. If this screen appears again, follow
these steps:

Check to make sure that any new hardware or software is properly installed.
If this is a new installation, ask your hardware or software manufacturer
for any Windows updates you might need.

If problems continue, disable or remove any newly installed hardware
or software. Disable BIOS memory options such as caching or shadowing.
If you need to use Safe Mode to remove or disable components, restart
your computer, press F8 to select Advanced Startup Options, and then
select Safe Mode.

Technical information:

*** STOP: 0x00000099 (0x00000000,0xF88308B3,0x00000008,0xC0000000)


***    vmxnet.sys - Address F88308B3 base at F8830000, DateStamp 36B055A7
```