McAfee



Good Viruses. Evaluating the Risks.

Dr. Igor Muttik | Senior Architect | McAfee | Avert Labs®

Good viruses

- It is just technology – neither bad nor good
- What could make it dangerous:
  - Lack of control
  - Wide availability
- If it is dangerous – it's bad
  - "Atomic bomb" is bad
  - "Splitting the atom"?
  - "Chain reaction"? (worst because control is lost)
- Can a virus be written accidentally?
- Can a good virus get out of control?

McAfee®

Agenda



- “Good virus” idea keeps coming up
- Already.71 – a tool and a virus
  (disassembly and operation)
- “Corrupted blood” epidemic in WoW **(video)**
- W32/Nachi – worm that exploited and patched a vulnerability
- Pros and cons of harnessing replicating code
- Conclusions

Google search for “good virus” and “bad virus”

Good		Bad	
Good virus	94,600	Bad virus	64,400
Good worm	12,200	Bad worm	17,000
Beneficial virus	1,860	Horrible/awful virus	44,410
Beneficial worm	306	Horrible/awful worm	1,793
Total	**108,966**	Total	**127,603**

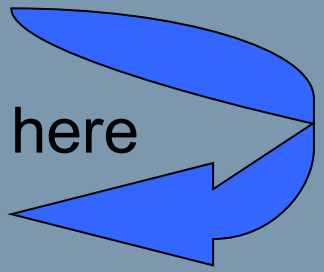
- People are very receptive to “a good virus” idea
- A lot of “bad virus” searches are emotional (“horrible” and ”awful”)

ALREADY.COM – a tool and a worm!

McAfee®

ALREADY.COM tool usage

```
@echo off
rem Start of AUTOEXEC.BAT file
rem Opening commands always execute
ALREADY.COM
IF ERRORLEVEL 1 GOTO skip
rem Things to do once a day go here
:skip
rem Following commands always execute
```



McAfee®

Already.71 – just 71 (0x47) bytes

```
0100                mov     ah, 2Ah
0102                int     21h             ; DOS - GET CURRENT DATE
0102                                        ; Return: DL = day, DH = month, CX = year
0102                                        ; AL = day of the week (0=Sunday, 1=Monday, etc.)
0104                cmp     dx, date
0108                jnz     different
010A                cmp     cx, year
010E                jnz     different
0110                mov     ax, 4C01h
0113                int     21h             ; DOS - 2+ - QUIT WITH EXIT CODE (EXIT)
0113                                        ; AL = exit code
0115 ; ---------------------------------------------------------------------------
0115
0115 different:                             ; CODE XREF: start+8↑j
0115                                        ; start+E↑j
0115                mov     date, dx
0119                mov     year, cx
011D                mov     dx, offset aAlready_com ; "ALREADY.COM"
0120                xor     cx, cx
0122                mov     ah, 3Ch
0124                int     21h             ; DOS - 2+ - CREATE A FILE WITH HANDLE (CREAT)
0124                                        ; CX = attributes for file
0124                                        ; DS:DX -> ASCIZ filename (may include drive and path)
0126                mov     bx, ax
0128                mov     dx, 100h
012B                mov     cx, 47h
012E                mov     ah, 40h
0130                int     21h             ; DOS - 2+ - WRITE TO FILE WITH HANDLE
0130                                        ; BX = file handle, CX = number of bytes to write, DS:DX -> buffer
0132                mov     ax, 4C00h
0135                int     21h             ; DOS - 2+ - QUIT WITH EXIT CODE (EXIT)
0135 start          endp                    ; AL = exit code
0135
0135 ; ---------------------------------------------------------------------------
0137 date           dw 711h                 ; DATA XREF: start+4↑r
0137                                        ; start+15↑w
0139 year           dw 7CBh                 ; DATA XREF: start+A↑r
0139                                        ; start+19↑w
013B aAlready_com   db 'ALREADY.COM',0      ; DATA XREF: start+1D↑o
```

McAfee

Already.71 – get current date (1st block of 3)

```
0100                mov     ah, 2Ah
0102                int     21h             ; DOS - GET CURRENT DATE
0102                                        ; Return: DL = day, DH = month, CX = year
0102                                        ; AL = day of the week (0=Sunday, 1=Monday, etc.)
0104                cmp     dx, date
0108                jnz     different
010A                cmp     cx, year
010E                jnz     different
0110                mov     ax, 4C01h
0113                int     21h             ; DOS - 2+ - QUIT WITH EXIT CODE (EXIT)
0113                                        ; AL = exit code
0115 ; ---------------------------------------------------------------------------
0115
0115 different:                             ; CODE XREF: start+8↑j
0115                                        ; start+E↑j
0115                mov     date, dx
0119                mov     year, cx
011D                mov     dx, offset aAlready_com ; "ALREADY.COM"
0120                xor     cx, cx
0122                mov     ah, 3Ch
0124                int     21h             ; DOS - 2+ - CREATE A FILE WITH HANDLE (CREAT)
0124                                        ; CX = attributes for file
0124                                        ; DS:DX -> ASCIZ filename (may include drive and path)
0126                mov     bx, ax
0128                mov     dx, 100h
012B                mov     cx, 47h
012E                mov     ah, 40h
0130                int     21h             ; DOS - 2+ - WRITE TO FILE WITH HANDLE
0130                                        ; BX = file handle, CX = number of bytes to write, DS:DX -> buffer
0132                mov     ax, 4C00h
0135                int     21h             ; DOS - 2+ - QUIT WITH EXIT CODE (EXIT)
0135 start          endp                    ; AL = exit code
0135
0135 ; ---------------------------------------------------------------------------
0137 date           dw 711h                 ; DATA XREF: start+4↑r
0137                                        ; start+15↑w
0139 year           dw 7CBh                 ; DATA XREF: start+A↑r
0139                                        ; start+19↑w
013B aAlready_com   db 'ALREADY.COM',0      ; DATA XREF: start+1D↑o
```

McAfee

Already.71 – compare (2nd block of 3)

```
0100                mov     ah, 2Ah
0102                int     21h             ; DOS - GET CURRENT DATE
0102                                        ; Return: DL = day, DH = month, CX = year
0102                                        ; AL = day of the week (0=Sunday, 1=Monday, etc.)
0104                cmp     dx, date
0108                jnz     different
010A                cmp     cx, year
010E                jnz     different
0110                mov     ax, 4C01h
0113                int     21h             ; DOS - 2+ - QUIT WITH EXIT CODE (EXIT)
0113                                        ; AL = exit code
0115 ; ---------------------------------------------------------------------------
0115
0115 different:                             ; CODE XREF: start+8↑j
0115                                        ; start+E↑j
0115                mov     date, dx
0119                mov     year, cx
011D                mov     dx, offset aAlready_com ; "ALREADY.COM"
0120                xor     cx, cx
0122                mov     ah, 3Ch
0124                int     21h             ; DOS - 2+ - CREATE A FILE WITH HANDLE (CREAT)
0124                                        ; CX = attributes for file
0124                                        ; DS:DX -> ASCIZ filename (may include drive and path)
0126                mov     bx, ax
0128                mov     dx, 100h
012B                mov     cx, 47h
012E                mov     ah, 40h
0130                int     21h             ; DOS - 2+ - WRITE TO FILE WITH HANDLE
0130                                        ; BX = file handle, CX = number of bytes to write, DS:DX -> buffer
0132                mov     ax, 4C00h
0135                int     21h             ; DOS - 2+ - QUIT WITH EXIT CODE (EXIT)
0135 start          endp                    ; AL = exit code
0135
0135 ; ---------------------------------------------------------------------------
0137 date           dw 711h                 ; DATA XREF: start+4↑r
0137                                        ; start+15↑w
0139 year           dw 7CBh                 ; DATA XREF: start+A↑r
0139                                        ; start+19↑w
013B aAlready_com   db 'ALREADY.COM',0      ; DATA XREF: start+1D↑o
```

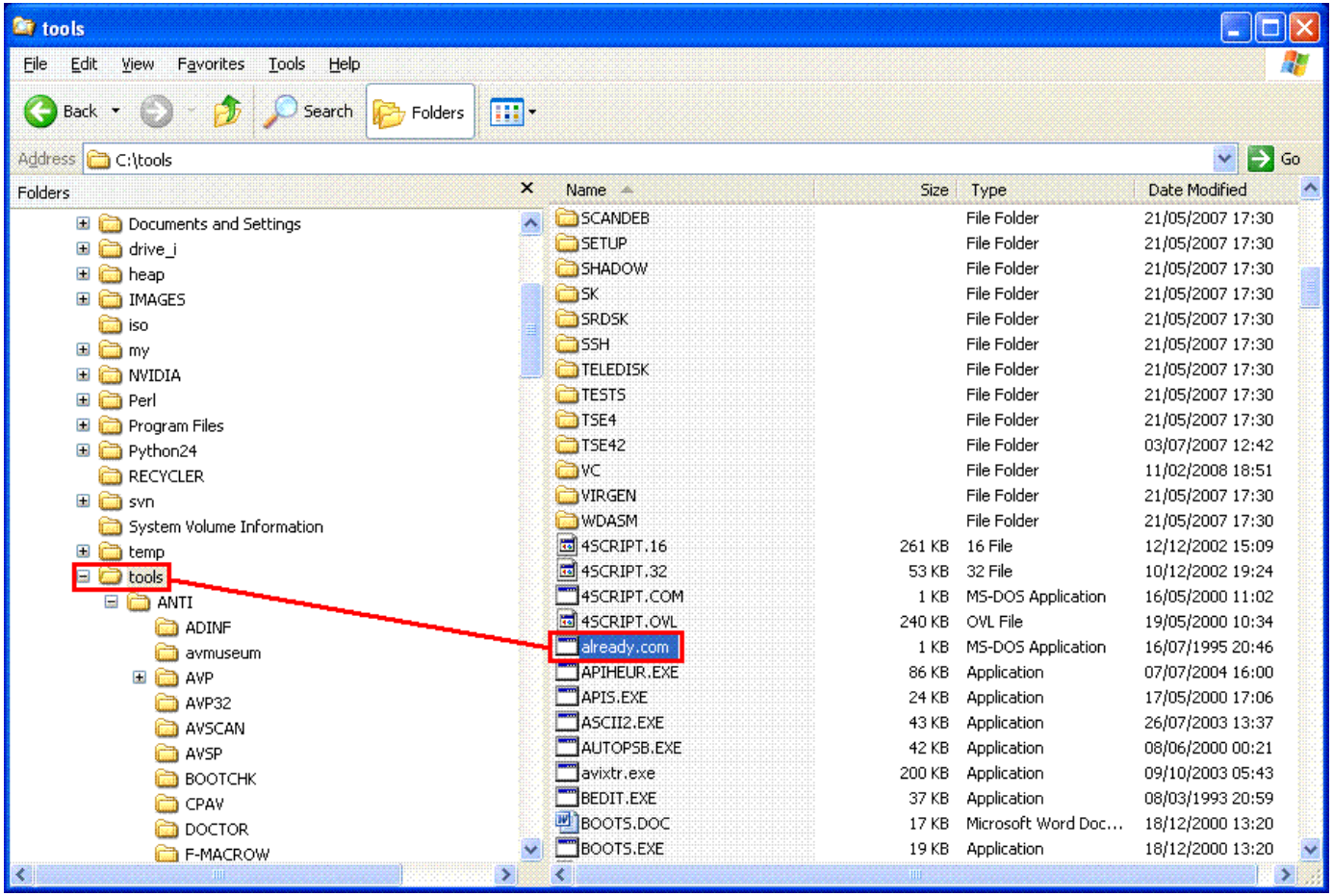
McAfee

Already.71 – write itself to disk (3rd block)

```
0100                mov     ah, 2Ah
0102                int     21h             ; DOS - GET CURRENT DATE
0102                                        ; Return: DL = day, DH = month, CX = year
0102                                        ; AL = day of the week (0=Sunday, 1=Monday, etc.)
0104                cmp     dx, date
0108                jnz     different
010A                cmp     cx, year
010E                jnz     different
0110                mov     ax, 4C01h
0113                int     21h             ; DOS - 2+ - QUIT WITH EXIT CODE (EXIT)
0113                                        ; AL = exit code
0115 ; ---------------------------------------------------------------------------
0115
0115 different:                             ; CODE XREF: start+8↑j
0115                                        ; start+E↑j
0115                mov     date, dx
0119                mov     year, cx
011D                mov     dx, offset aAlready_com ; "ALREADY.COM"
0120                xor     cx, cx
0122                mov     ah, 3Ch
0124                int     21h             ; DOS - 2+ - CREATE A FILE WITH HANDLE (CREAT)
0124                                        ; CX = attributes for file
0124                                        ; DS:DX -> ASCIZ filename (may include drive and path)
0126                mov     bx, ax
0128                mov     dx, 100h
012B                mov     cx, 47h
012E                mov     ah, 40h
0130                int     21h             ; DOS - 2+ - WRITE TO FILE WITH HANDLE
0130                                        ; BX = file handle, CX = number of bytes to write, DS:DX -> buffer
0132                mov     ax, 4C00h
0135                int     21h             ; DOS - 2+ - QUIT WITH EXIT CODE (EXIT)
0135 start          endp                    ; AL = exit code
0135
0135 ; ---------------------------------------------------------------------------
0137 date           dw 711h                 ; DATA XREF: start+4↑r
0137                                        ; start+15↑w
0139 year           dw 7CBh                 ; DATA XREF: start+A↑r
0139                                        ; start+19↑w
013B aAlready_com   db 'ALREADY.COM',0      ; DATA XREF: start+1D↑o
```

McAfee®

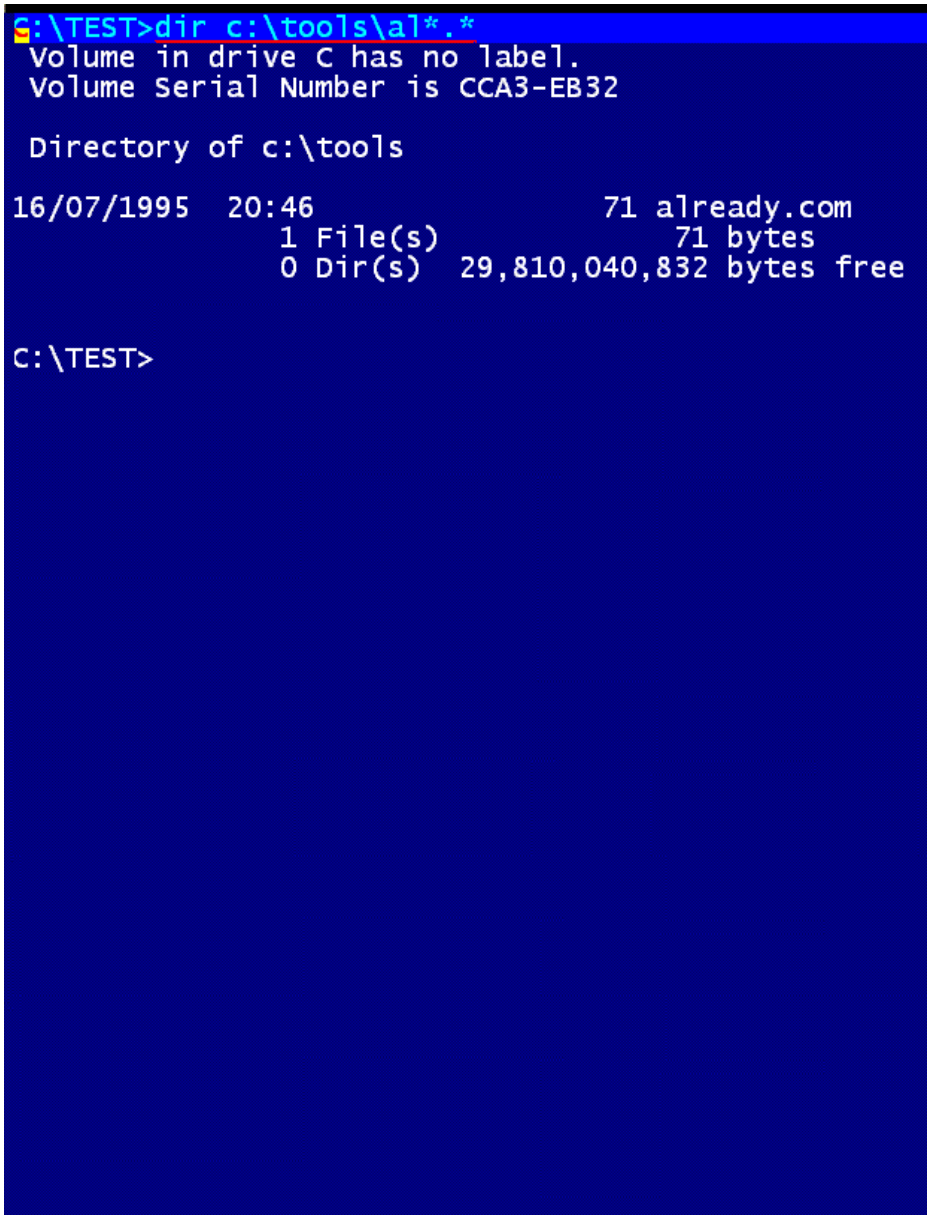
How does Already.71 spread?



Due to “current folder” concept.

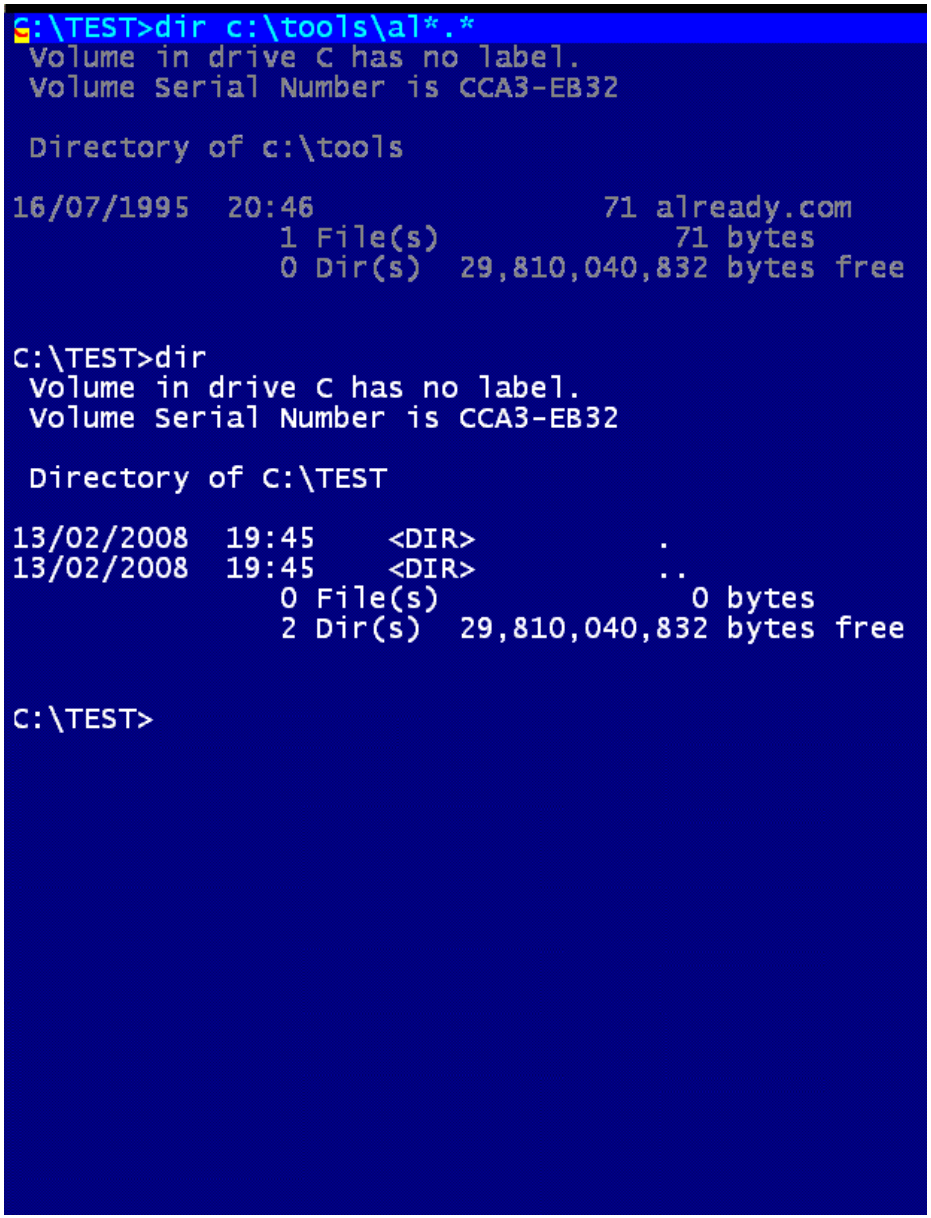
McAfee

A tool



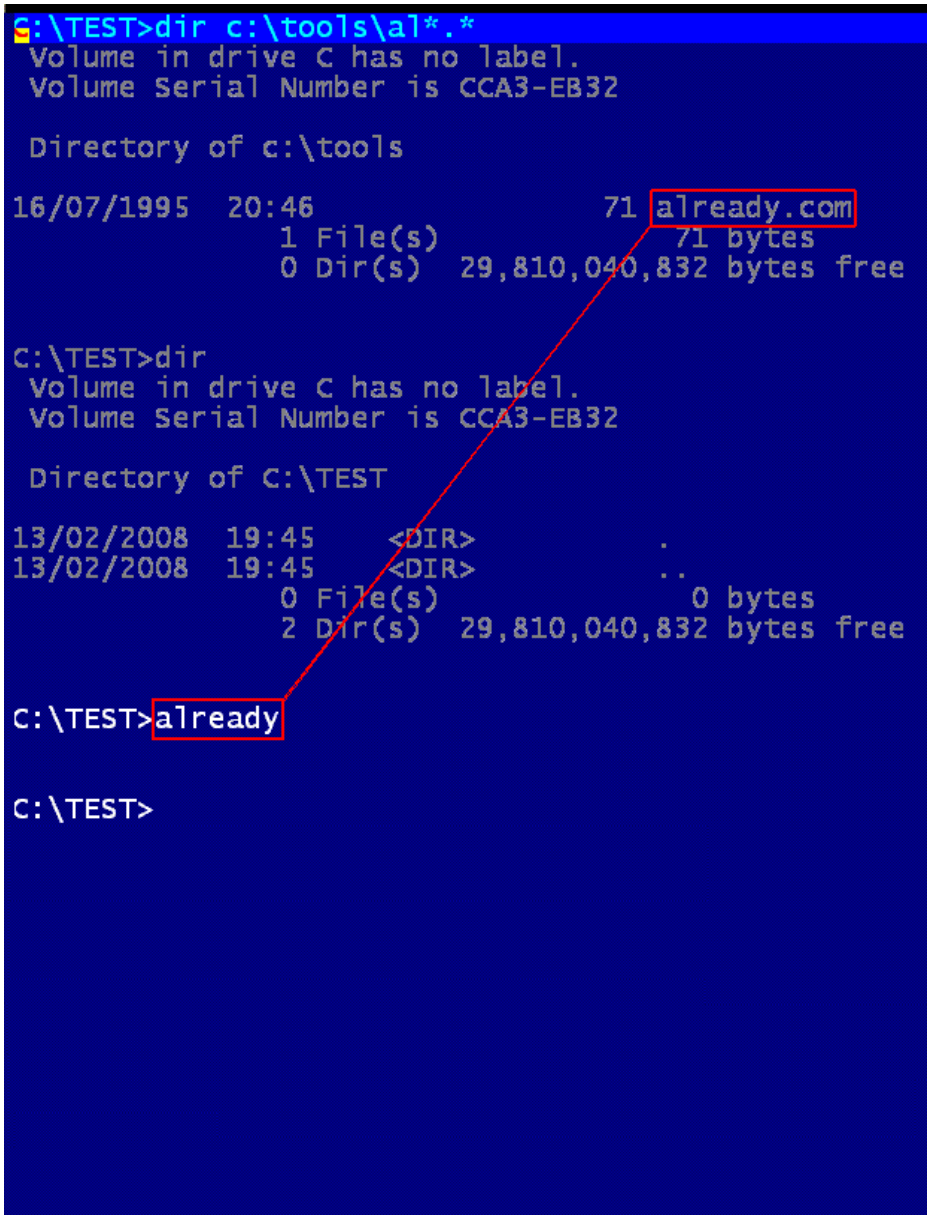
McAfee

Empty folder



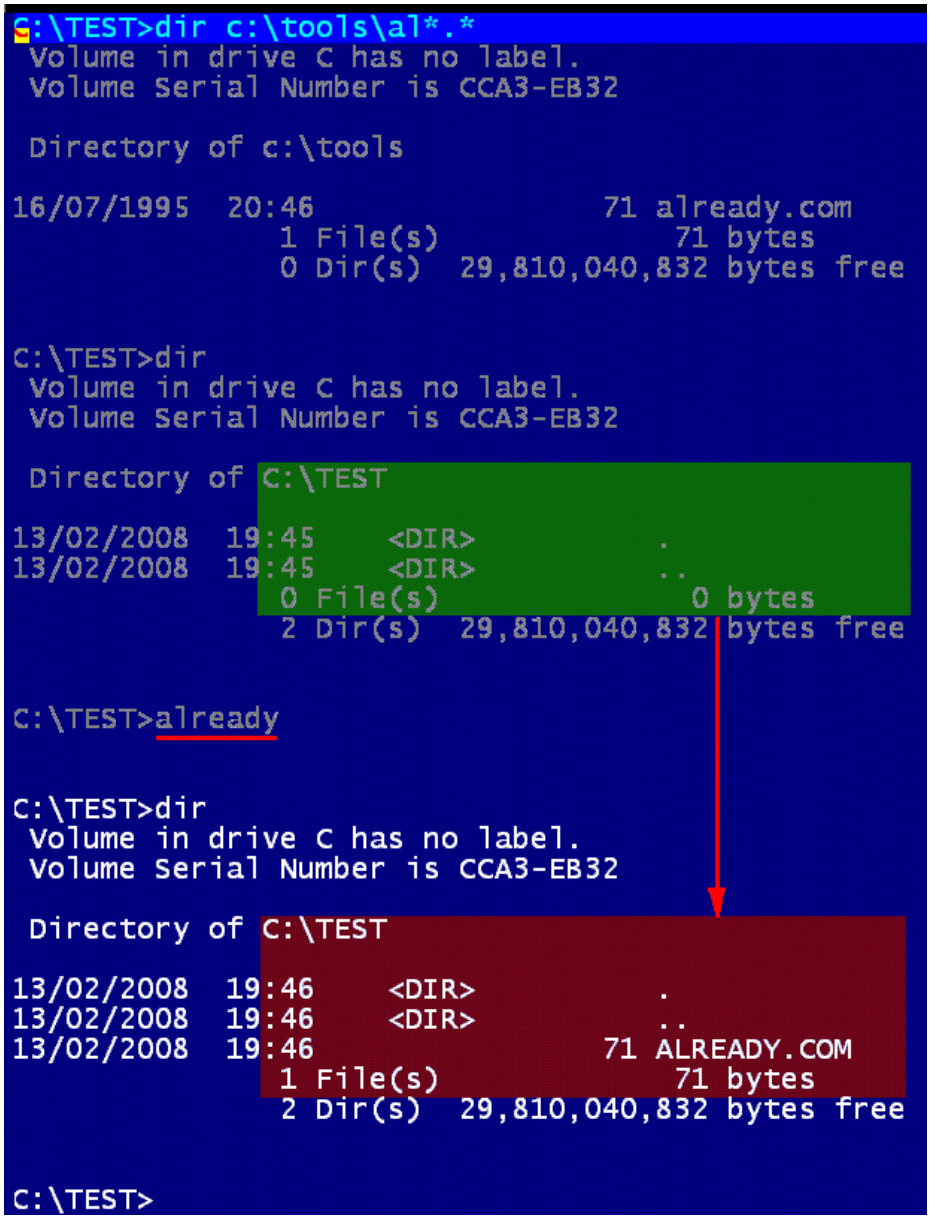
McAfee®

Execution



McAfee®

Replicant!



McAfee

What did we learn?



Insecure environment
+ Insecure programming techniques
= Replicating worm

- Probability of a mistake grows when insecure programming techniques are used:
  - Self-modifying code
  - Modifying other programs on disk or in memory
  - Using exploits
- Insecure environments are unexpectedly common

“Corrupted blood” incident in WoW

McAfee®

“Corrupted blood” epidemic (Sep 2005)

- Zul’Gurub instance dungeon (added in WoW 1.7 for 60+ lvl players):



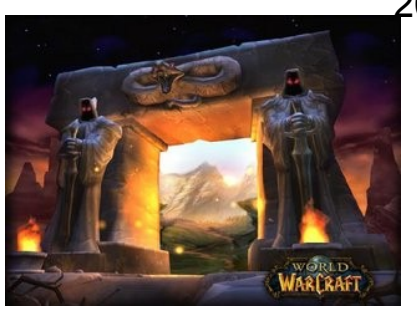
“Hakkar the Soulflayer” monster

- Casts a powerful “Corrupted blood” spell
- Infectious!
- Epidemic started



McAfee

What went wrong?



- Timeline
  - WoW 1.7 went out on 13 Sep 2005
  - Epidemics started on several servers on 15 Sep 2005
  - Source - Hakkar monster from Zul'Gurub instance dungeon
- "Corrupted blood" - spell parameters:
  - Damage: 200 HP (60+ level players have 4000-5000 HP)
  - Duration: 10 sec (every 2 seconds)
  - Radius: 100 yards (infectious with 100% probability!)
  - By design it should be very limited in time and space…
  - But spreads from a player to a player (+ NPCs and pets)
- And could be "conserved" in an un-summoned pet!
  - A design oversight (due to environment complexity)

Corrupted blood disease in WoW

- Infected Ironforge city:



McAfee®

Corrupted blood disease (video)

- Corpses in the city:



McAfee

Dead characters everywhere (skeletons)

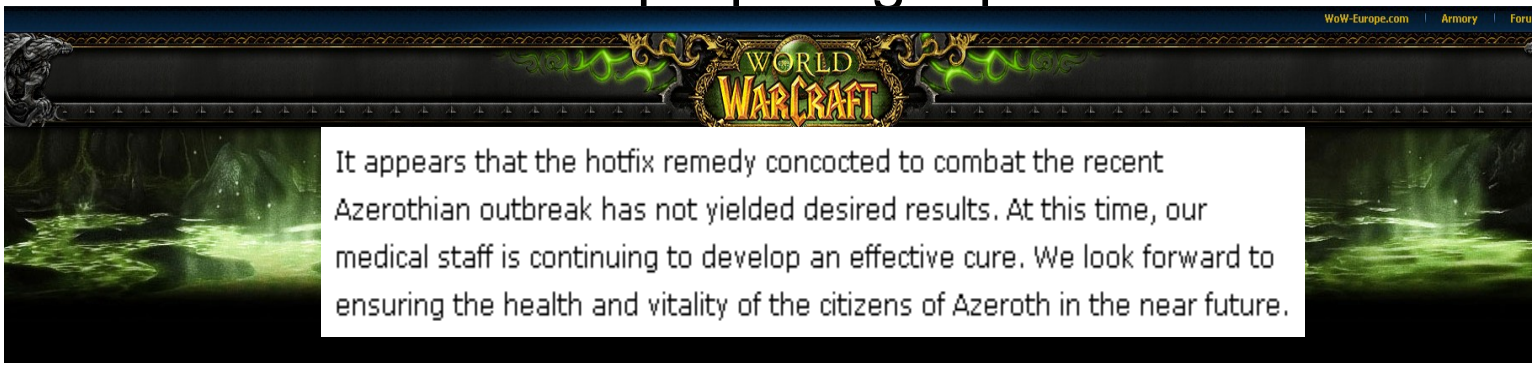
- Fortunately, in WoW death is “temporary”
- Game was effectively unplayable for many days – a lot of upset users



McAfee®

Reaction

- Official reaction while preparing a patch:



- Many players excited: ”first proper world event”
- Fix in 1.8 (10 Oct 2005): “Fixed a bug that would allow Hakkar's Corrupted Blood ability to target pets.”
- Fix in 1.9.3 (07 Feb 2006): “Corrupted Blood now deals direct damage with a following damage over time effect and **no longer spreads to others in the raid**.”

McAfee

What did we learn?



- Replication went out of control (Chernobyl!)
- If it is implemented in a complex environment it is hard to predict all possible scenarios
  - To some extent Already.71 too
  - The Morris worm
  - Internet is a lot more complex

W32/Nachi – a vulnerability-patching worm.

McAfee®

W32/Nachi (aka W32/Welchia)



- W32/MSBlaster (aka LovSan) – 11 Aug 2003
- W32/Nachi – released 18 Aug 2003
  - Contains code to download and run Microsoft's patch for MS03-026 RpcDcom vulnerability
  - Overloaded many networks
  - But, to give credit to the author, was time-limited (removes itself in 2004)
  - At the time of its "suicide" ~30,000 IPs had W32/Nachi

What did we learn?



- Beneficial worms can and will contain bugs
- W32/Nachi lacked control in two areas
  - Network load
  - Did not die as quickly as was expected
- Internet is a very complex environment

To be or not to be? Pros and cons.

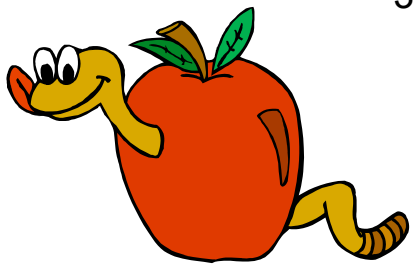
Pro and contra



- Dr. Bontchev's «Are "Good" Computer Viruses Still a Bad Idea?» 1994 paper:
  - A useful worm can be created but with all the controls in place most people would not consider it to be a virus
- Arguments for:
  - Compress/encrypt files/disks
  - "Maintenance" worm
  - Quicker (and forceful) patching
  - Remove bad worms
  - Better administration through computers' discovery
  - Support human rights (censorship in China)

McAfee

Patching using replication



- Very quick (Warhol and flash) worms
- Patching needs to outrun worm propagation
- If there is a replicating patch – should it be released?
- No, because:
  - It is technically risky
  - In a rush there is unlikely to be enough time for proper QA
  - It is legal minefield too

Conclusions



- Replicative property is a rather dangerous technology:
  - Available to everybody
  - Control is hard (WoW, Nachi)
- Can a useful virus be created? Yes.
- Is it dangerous? Yes, and more then we expect.
- Messing with infections or viral properties?
  Not a good idea.

Key references



- Already:
  - http://home.flash.net/~hoselton/pubs/mah_010.txt
- Wow:
  - http://www.wowwiki.com/Corrupted_Blood
  - http://www.securityfocus.com/news/11330
  - http://www.worldofwarcraft.com/patchnotes/patch1p7.html
  - http://events.ccc.de/congress/2007/Fahrplan/events/2322.en.html
- Nachi:
  - http://vil.nai.com/vil/content/v_100559.htm
  - P.Szor “Virus Research and Defense”, Symantec Press, ISBN 0-321-30454-3
- Bad viruses:
  - http://www.people.frisk-software.com/~bontchev/papers/goodvir.html (by V.Bontchev)
  - http://www.avertlabs.com/research/blog/index.php/2008/02/18/friendly-worms-facing-l (and see a comment by V.Bontchev to this blog)
- Good viruses:
  - http://pages.cpsc.ucalgary.ca/~aycock/papers/china.pdf

McAfee

Questions, please



Email: mig@mcafee.com

McAfee