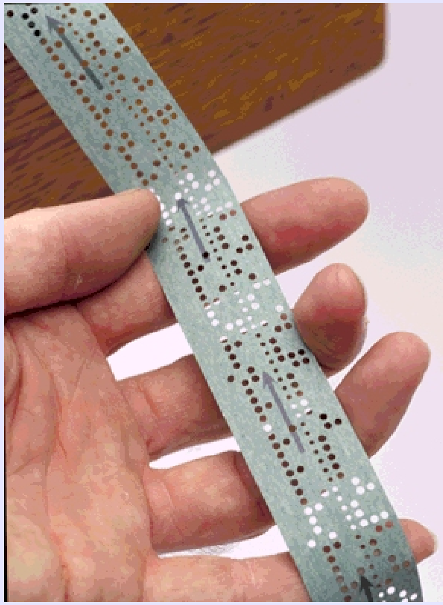
The biggest **MISTAKES** of the antivirus history

Introduction



István Csizmazia-Darab
[Rambo]

http://antivirus.blog.hu

1979-1980:	FÜTI, R20/R40 Computer operator
1981-1987:	HUNGAROTON Records Inc., technical assistant, C64
1988-1990:	Volán Tefu Inc., IBM PC-XT, programmer
1990-2000:	ERŐTERV Inc., 286, 386, 486, programmer + network virus admin
2001-2003:	2F Ltd., F-Secure & Kaspersky support + Vírus Híradó editor in chief
2003-2005:	IDG PC World, Online-editor, journalist, technical support
2006-2007:	Virus Buster Ltd., Virus-analyst, Online-editor, journalist
2007-2014:	Sicontact Ltd., IT security specialist, journalist

What will be discussed?

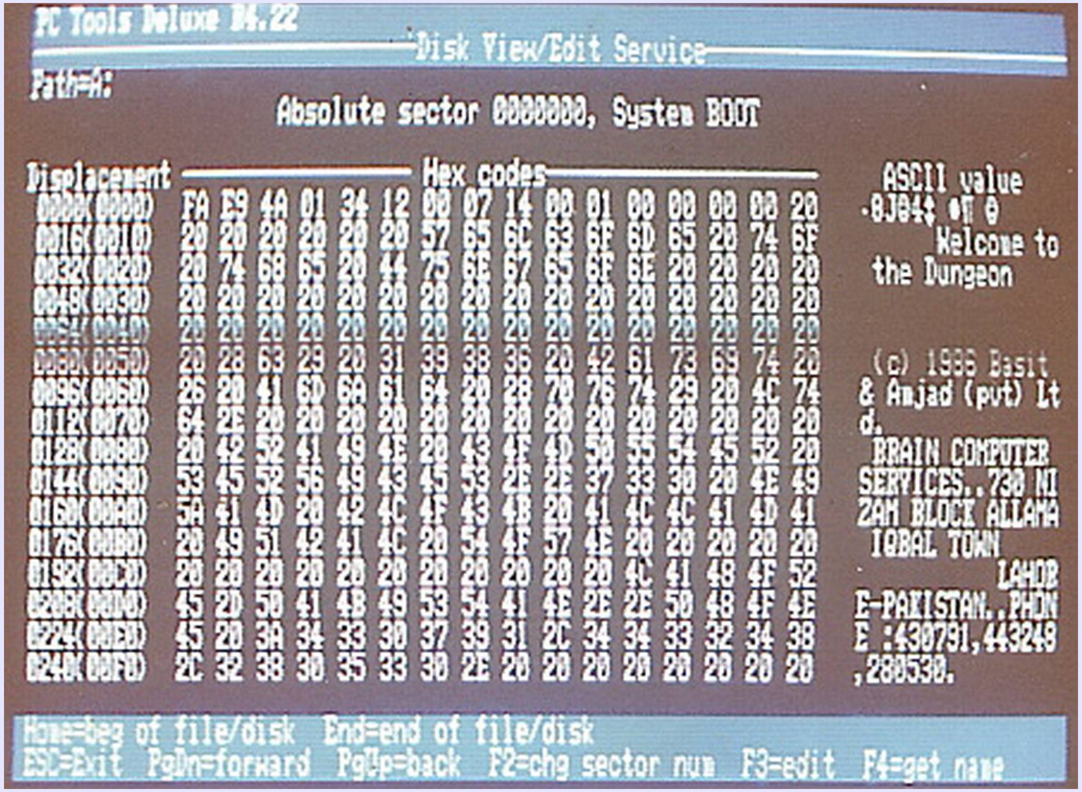
- Where we started?
- Players in the Computer economy (AVz, USERz, BGUYz, DEVELOPz)
- Who made the most crucial mistake?
- Conclusion or something like that

Where we started?

"Dwell on the past and you'll lose an eye;
forget the past and you'll lose both eyes"
Alexander Solzhenitsyn: The Gulag Archipelago

1986.

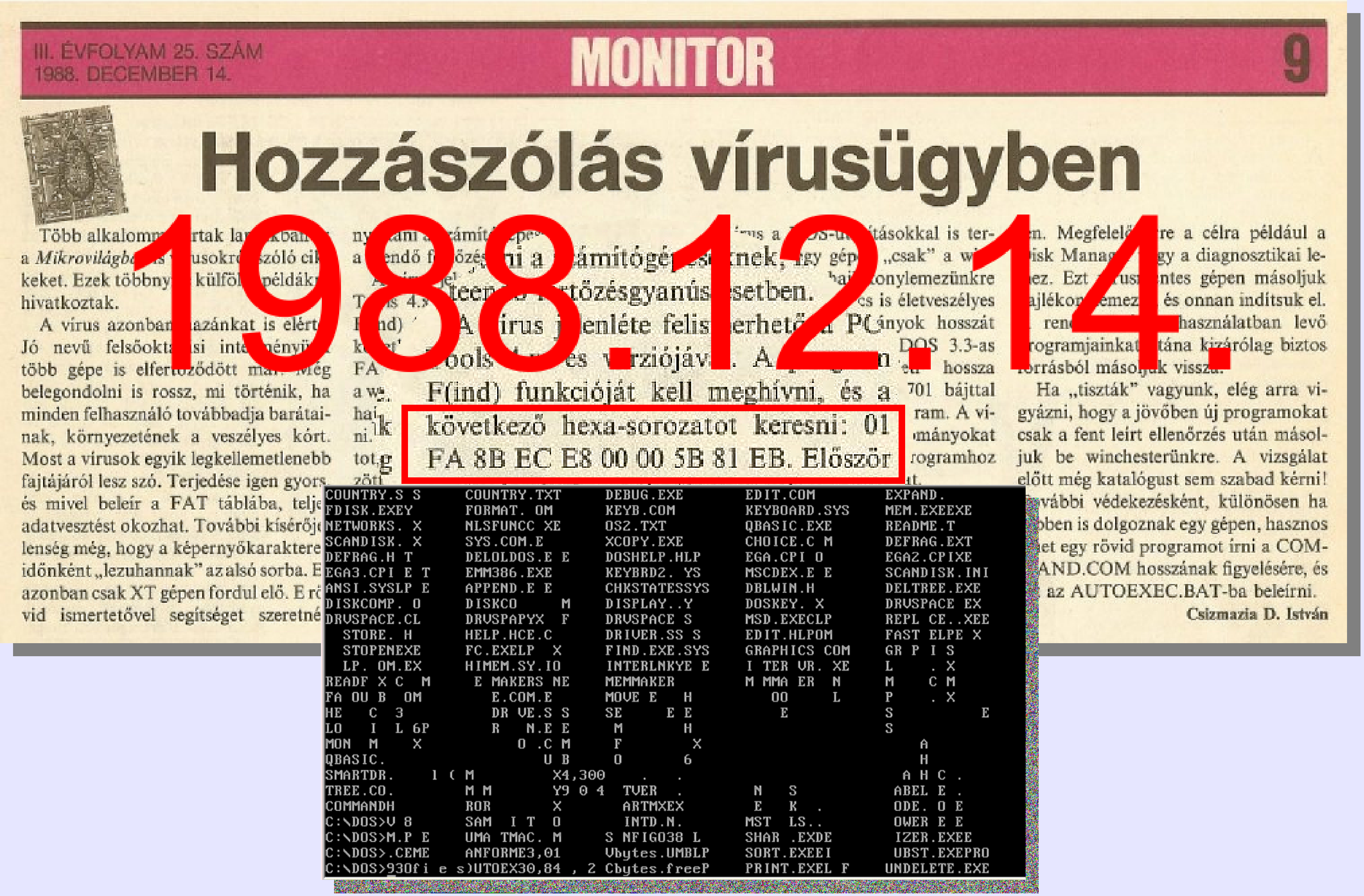
- Ronald Reagen is the President of the USA
- Super Bowl: Chicago d. New England (46-10)
- Wimbledon: Boris Becker d. Ivan Lendl (6-4 6-3 7-5)
- Brain virus (Pakistan): name, address, phone number :-)



```
PC Tools Deluxe R4.22
                              Disk View/Edit Service
Path=A:
                Absolute sector 0000000, System BOOT

Displacement  ----------------Hex codes-----------------------    ASCII value
0000(0000)  FA E9 4A 01 34 12 00 07 14 00 01 00 00 00 00 20   .8J04‡ •╥ Θ
0016(0010)  20 20 20 20 20 20 57 65 6C 63 6F 6D 65 20 74 6F         Welcome to
0032(0020)  20 74 68 65 20 44 75 6E 67 65 6F 6E 20 20 20 20    the Dungeon
0048(0030)  20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
0064(0040)  20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
0080(0050)  20 28 63 29 20 31 39 38 36 20 42 61 73 69 74 20    (c) 1986 Basit
0096(0060)  26 20 41 6D 6A 61 64 20 28 70 76 74 29 20 4C 74   & Amjad (pvt) Lt
0112(0070)  64 2E 20 20 20 20 20 20 20 20 20 20 20 20 20 20   d.
0128(0080)  20 42 52 41 49 4E 20 43 4F 4D 50 55 54 45 52 20    BRAIN COMPUTER
0144(0090)  53 45 52 56 49 43 45 53 2E 2E 37 33 30 20 4E 49   SERVICES..730 NI
0160(00A0)  5A 41 4D 20 42 4C 4F 43 4B 20 41 4C 4C 41 4D 41   ZAM BLOCK ALLAMA
0176(00B0)  20 49 51 42 41 4C 20 54 4F 57 4E 20 20 20 20 20    IQBAL TOWN
0192(00C0)  20 20 20 20 20 20 20 20 20 20 20 4C 41 48 4F 52              LAHOR
0208(00D0)  45 2D 50 41 4B 49 53 54 41 4E 2E 2E 50 48 4F 4E   E-PAKISTAN..PHON
0224(00E0)  45 20 3A 34 33 30 37 39 31 2C 34 34 33 32 34 38   E :430791,443248
0240(00F0)  2C 32 38 30 35 33 30 2E 20 20 20 20 20 20 20 20   ,280530.

Home=beg of file/disk  End=end of file/disk
ESC=Exit  PgDn=forward  PgUp=back  F2=chg sector num  F3=edit  F4=get name
```

Where we started?

"VIRUSCAN version 0.3V19 can identify 19 major virus strains and numerous sub-varieties for each strain. The 19 viruses include the ten most common viruses which account for over 90% of all reported PC infections."



III. ÉVFOLYAM 25. SZÁM
1988. DECEMBER 14.

MONITOR 9

Hozzászólás vírusügyben

1988.12.14.

Több alkalomm[illegible]rtak la[illegible]kban a *Mikrovilágba*[illegible] [illegible]usokr[illegible]szóló cik[illegible]keket. Ezek többny[illegible] külföl[illegible] példák[illegible] hivatkoztak.

A vírus azonban [illegible]azánkat is elérte. Jó nevű felsőokt[illegible]si int[illegible]ényü[illegible] több gépe is elfertőződött m[illegible]. Még belegondolni is rossz, mi történik, ha minden felhasználó továbbadja barátainak, környezetének a veszélyes kórt. Most a vírusok egyik legkellemetlenebb fajtájáról lesz szó. Terjedése igen gyors, és mivel beleír a FAT táblába, telje[illegible] adatvesztést okozhat. További kísérője[illegible] lenség még, hogy a képernyőkaraktere[illegible] időnként „lezuhannak" az alsó sorba. E[illegible] azonban csak XT gépen fordul elő. E rö[illegible]vid ismertetővel segítséget szeretné[illegible]

ny[illegible] a [illegible]ámít[illegible] a [illegible]endő f[illegible]özé[illegible] T[illegible]s 4.[illegible] F[illegible]nd) k[illegible] FA a w[illegible] hai[illegible] ni. tot[illegible] zött

[illegible]ni a [illegible]ámítógép[illegible]nek, [illegible] teen[illegible] [illegible]rtőzésgyanús [illegible]setben.

A [illegible]írus j[illegible]enléte felis[illegible]erhető [illegible] P[illegible] [illegible]ools [illegible]es v[illegible]rziójáv[illegible]. A [illegible] F(ind) funkcióját kell meghívni, és a következő hexa-sorozatot keresni: 01 FA 8B EC E8 00 00 5B 81 EB. Először

[illegible]rus a [illegible]S-u[illegible]tásokkal is ter[illegible] „csak" a w[illegible] [illegible]ha[illegible]onylemezünkre [illegible]cs is életveszélyes [illegible]ányok hosszát DOS 3.3-as [illegible] hossza [illegible]701 bájttal [illegible]ram. A ví[illegible]mányokat [illegible]rogramhoz [illegible]t.

[illegible]n. Megfelel[illegible]re a célra például a [illegible]isk Manag[illegible]gy a diagnosztikai le[illegible]ez. Ezt [illegible]us[illegible]ntes gépen másoljuk [illegible]ajlékon[illegible]emez[illegible] és onnan indítsuk el. [illegible] ren[illegible] használatban levő [illegible]rogramjainkat [illegible]tána kizárólag biztos forrásból másoljuk vissza.

Ha „tiszták" vagyunk, elég arra vigyázni, hogy a jövőben új programokat csak a fent leírt ellenőrzés után másoljuk be winchesterünkre. A vizsgálat előtt még katalógust sem szabad kérni! [illegible]vábbi védekezésként, különösen ha [illegible]bben is dolgoznak egy gépen, hasznos [illegible]et egy rövid programot írni a COM[illegible]AND.COM hosszának figyelésére, és [illegible] az AUTOEXEC.BAT-ba beleírni.

Csizmazia D. István

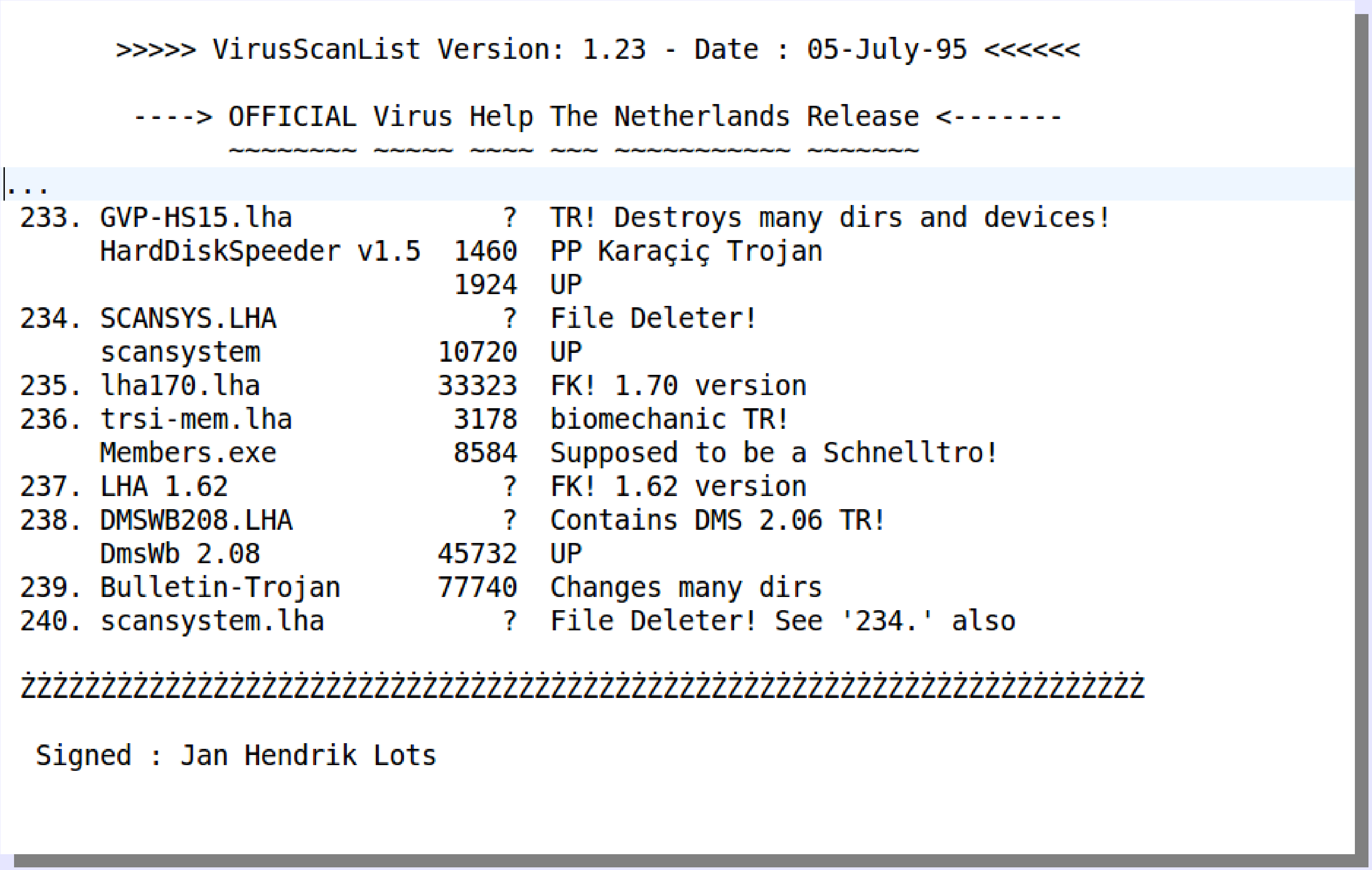
```
COUNTRY.S S      COUNTRY.TXT      DEBUG.EXE        EDIT.COM         EXPAND.
FDISK.EXEY       FORMAT. OM       KEYB.COM         KEYBOARD.SYS     MEM.EXEEXE
NETWORKS. X      NLSFUNCC XE      OSZ.TXT          QBASIC.EXE       README.T
SCANDISK. X      SYS.COM.E        XCOPY.EXE        CHOICE.C M       DEFRAG.EXT
DEFRAG.H T       DELOLDOS.E E     DOSHELP.HLP      EGA.CPI O        EGAZ.CPIXE
EGA3.CPI E T     EMM386.EXE       KEYBRDZ. YS      MSCDEX.E E       SCANDISK.INI
ANSI.SYSLP E     APPEND.E E       CHKSTATESSYS     DBLWIN.H         DELTREE.EXE
DISKCOMP. O      DISKCO      M    DISPLAY..Y       DOSKEY. X        DRVSPACE EX
DRVSPACE.CL      DRVSPAPYX   F    DRVSPACE S       MSD.EXECLP       REPL CE..XEE
  STORE. H       HELP.HCE.C       DRIVER.SS S      EDIT.HLPOM       FAST ELPE X
  STOPENEXE      FC.EXELP   X     FIND.EXE.SYS     GRAPHICS COM     GR P I S
  LP. OM.EX      HIMEM.SY.IO      INTERLNKYE E     I TER VR. XE     L     . X
READF X C  M      E MAKERS NE     MEMMAKER         M MMA ER  N      M     C M
FA OU B  OM         E.COM.E       MOVE E    H        OO      L      P     . X
HE   C  3           DR VE.S S     SE       E E        E             S          E
LO   I  L 6P        R   N.E E      M        H                       S
MON  M    X            O .C M      F          X                        A
QBASIC.                   U B      O        6                          H
SMARTDR.    1 ( M          X4,300      .    .                        A H C .
TREE.CO.          M M      Y9 0 4  TVER    .         N   S          ABEL E .
COMMANDH          ROR         X      ARTMXEX         E   K  .       ODE. O E
C:\DOS>V 8        SAM  I T    O      INTD.N.        MST  LS..       OWER E E
C:\DOS>M.P E      UMA TMAC. M     S NFIG038 L      SHAR .EXDE       IZER.EXEE
C:\DOS>.CEME      ANFORME3,01     Vbytes.UMBLP     SORT.EXEEI       UBST.EXEPRO
C:\DOS>930fi e s)UTOEX30,84 , 2 Cbytes.freeP     PRINT.EXEL F     UNDELETE.EXE
```

02.07.1989

- Pakistani Brain
- Jerusalem
- Alameda
- Cascade (1701)
- Ping Pong
- Stoned
- Lehigh
- Den Zuk
- Datacrime (1280)
- Fu Manchu

Where we started?

July 1995
- 240 viruses alltogether (2014 >= 200 million uniq samples)
- VIRNET BBS, 300 baud modem
- Let's Nostalgia: Slovakian Antivirus Center - www.sac.sk



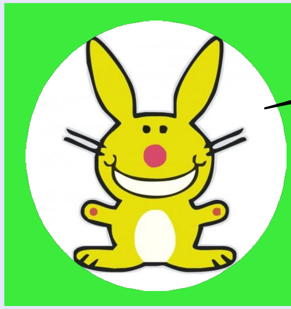
```
      >>>>> VirusScanList Version: 1.23 - Date : 05-July-95 <<<<<<

       ----> OFFICIAL Virus Help The Netherlands Release <-------
             ~~~~~~~~ ~~~~~ ~~~~ ~~~ ~~~~~~~~~~~ ~~~~~~~
...
233. GVP-HS15.lha             ?  TR! Destroys many dirs and devices!
     HardDiskSpeeder v1.5  1460  PP Karaçiç Trojan
                           1924  UP
234. SCANSYS.LHA              ?  File Deleter!
     scansystem           10720  UP
235. lha170.lha           33323  FK! 1.70 version
236. trsi-mem.lha          3178  biomechanic TR!
     Members.exe           8584  Supposed to be a Schnelltro!
237. LHA 1.62                 ?  FK! 1.62 version
238. DMSWB208.LHA             ?  Contains DMS 2.06 TR!
     DmsWb 2.08           45732  UP
239. Bulletin-Trojan      77740  Changes many dirs
240. scansystem.lha           ?  File Deleter! See '234.' also

żżżżżżżżżżżżżżżżżżżżżżżżżżżżżżżżżżżżżżżżżżżżżżżżżżżżżżżżżżżżżżżżżżżżżżżż

 Signed : Jan Hendrik Lots
```

Players in the Computer economy

I. AV labors and industry

II. Users

III. Bad guys



IV. OS and Application developers

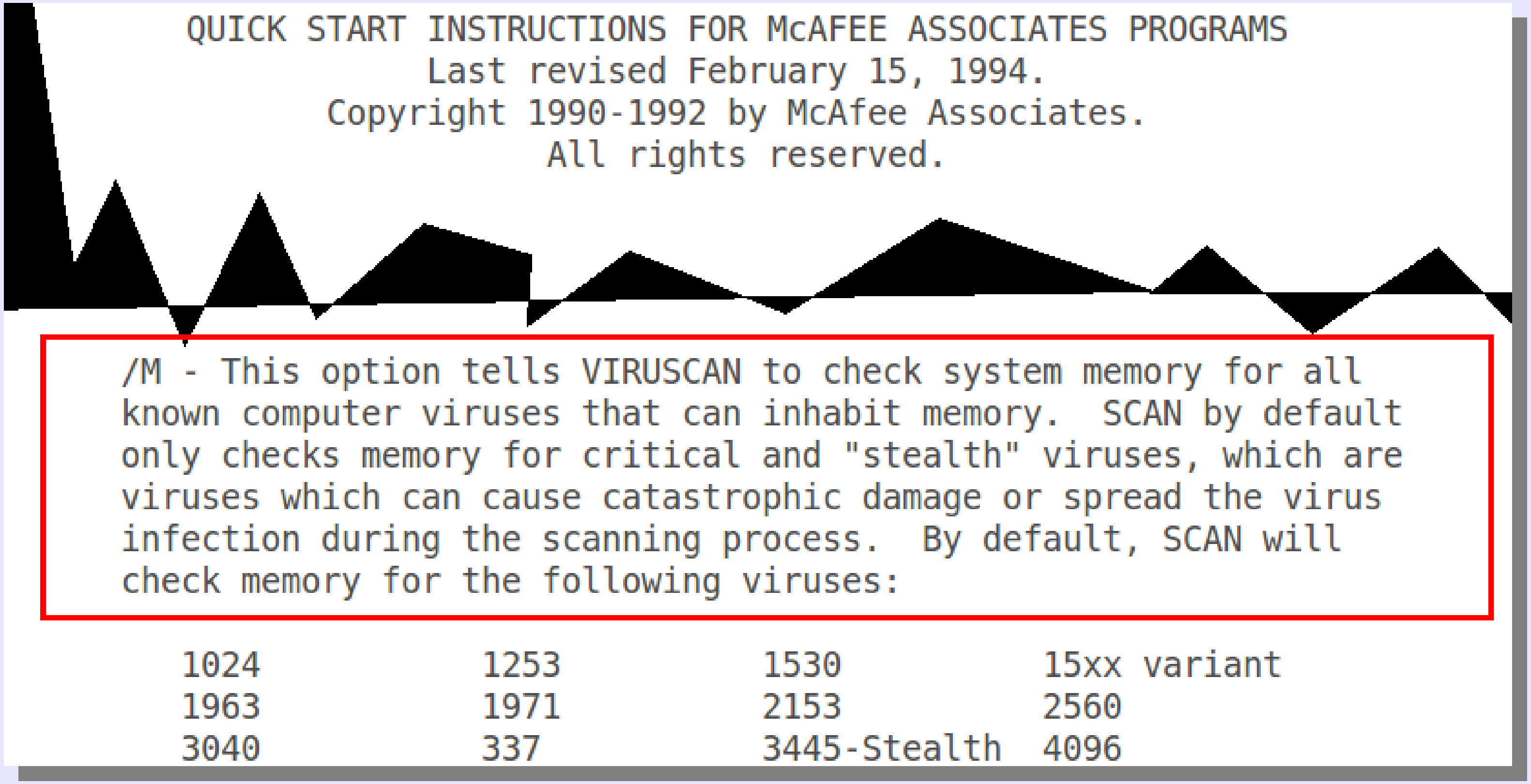
I just realized,
but I don't care...

Only the virus writers are responsible?

Let's take a tour, which participant made more foolish mistakes!

Unexpected changes to the default values

- 15.07.1994 McAfee VIRUSSCAN.EXE 1.17 version
- Suddenly checks ONLY the „common viruses???” in the memory by default
- We have to notice and manually override this option with „/M" command



```
           QUICK START INSTRUCTIONS FOR McAFEE ASSOCIATES PROGRAMS
                       Last revised February 15, 1994.
                   Copyright 1990-1992 by McAfee Associates.
                           All rights reserved.

     /M - This option tells VIRUSCAN to check system memory for all
     known computer viruses that can inhabit memory.  SCAN by default
     only checks memory for critical and "stealth" viruses, which are
     viruses which can cause catastrophic damage or spread the virus
     infection during the scanning process.  By default, SCAN will
     check memory for the following viruses:

        1024           1253           1530           15xx variant
        1963           1971           2153           2560
        3040           337            3445-Stealth   4096
```

The sky is blue, the plagiarist copies

- January 2010: about 50,000 samples/day

- Kaspersky suspects stolen detections

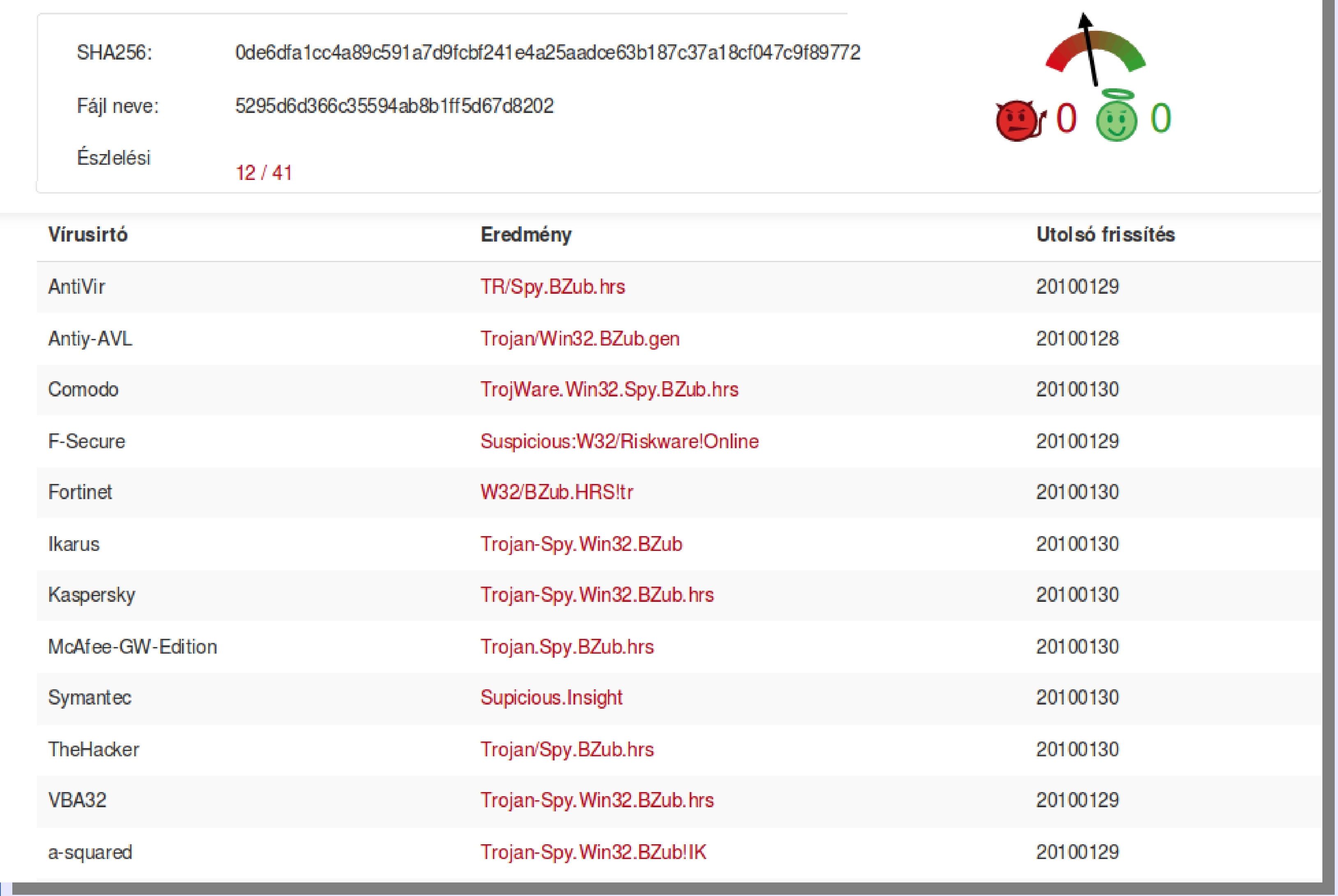
- Uploaded 10 clean samples ("Hello World" with Linux mingw crosscompiler) with fake virusnames to VirusTotal system

- "Trojan-Downloader.Win32.Zlob.bmwy", "Trojan-Spy.Win32.BZub.hrs" and "Trojan.Win32.KillWin.se" were born :-)

- After 10 days 12-14 additional AV vendors „detect” them

- 9 of them with the same name: a-squred, AntiVir, Antiy-AVL, Comodo, Fortinet, Ikarus, McAfee-GW-Edition, TheHacker, VBA32

I. AV labors and industry



SHA256:	0de6dfa1cc4a89c591a7d9fcbf241e4a25aadce63b187c37a18cf047c9f89772
Fájl neve:	5295d6d366c35594ab8b1ff5d67d8202
Észlelési	12 / 41

0 0

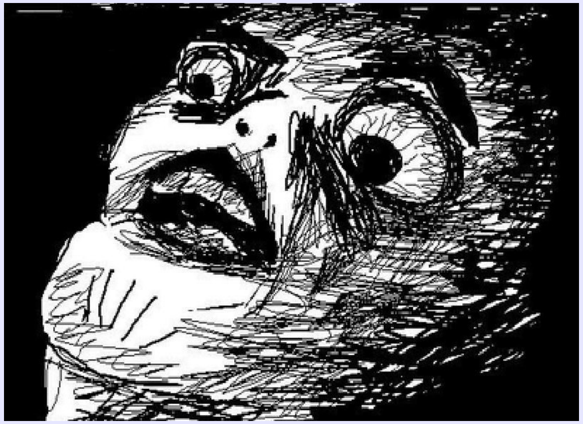
Vírusirtó	Eredmény	Utolsó frissítés
AntiVir	TR/Spy.BZub.hrs	20100129
Antiy-AVL	Trojan/Win32.BZub.gen	20100128
Comodo	TrojWare.Win32.Spy.BZub.hrs	20100130
F-Secure	Suspicious:W32/Riskware!Online	20100129
Fortinet	W32/BZub.HRS!tr	20100130
Ikarus	Trojan-Spy.Win32.BZub	20100130
Kaspersky	Trojan-Spy.Win32.BZub.hrs	20100130
McAfee-GW-Edition	Trojan.Spy.BZub.hrs	20100130
Symantec	Supicious.Insight	20100130
TheHacker	Trojan/Spy.BZub.hrs	20100130
VBA32	Trojan-Spy.Win32.BZub.hrs	20100129
a-squared	Trojan-Spy.Win32.BZub!IK	20100129

- Press conference in Moscow, AMTSO dissociates, the TheRegister criticizes

Strange testing conditions

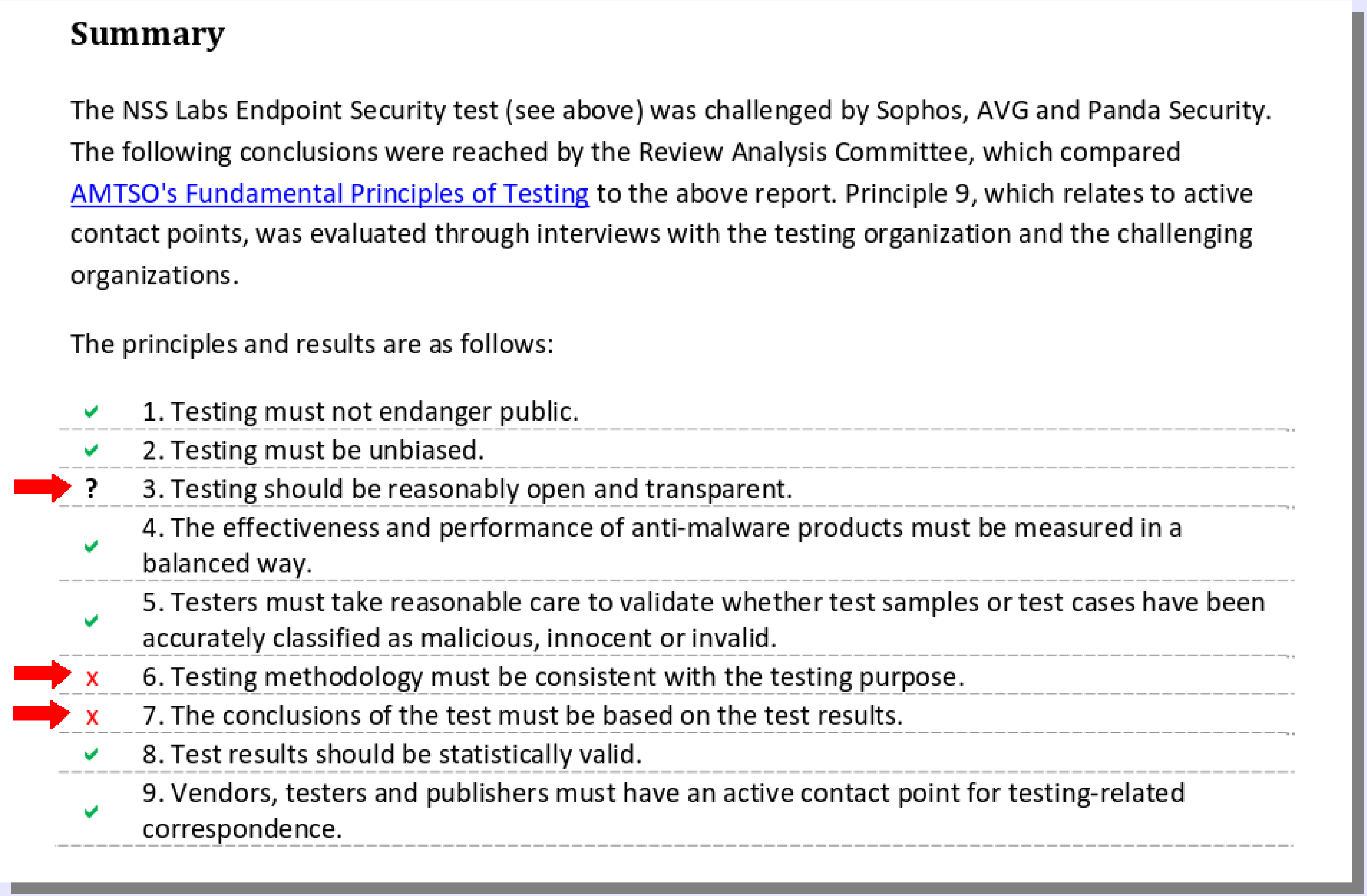
- 08.09.2009: NSS Labs published its review analysis of the Endpoint Security Test
- Strange testing conditions but was not published
- There is no relationship with the manufacturers, therefore they couldn't check and correct the problems
- The conclusions of the test didn't base on the test results
- You can buy the detailed test results for 2000 USD

- Unorthodox method ;-) You can determine the test methodology for 5000 USD :-/
- 2010. Excluded from the AMTSO



Since correcting this error, many interesting and valuable researches have been made

I. AV labors and industry



Summary

The NSS Labs Endpoint Security test (see above) was challenged by Sophos, AVG and Panda Security. The following conclusions were reached by the Review Analysis Committee, which compared AMTSO's Fundamental Principles of Testing to the above report. Principle 9, which relates to active contact points, was evaluated through interviews with the testing organization and the challenging organizations.

The principles and results are as follows:

✓ 1. Testing must not endanger public.

✓ 2. Testing must be unbiased.

? 3. Testing should be reasonably open and transparent.

✓ 4. The effectiveness and performance of anti-malware products must be measured in a balanced way.

✓ 5. Testers must take reasonable care to validate whether test samples or test cases have been accurately classified as malicious, innocent or invalid.

x 6. Testing methodology must be consistent with the testing purpose.

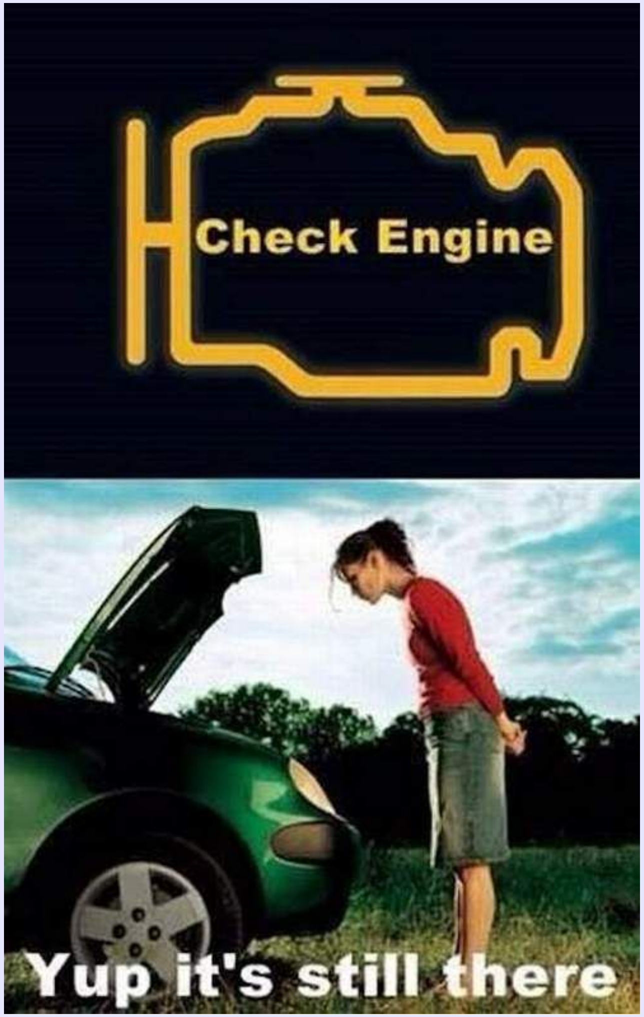
x 7. The conclusions of the test must be based on the test results.

✓ 8. Test results should be statistically valid.

✓ 9. Vendors, testers and publishers must have an active contact point for testing-related correspondence.

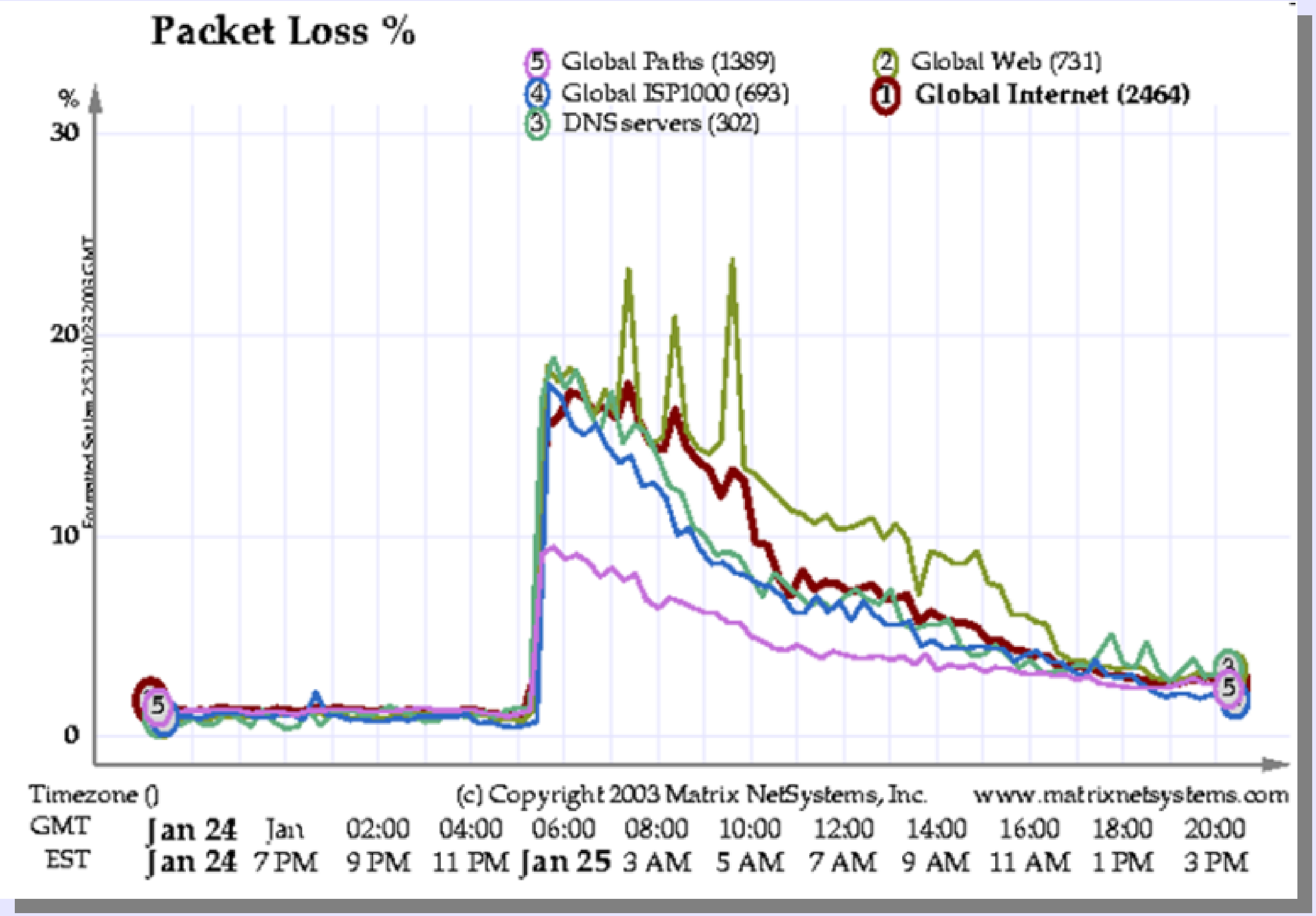
II. Users

Neglect Servers updates



- 01.25.2003: SQL Slammer/Zaphire worm
- MS SQL Server 2000 vulnerability - buffer overflow
- The patch was issued in 2002 :-)
- WoooW! - Importance of Security updates
- „Flashworm”, no infected file, just in memory
- The AV-s there was no chance

II. Users

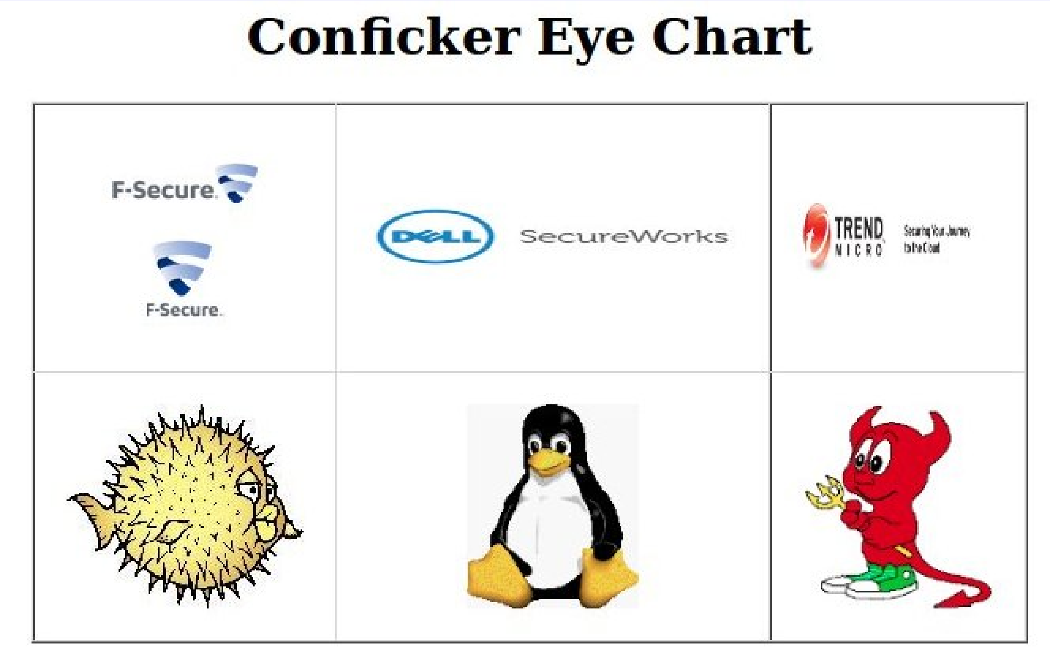


- 90% of PCs were infected in the first 10 minutes

- It caused a damage of 750 million USD

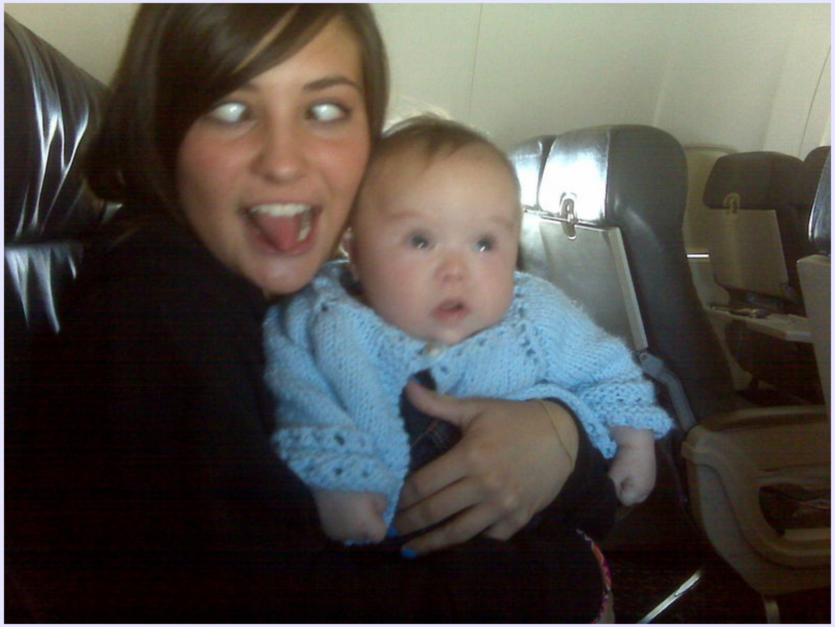
Neglect Desktop updates

- 2007. Win32/Conficker network worm
- Microsoft Windows MS08-067 security bulletin
- Exploits RPC (Remote Procedure Call)
- Contacts with remote servers
- Modifies local HOSTS file - blocks AV webpages
- Still in Virus top10 in 2014



II. Users

PEBKAC

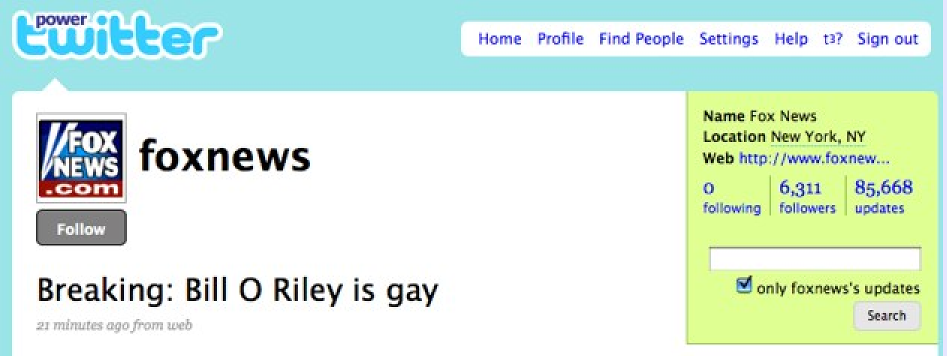


- Sept 2008 - Republican Senator Sarah Palin's Yahoo! mailbox was hacked and published

- NOT a virus, not a spyware, not a real hack, but a request new password trick

- The place and date of her birth was very easy to find out by searching with Google

- The "secret" security question: Where she met with her husband - in high school



foxnews

Breaking: Bill O Riley is gay

21 minutes ago from web

Name Fox News
Location New York, NY
Web http://www.foxnew...

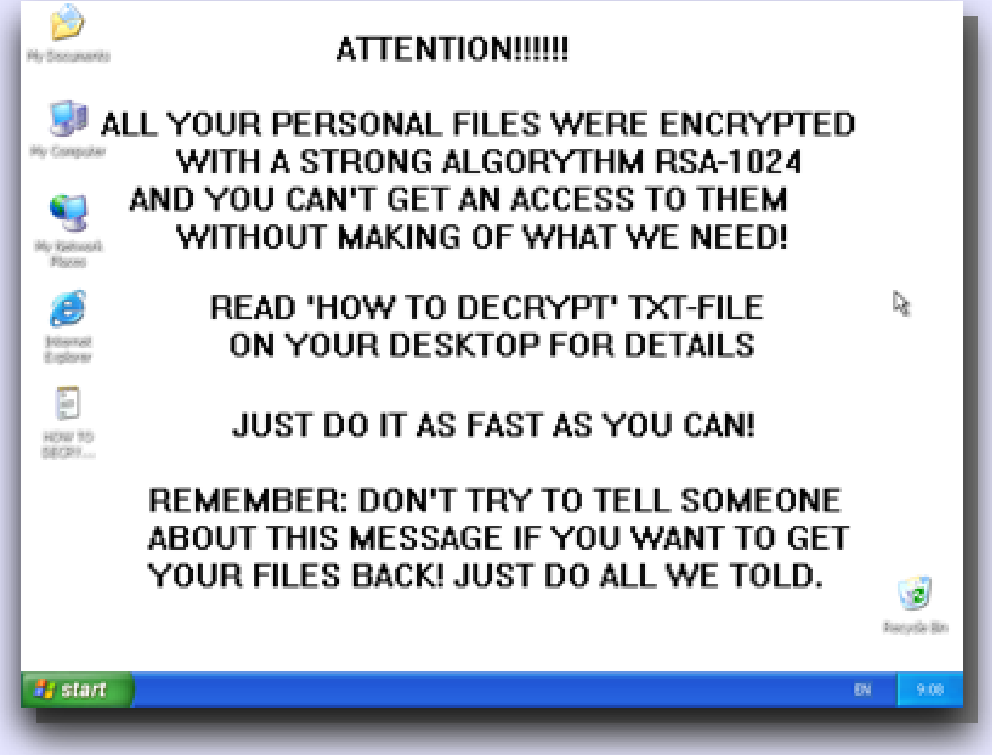
0 following | 6,311 followers | 85,668 updates

☑ only foxnews's updates

- Do not protect our secrets with public information!

- 01.06.2009 - Weak Password Brings ‘Happiness’ to Twitter Hacker (Obama, FoxNews, etc.)

Capital bug in the GPCode



ATTENTION!!!!!!

ALL YOUR PERSONAL FILES WERE ENCRYPTED
WITH A STRONG ALGORYTHM RSA-1024
AND YOU CAN'T GET AN ACCESS TO THEM
WITHOUT MAKING OF WHAT WE NEED!

READ 'HOW TO DECRYPT' TXT-FILE
ON YOUR DESKTOP FOR DETAILS

JUST DO IT AS FAST AS YOU CAN!

REMEMBER: DON'T TRY TO TELL SOMEONE
ABOUT THIS MESSAGE IF YOU WANT TO GET
YOUR FILES BACK! JUST DO ALL WE TOLD.

- 2008. GPCode – an old file encryptor ransom malware

- with strong, 1024 bit RSA encryption

- in the first PoC version it used simple deletion after encoding

- no overwriting, no wiping

- security specialist published it

- after a few weeks the bad guys corrected the mistake

III. Bad guys

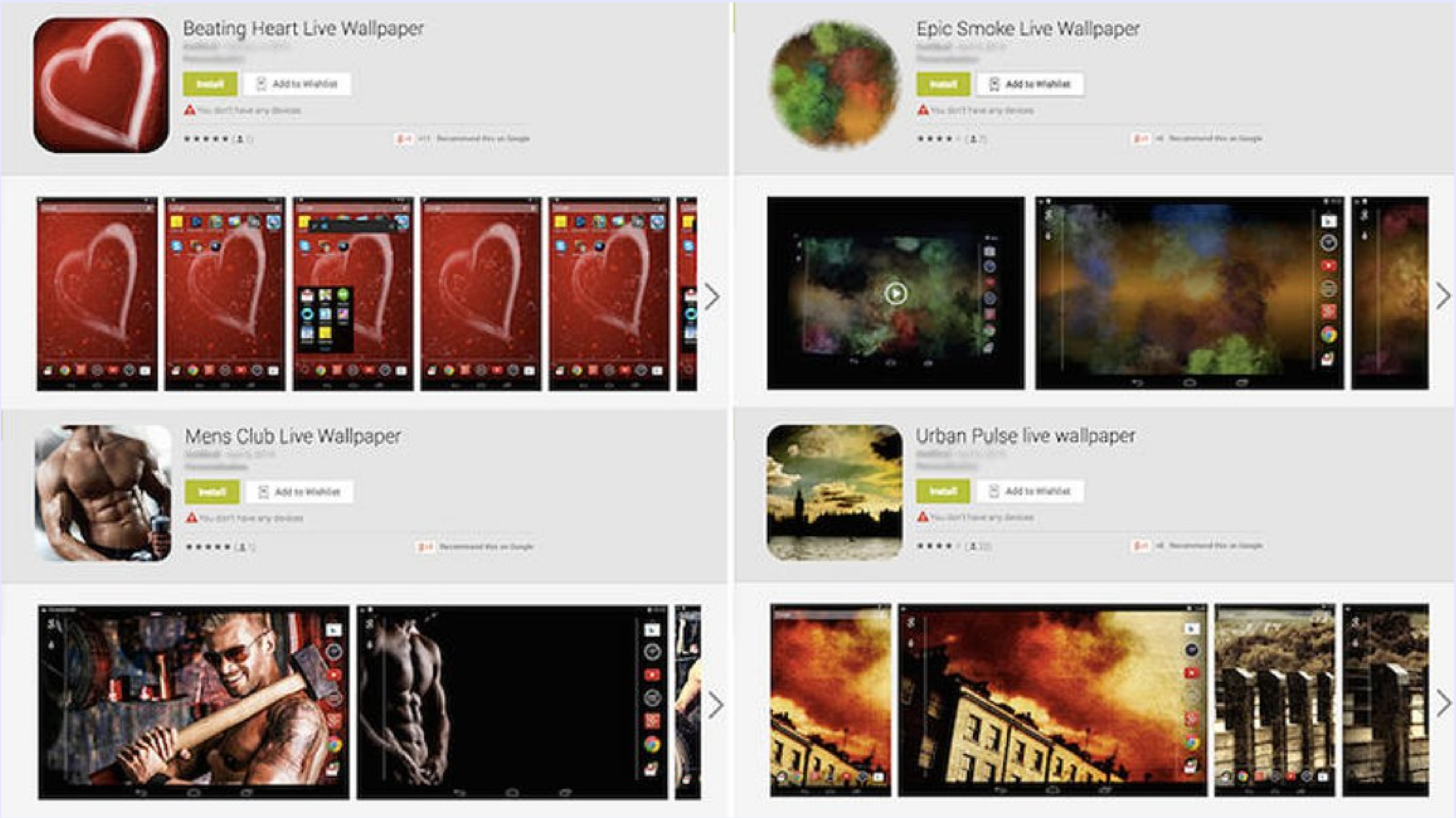
A plan without brain

- April 2014.: Bitcoin miner malware on the Google Play
- Bitcoin miner malware is a good idea on PCs, it generates significant revenue
- in a 2 mill. network 58,000 USD/day, 1.7 million USD/month (416 mHUF/month)

- But is it worth to run a zombinetwork on a weak Android hardware? (No :-)
- due to serious battery problems the trojan can only run in connected mode
- Checks the battery level in every 5th seconds
- Battery over 50% + connected to power + active screen turned off = Bitcoin mining
- being detected due to the rapid warming and the shortened battery time
- Dodgy, but the author certainly did not think it through

- **bad and VERY SLOW idea :-)**

III. Bad guys



Beating Heart Live Wallpaper

Epic Smoke Live Wallpaper

Mens Club Live Wallpaper

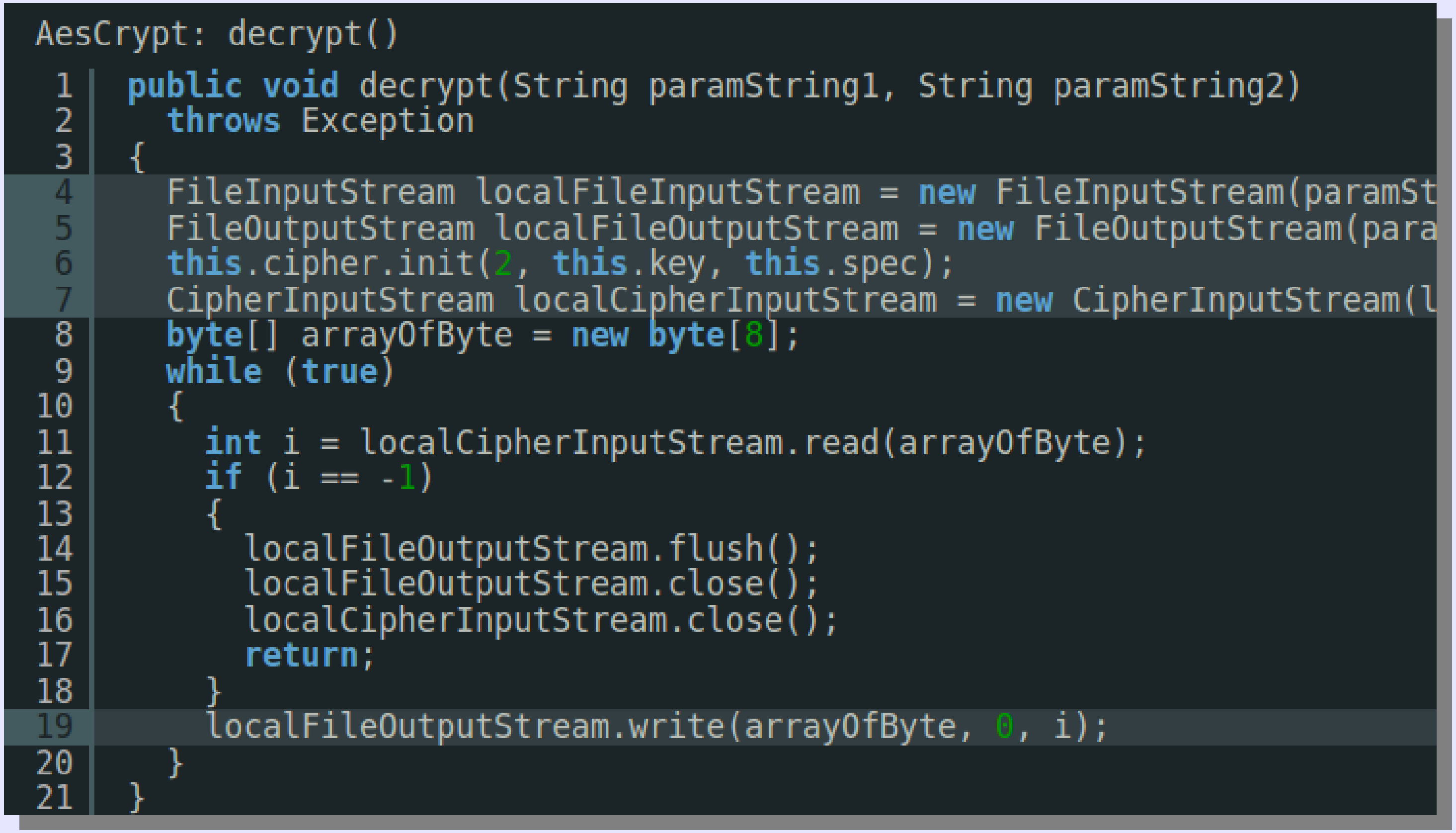
Urban Pulse live wallpaper

Bitcoin miner malware on the Google Play

Capital bug in the SimpLocker

- June 2014: Simplocker, the first encryption ransom malware on Android
- Reads the entire contents of the SD card, and then encrypts the data
- Restores only after the ransom was paid
- AES encoded files
- Encrypts all jpeg, jpg, png, bmp, gif, pdf, doc, docx, txt, avi, mkv, 3gp and mp4 files
- Demands ransom in Hrivnya (Ukrainian currency) in Russian language
- The C&C server registered via TOR .onion domain
- No Cryptolocker-like field for entering a payment code
- The remote C&C server will wait for the actual payment to unlock your device
- Fortunately, encryption did not happen to be perfect
- The decoding passwords were stored as fixed constants :-)

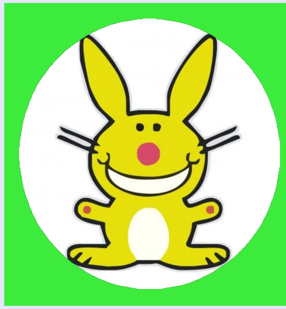
III. Bad guys



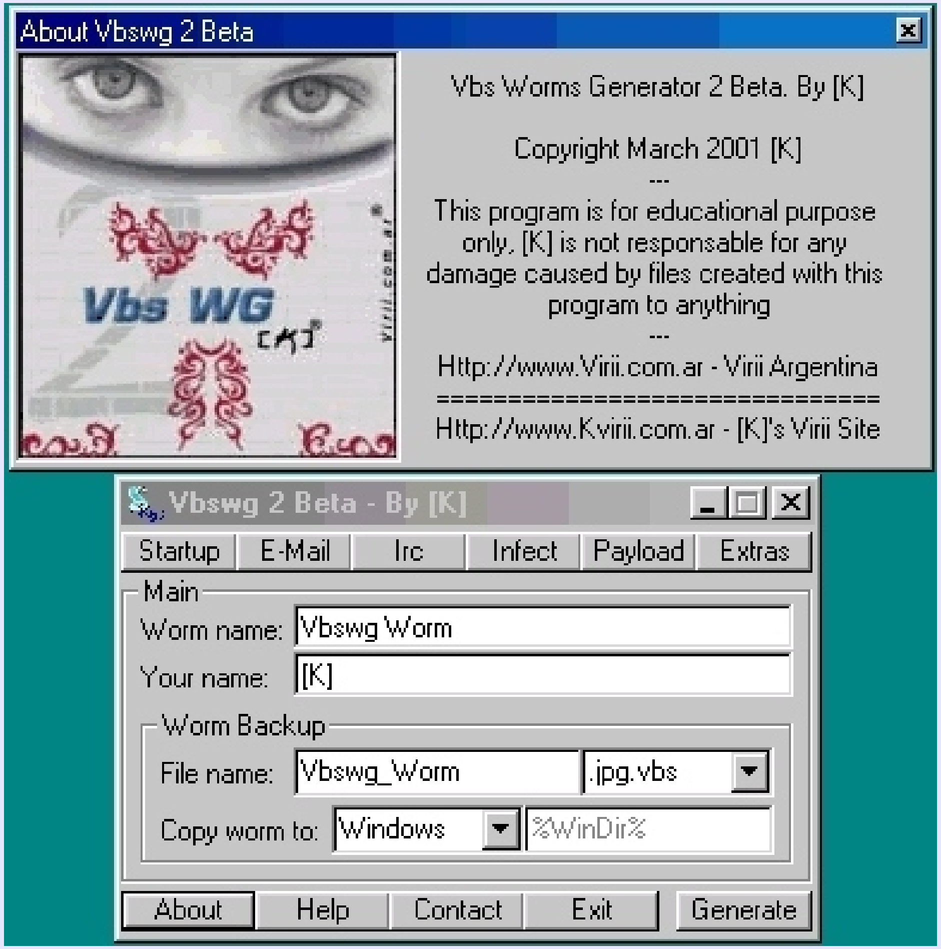
```
AesCrypt: decrypt()
 1  public void decrypt(String paramString1, String paramString2)
 2    throws Exception
 3  {
 4    FileInputStream localFileInputStream = new FileInputStream(paramSt
 5    FileOutputStream localFileOutputStream = new FileOutputStream(para
 6    this.cipher.init(2, this.key, this.spec);
 7    CipherInputStream localCipherInputStream = new CipherInputStream(l
 8    byte[] arrayOfByte = new byte[8];
 9    while (true)
10    {
11      int i = localCipherInputStream.read(arrayOfByte);
12      if (i == -1)
13      {
14        localFileOutputStream.flush();
15        localFileOutputStream.close();
16        localCipherInputStream.close();
17        return;
18      }
19      localFileOutputStream.write(arrayOfByte, 0, i);
20    }
21  }
```

Lines 4 and 5 create variables used for the file input and output. Line 6 initialises the cipher (to encrypt data). Line 7 is where the encryption occurs and line 19 writes the encrypted bytes to the output file.

- The AV vendors offer decryption tools, scripts
- July 2014: SimpLocker 2.0 - ZIP, 7z and RAR



1995. Microsoft – Macro viruses I.



Vbs Worms Generator 2 Beta. By [K]

Copyright March 2001 [K]

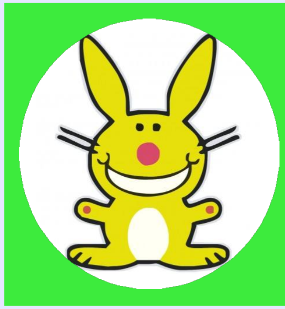
This program is for educational purpose only. [K] is not responsable for any damage caused by files created with this program to anything

---

Http://www.Virii.com.ar - Virii Argentina
===================================
Http://www.Kvirii.com.ar - [K]'s Virii Site

Worm name: Vbswg Worm
Your name: [K]
File name: Vbswg_Worm .jpg.vbs
Copy worm to: Windows %WinDir%

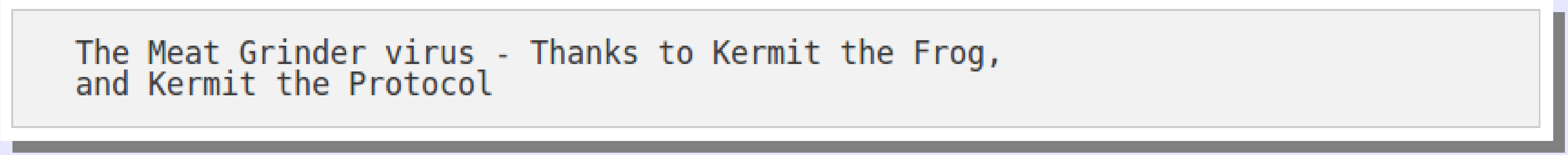
- 1995, the first macro viruses on Office 95
- The auto macros ran by default until 2000
- „Shifted” method, and was left open for 6 years
- The MS did not help, did not share the file structure info with AV vendors
- They had to debug and analyze office structure
- Easy way to make a lot of new variants
- Mass appearance of VBS Wormgenerator kits



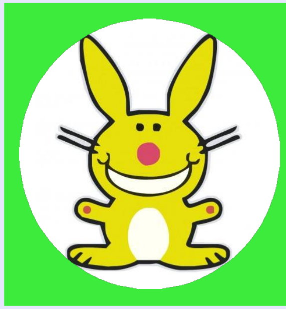
1997. Microsoft – Macro viruses II.

- Only a few – dozen – detections in the macro protection of Office 97 pack
- Unfortunately it was missing in the beta version, there was no protection at all :-(
- Initial macros were written in Word Basic, later made by Visual Basic for Applications
- They AUTOMATICALLY converted all WB macros into VBA macros in the Office documents
- previously there was only one macro virus version - for example Wazzu.A
- But „thanks” for the autoconversion, a huge amount of minor versions were born because of the different languages alone
- The number of macro viruses increased sharply :-O

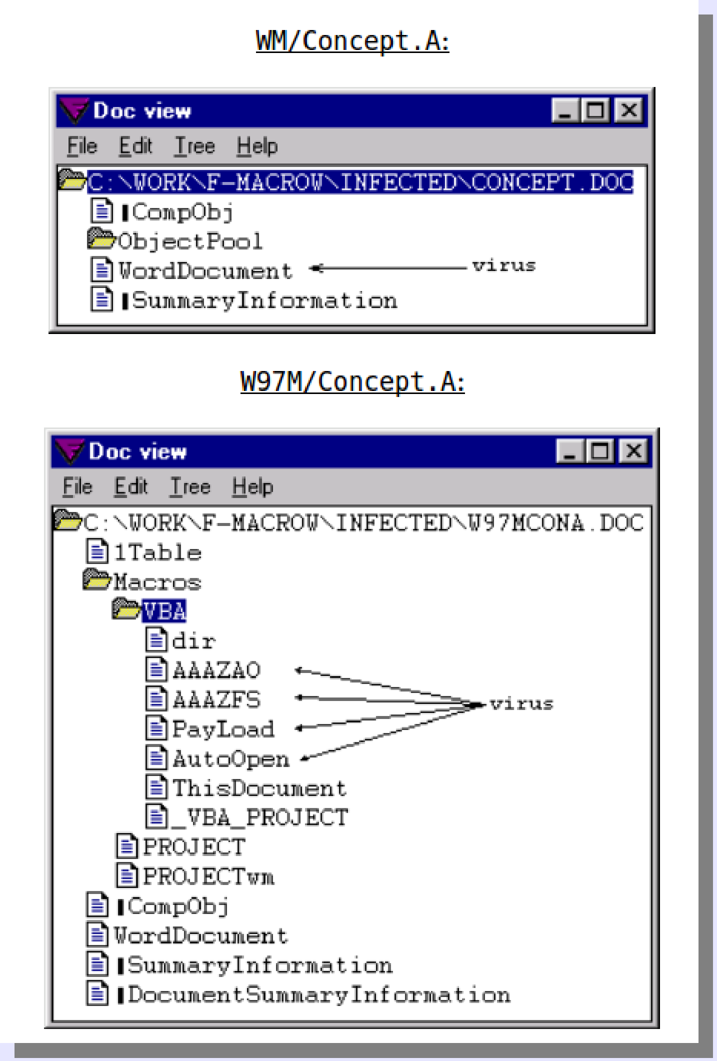
(The "Pros" and "Cons" of WordBasic Virus Upconversion - by Vesselin Bontchev)



```
   The Meat Grinder virus - Thanks to Kermit the Frog,
   and Kermit the Protocol
```



2014. Microsoft – Macro viruses III.



WM/Concept.A:

```
Doc view
File  Edit  Tree  Help
C:\WORK\F-MACROW\INFECTED\CONCEPT.DOC
  CompObj
  ObjectPool
  WordDocument  <-------------- virus
  SummaryInformation
```

W97M/Concept.A:

```
Doc view
File  Edit  Tree  Help
C:\WORK\F-MACROW\INFECTED\W97MCONA.DOC
  1Table
  Macros
    VBA
      dir
      AAAZAO   <--
      AAAZFS   <--
      PayLoad  <--   virus
      AutoOpen <--
      ThisDocument
      _VBA_PROJECT
    PROJECT
    PROJECTwm
  CompObj
  WordDocument
  SummaryInformation
  DocumentSummaryInformation
```

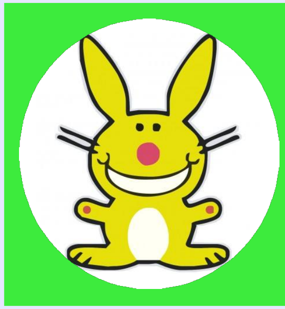
EPILOGUE

- Summer of 2014: Malicous macros came back, ex. Office files spam

- „invoice”, „parcel delivery”, „court summon”, etc.

- „please switch on the running of Macros” trick :-)

- from June to July the proportion of VBS worms increased from 6% to 28% (Sophos Lab)



1999. MS Outlook Express quick preview

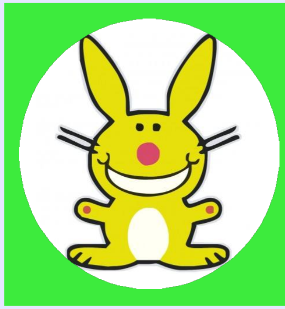
- 1999. KAK worm infected PCs via Outlook Express automatic mail preview

- It ran the Javascript code without opening the the mail

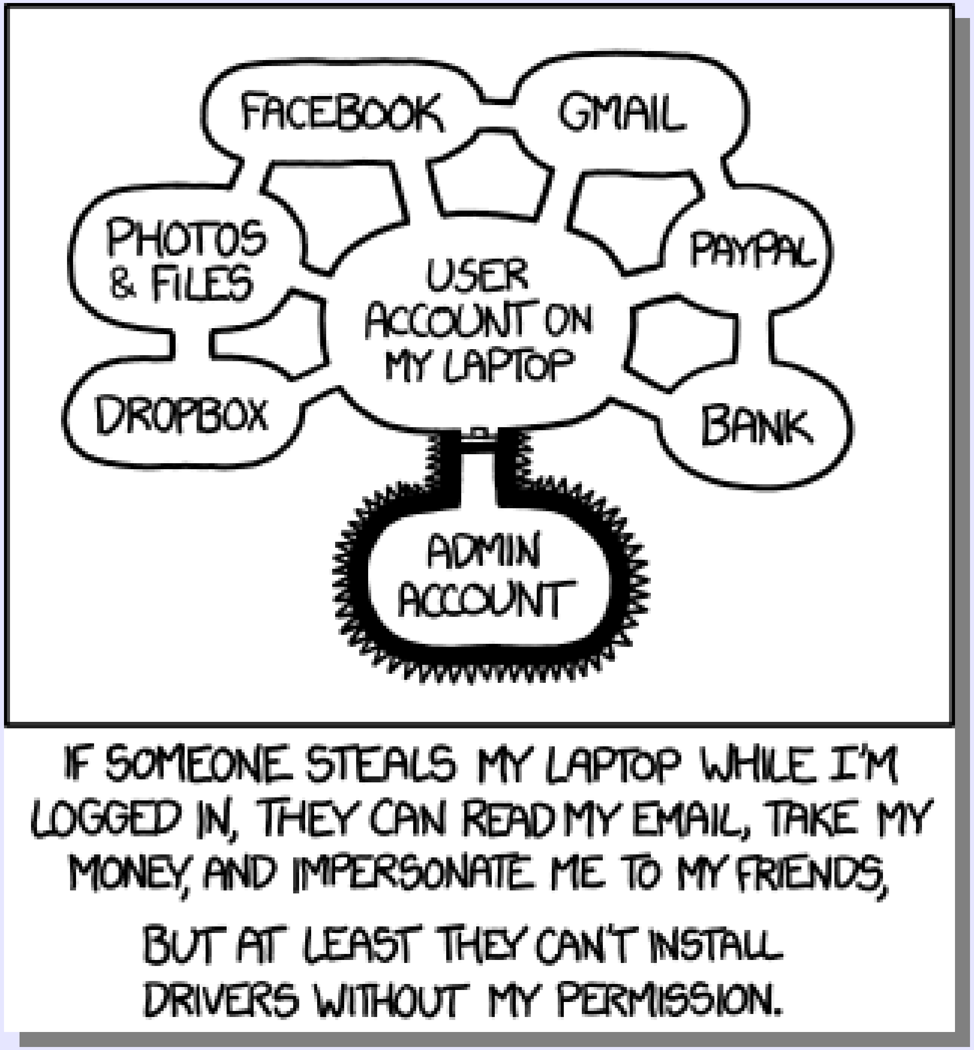
- 2004. After 6 years, the XP SP2 put an end to it

Driver Memory Error

Kagou-Anti-Kro$oft says not today !



2001. Microsoft - Admin rights

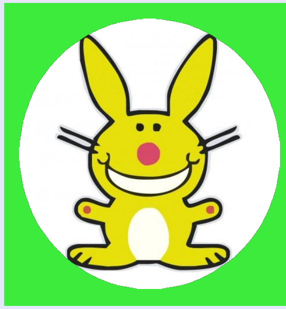

FACEBOOK
GMAIL
PHOTOS & FILES
PAYPAL
USER ACCOUNT ON MY LAPTOP
DROPBOX
BANK
ADMIN ACCOUNT
IF SOMEONE STEALS MY LAPTOP WHILE I'M LOGGED IN, THEY CAN READ MY EMAIL, TAKE MY MONEY, AND IMPERSONATE ME TO MY FRIENDS,
BUT AT LEAST THEY CAN'T INSTALL DRIVERS WITHOUT MY PERMISSION.

- 2001. XP admin rights by default

- Vista (2007) introduced UAC

- It was left open for 6 years

- DropMyRights utility



2001. Microsoft – hidden file extensions

- 2001. XP hide extensions for known file types by default

- 2014. Windows 8 also hides them

- It's a bad idea – ex. malwares

- LOVELETTER 2000: „Love-letter-for-you.TXT.VBS”

- Kournikova worm Februray 2001: „AnnaKournikova.jpg.vbs”

- Also recommended on OS X Macintosh

2007. Microsoft - Autorun

- June 2007.: The very first Autorun virus detection

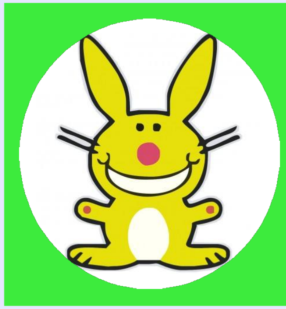
- Fixing autorun could have prevented it, if MS had cared as much as about WGA (Windows Genuine Advantage)

- February 2011. - MS finally issued the Autorun disabling fix

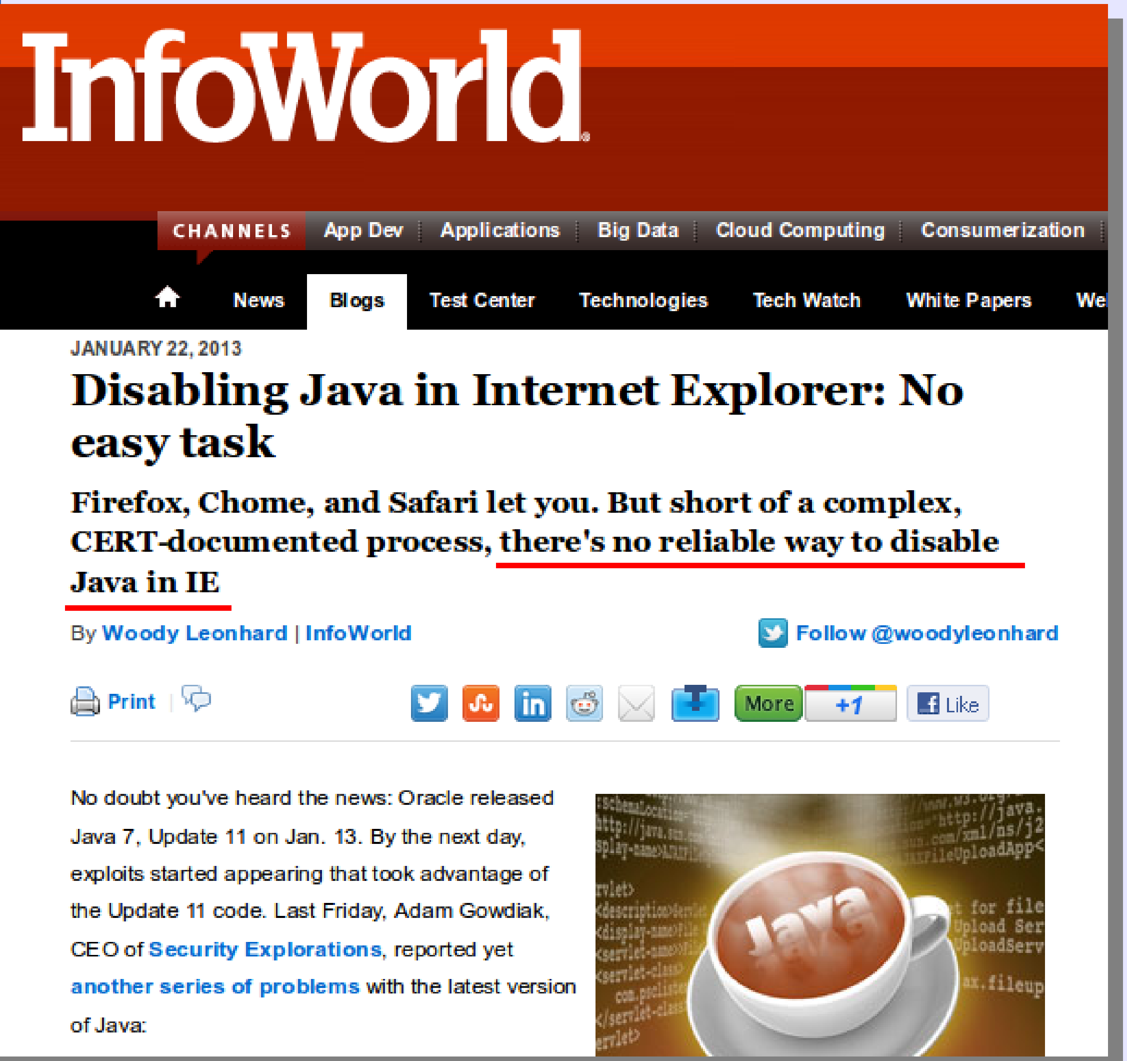
- It had been vulnerable for 5 years

- „It has been injured the user comfort...”

- Still, many users have not updated yet
  Ex. illegal Windows copies, laziness, etc.



2013. Microsoft - JAVA



JANUARY 22, 2013

Disabling Java in Internet Explorer: No easy task

Firefox, Chome, and Safari let you. But short of a complex, CERT-documented process, there's no reliable way to disable Java in IE

By Woody Leonhard | InfoWorld

Follow @woodyleonhard

No doubt you've heard the news: Oracle released Java 7, Update 11 on Jan. 13. By the next day, exploits started appearing that took advantage of the Update 11 code. Last Friday, Adam Gowdiak, CEO of Security Explorations, reported yet another series of problems with the latest version of Java:

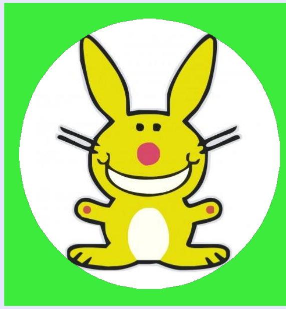
- 2013. Need to disable Java plugin on Windows due to critical exploits

- Disabling works perfectly in Firefox, Opera, Safari and Chrome

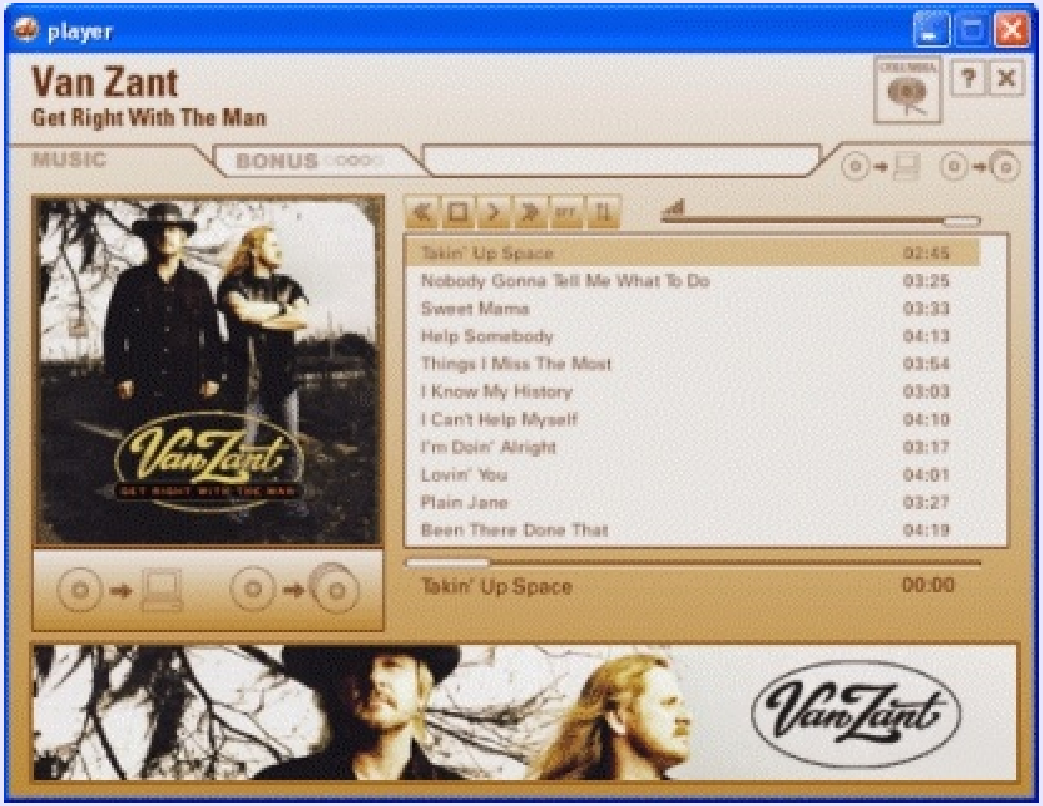
- In Internet Explorer, disabling Java didn't switch it off

- Need a special registry Workaround (CERT)

- JAVA is important for CIB bank, CITI bank, Adobe Creative Suite 5.5, a CrashPlan PRO online secure backup, LibreOffice, etc.



November 2005 - SONY rootkit



Takin' Up Space	02:45
Nobody Gonna Tell Me What To Do	03:25
Sweet Mama	03:33
Help Somebody	04:13
Things I Miss The Most	03:54
I Know My History	03:03
I Can't Help Myself	04:10
I'm Doin' Alright	03:17
Lovin' You	04:01
Plain Jane	03:27
Been There Done That	04:19

Takin' Up Space 00:00

- Rootkit copy protection (XCP) on the Van Zant music CD disc

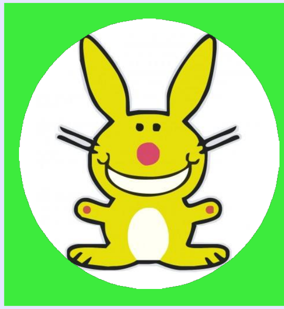
- It generated unknown network Traffic to Sony servers

- It reported, who, when and from which IP address played the album

- Later different malwares could hide in the rootkit's hidden folder

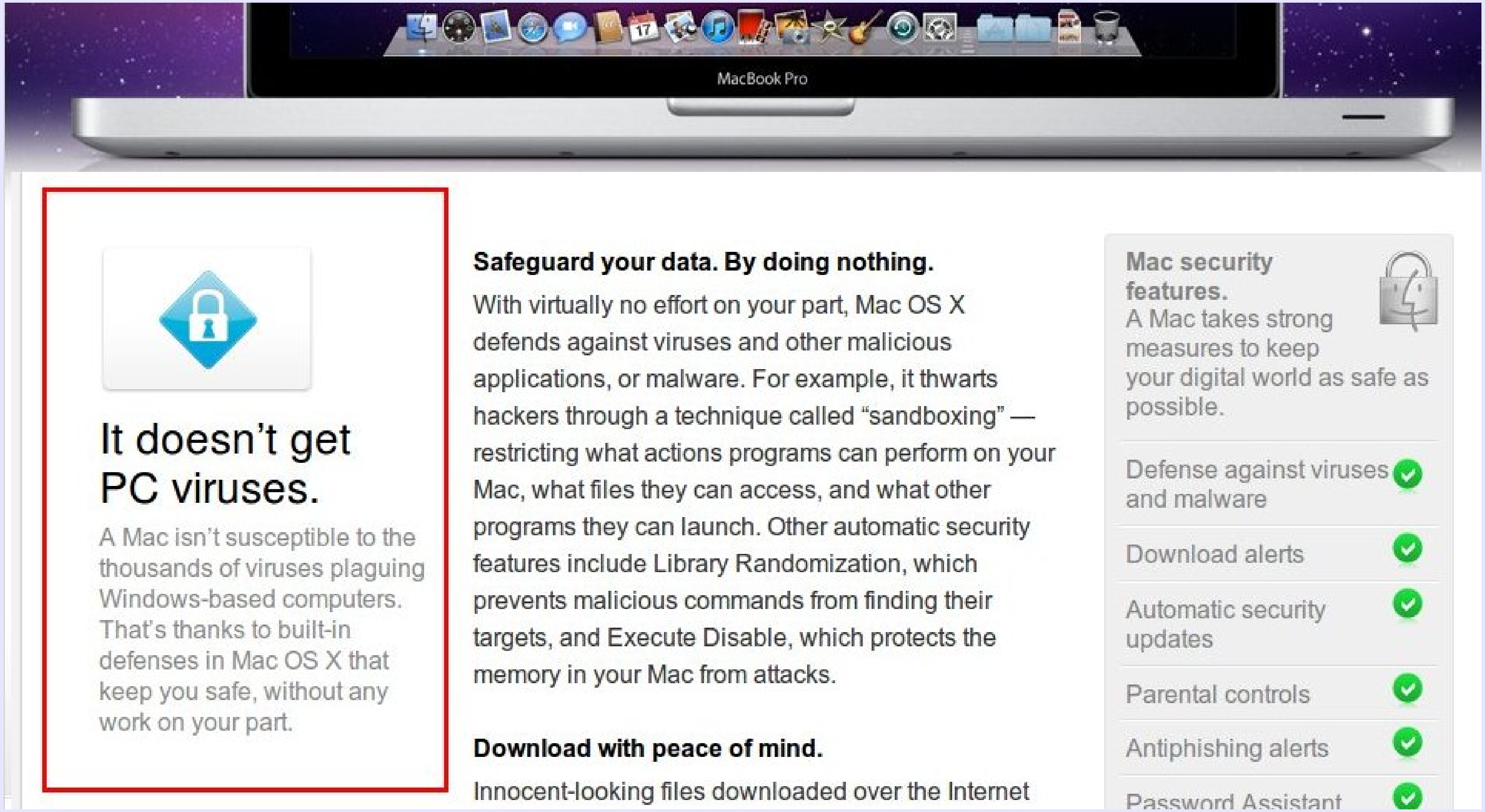
- Accidentally revealed (Mark Russinovich, Winternals)

- First denied, but finally withdrawn



OS X is Inherently a Safer Operating System

Why you'll love a Mac: www.apple.com
2011 - "It doesn't get PC viruses" (Wayback Machine)



It doesn't get PC viruses.

A Mac isn't susceptible to the thousands of viruses plaguing Windows-based computers. That's thanks to built-in defenses in Mac OS X that keep you safe, without any work on your part.

Safeguard your data. By doing nothing.

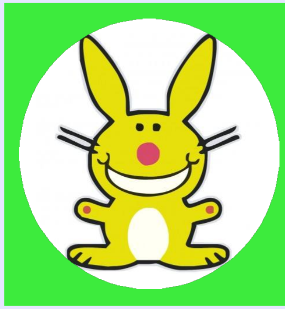
With virtually no effort on your part, Mac OS X defends against viruses and other malicious applications, or malware. For example, it thwarts hackers through a technique called "sandboxing" — restricting what actions programs can perform on your Mac, what files they can access, and what other programs they can launch. Other automatic security features include Library Randomization, which prevents malicious commands from finding their targets, and Execute Disable, which protects the memory in your Mac from attacks.

Download with peace of mind.

Innocent-looking files downloaded over the Internet

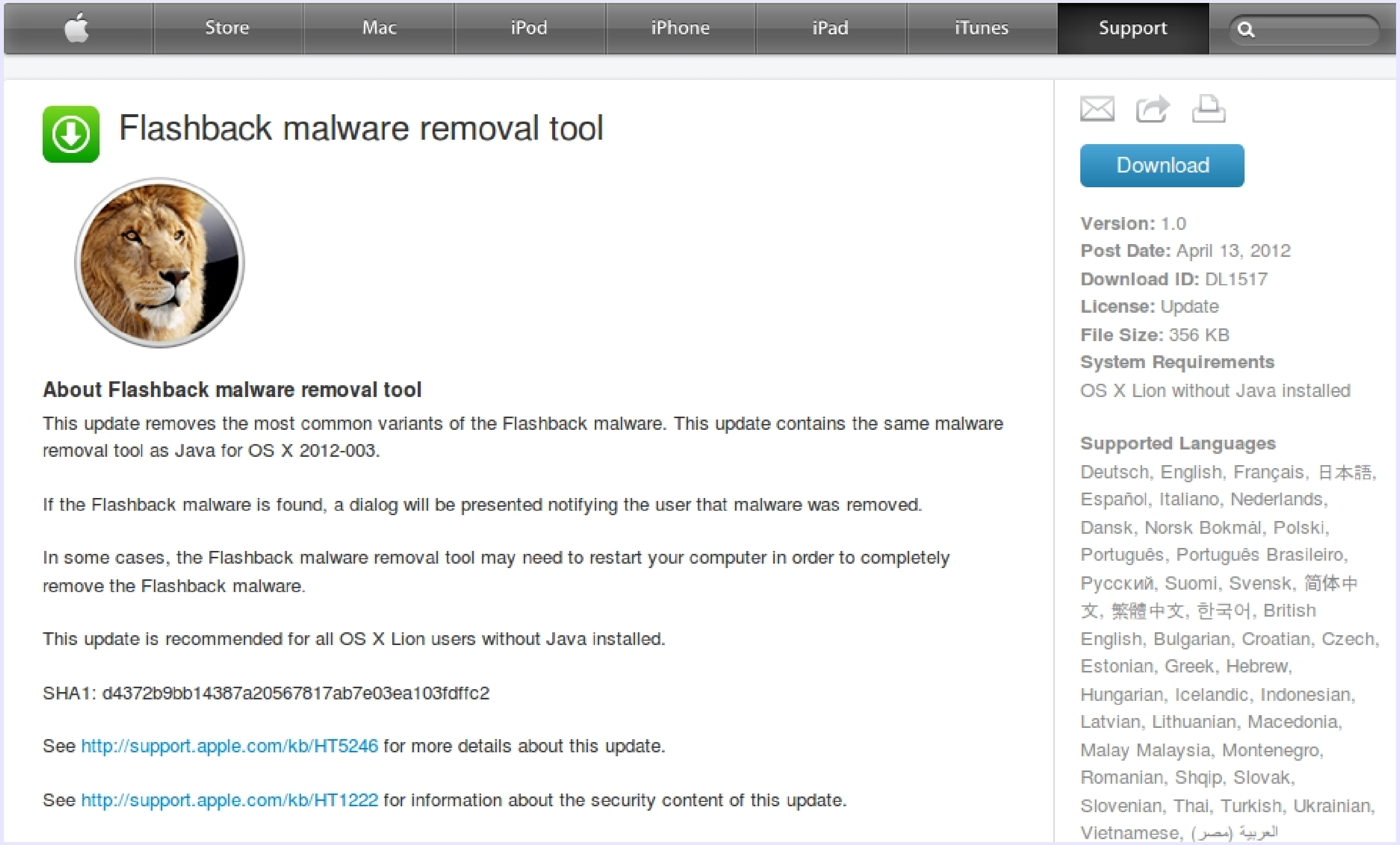
Mac security features.
A Mac takes strong measures to keep your digital world as safe as possible.

Defense against viruses and malware	✓
Download alerts	✓
Automatic security updates	✓
Parental controls	✓
Antiphishing alerts	✓
Password Assistant	✓



OS X is Inherently a Safer Operating System

March 2012 - Flashback botnet on OS X 600,000 infected zombie Macintosh (Java)
13.04.2012 - Flashback malware removal tool - Apple security update
26.09.2014 – Mac.BackDoor.iWorm 17,000 botnet, Reddit C&C



Flashback malware removal tool

About Flashback malware removal tool

This update removes the most common variants of the Flashback malware. This update contains the same malware removal tool as Java for OS X 2012-003.

If the Flashback malware is found, a dialog will be presented notifying the user that malware was removed.

In some cases, the Flashback malware removal tool may need to restart your computer in order to completely remove the Flashback malware.

This update is recommended for all OS X Lion users without Java installed.

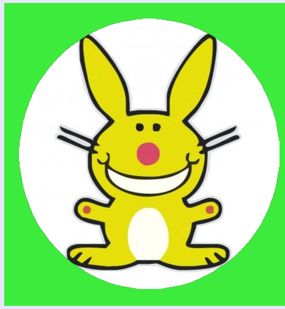
SHA1: d4372b9bb14387a20567817ab7e03ea103fdffc2

See http://support.apple.com/kb/HT5246 for more details about this update.

See http://support.apple.com/kb/HT1222 for information about the security content of this update.

Version: 1.0
Post Date: April 13, 2012
Download ID: DL1517
License: Update
File Size: 356 KB
System Requirements
OS X Lion without Java installed

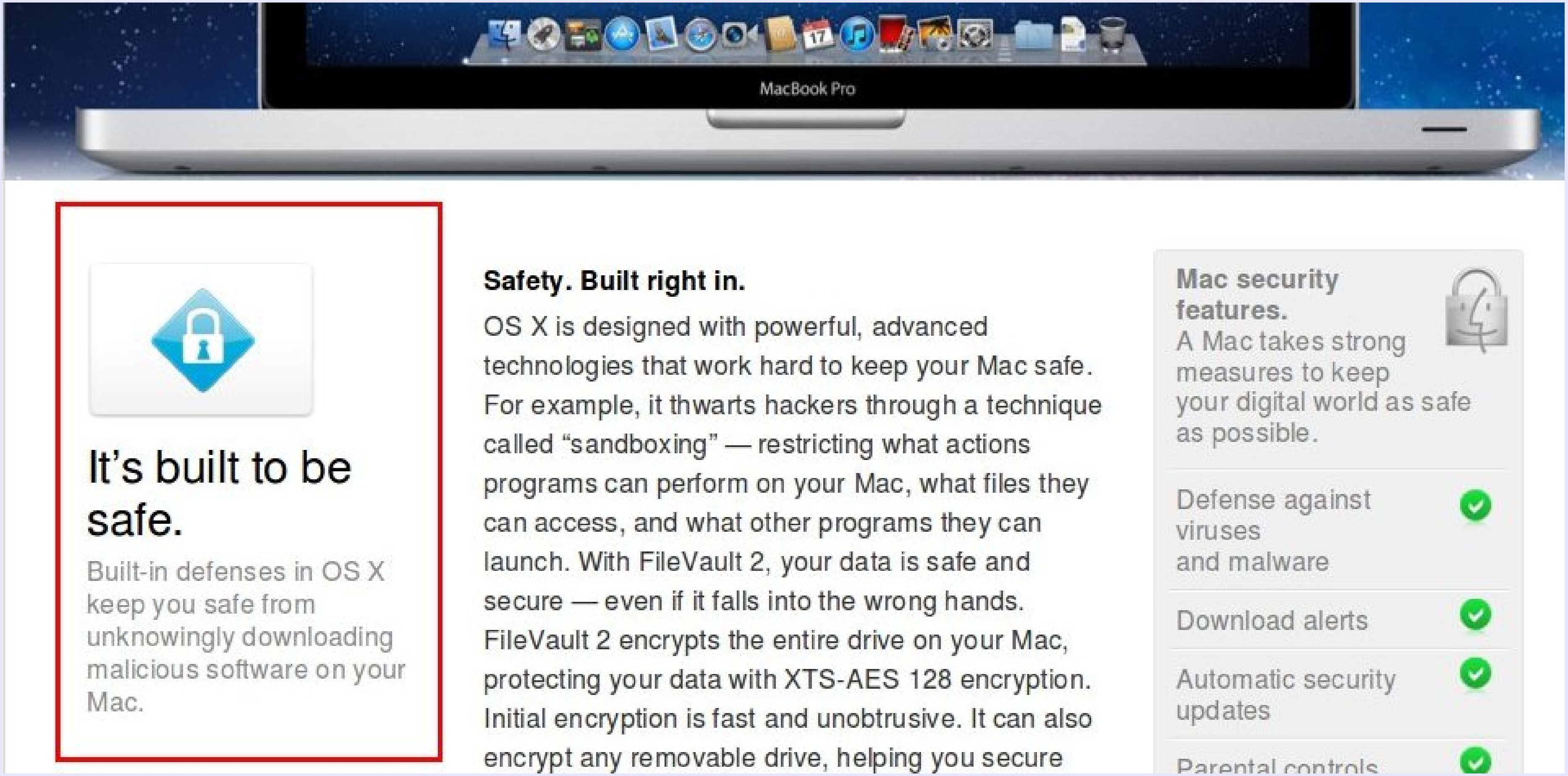
Supported Languages
Deutsch, English, Français, 日本語, Español, Italiano, Nederlands, Dansk, Norsk Bokmål, Polski, Português, Português Brasileiro, Русский, Suomi, Svensk, 简体中文, 繁體中文, 한국어, British English, Bulgarian, Croatian, Czech, Estonian, Greek, Hebrew, Hungarian, Icelandic, Indonesian, Latvian, Lithuanian, Macedonia, Malay Malaysia, Montenegro, Romanian, Shqip, Slovak, Slovenian, Thai, Turkish, Ukrainian, Vietnamese, العربية (مصر)



IV. OS and Application developers

OS X is Inherently a Safer Operating System

Why you'll love a Mac: www.apple.com
2012 - "It's built to be safe"



It's built to be safe.

Built-in defenses in OS X keep you safe from unknowingly downloading malicious software on your Mac.

Safety. Built right in.

OS X is designed with powerful, advanced technologies that work hard to keep your Mac safe. For example, it thwarts hackers through a technique called "sandboxing" — restricting what actions programs can perform on your Mac, what files they can access, and what other programs they can launch. With FileVault 2, your data is safe and secure — even if it falls into the wrong hands. FileVault 2 encrypts the entire drive on your Mac, protecting your data with XTS-AES 128 encryption. Initial encryption is fast and unobtrusive. It can also encrypt any removable drive, helping you secure

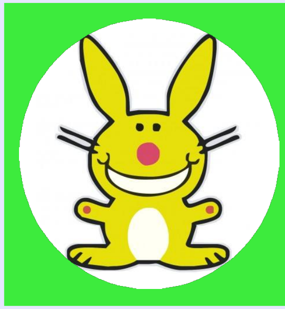
Mac security features.
A Mac takes strong measures to keep your digital world as safe as possible.

- Defense against viruses and malware ✓
- Download alerts ✓
- Automatic security updates ✓
- Parental controls ✓

OS X is Inherently a Safer Operating System

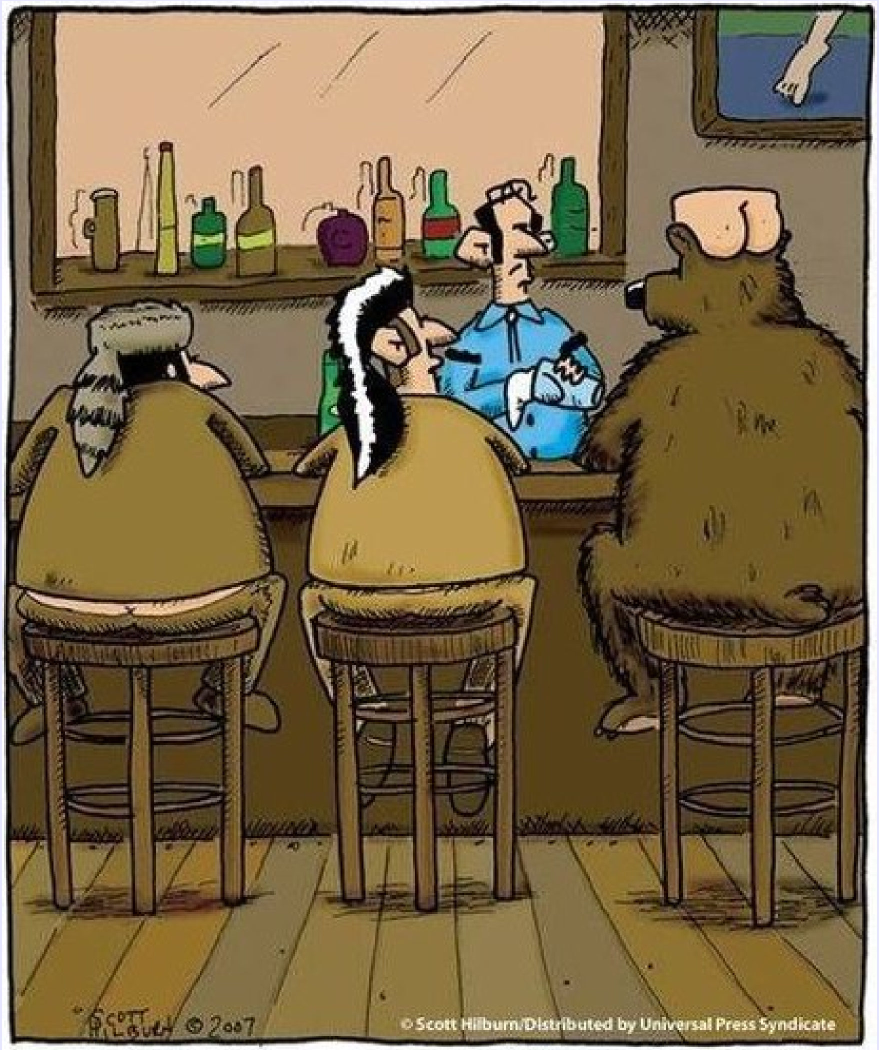
June 2012 - OS X Mountain Lion 10.8
- Automatic daily security updates
- Gatekeeper execution prevention technology

May 2013
- OSX/KitM.A trojan
- social engineering: please install me :-)
- valid Apple Developer ID associated with the name Rajender Kumar
- bypasses Apple's Gatekeeper
- If it passes Gatekeeper on first run, it will continue to run and never be queried again by Gatekeeper



IV. OS and Application developers

2008. Adobe Reader JavaScript

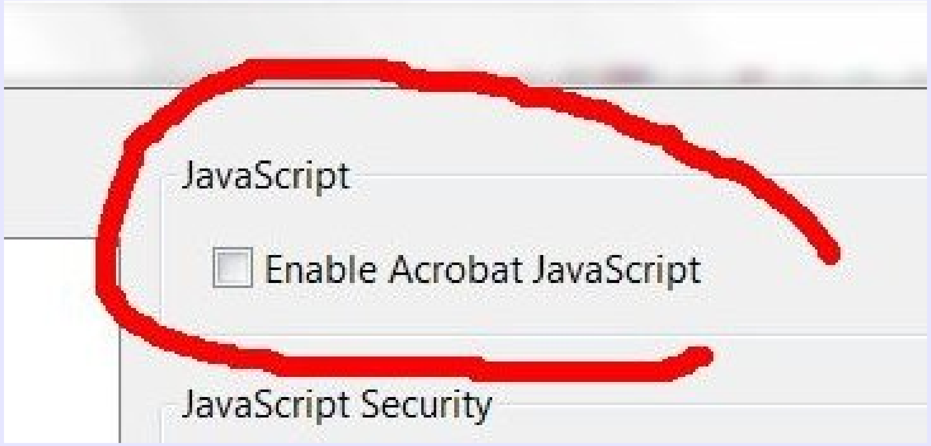


- 2008. The very first appearance of a Malicious JavaScript in a PDF file

- Allegedly the JS is necessary and useful in PDF interactive forms

- 2014. The JS is still on by default

- This has also been for 6 years



JavaScript

□ Enable Acrobat JavaScript

JavaScript Security

Conclusion

We may find eventually a new Award, something like Darwin Award.
„Who messed up the most?”

- the OS developers could patch the known vulnerabilities much quicker ex. OpenSSL, ShellShock, etc.
- the users could understand that the security awareness and the patch management are just as important as using AV
- the AV industry could make more effort to improve proactive capabilities

but the Bad Guys don't need to fix their dysfunctional ideas and defective codes ;-)

Please Be safe.

Do not stand, sit, climb or lean on zoo fences.
If you fall, animals could eat you and that might make them sick.
Thank you.

Thank you for your attention!

csizmazia.istvan@webwell.hu

Security awareness rulez :-)