Classic Viruses

Computer viruses can be classified according to their environment and infection methods. The environment is the application or operating system required by any given virus to infect files within these systems. Infection methods are the techniques used to inject the virus code into an object.

Environment

Most viruses can be found in one of the following environments:

- File systems
- Boot sectors
- Macro environments
- Script hosts

File viruses use the file system of a given operating system (or more than one) to propagate. File viruses can be divided into the following categories:

- Those that infect executable files (the largest group of file viruses)
- Those that create duplicates of files (companion viruses)
- Those that create copies of themselves in various directories
- Those that utilize file systems features (link viruses)

Boot sector viruses write themselves either to the boot sector or to the master boot record or displace the active boot-sector. These viruses were widespread in the 1990s, but have almost disappeared since the introduction of 32-bit processors as standard and the decline of the floppy disks. It would be technically possible to write boot sector viruses for CDs and USB flash ROMs, but no such viruses have yet been detected.

Many word processing, accounting, editing and project applications have built-in macro scripts which automate frequently used sequences. These macro languages are often complex and include a wide range of commands. Macro viruses are written in macro languages and infect applications with built-in macros. Macro viruses propagate by exploiting macro language properties in order to transfer from an infected file to another file.

Infection Methods

The groups of viruses listed above can be sub-divided according to the technique a virus uses to infect objects.

File Viruses

File viruses use the following infection methods:

- Overwriting
- Parasitic
- Companion
- Links
- Object modules (OBJ)
- Compiling libraries (LIB)
- Application source code

Overwriting

This is the simplest infection method: the virus replaces the code of the infected file with its own, erasing the original code. The file is rendered useless and cannot be restored. These viruses are easily detected because the operating system and affected applications will cease to function shortly after infection.

Parasitic

Parasitic viruses modify the code of the infected file. The infected file remains partially or fully functional.

Parasitic viruses are grouped according to the section of the file they write their code to:

- Prepending: the malicious code is written to the beginning of the file
- Appending: the malicious code is written to the end of the file

- Inserting: the malicious code is inserted in the middle of the file

Inserting file viruses use a variety of methods to write code to the middle of a file: they either move parts of the original file to the end or copy their own code to empty sections of the target file. These are sometimes called cavity viruses.

Prepending viruses

Prepending viruses write their code to target files in two ways. In the first scenario, the virus moves the code from the beginning of the target file to the end and writes its own code to this space. In the second scenario the virus adds the code of the target file to its own code.

In both cases, every time the infected file is launched, the virus code is executed first. In order to maintain application integrity, the virus may clean the infected file, re-launch it, wait for the file to execute, and once this process is over, the virus will copy itself again to the beginning of the file. Some viruses use temp files to store clean versions of infected files. Some viruses will restore the application code in memory, and reset necessary addresses in the body, thus duplicating the work of the operating system.

Appending viruses

Most viruses fall into this category. Appending viruses write themselves to the end of the infected files. However, these viruses usually modify the files (change the entry point in the file header) to ensure that the commands contained in the virus code are executed before infected object commands.

Inserting viruses

Virus writers use a variety of methods to inject viruses into the middle of a file. The simplest methods are moving part of the file code to the end of the file or pushing the original code aside to create a space for the virus.

Inserting viruses include so-called cavity viruses; these write their code to sections of files that are known to be empty.. For instance, cavity viruses can copy themselves to the unused part of exe file headers, to the gaps between exe file sections, or to text areas of popular compilers. Some cavity viruses will only infect files where a certain block contains a certain byte; the chosen block will be overwritten with the virus code.

Finally, some inserting viruses are badly written and simply overwrite sections of code which are essential for the infected file to function. This causes the file to be irrevocably corrupted.

Entry point obscuring viruses - EPOs

There is a small group of parasitic viruses which includes both appending and inserting viruses which do not modify the entry point address in the headers of exe files. EPO viruses write the routine pointing to the virus body to the middle of the infected file. The virus code is then executed only if the routine containing the virus executable is called. If this routine is rarely used, (i.e. a rare error notification) an EPO virus can remain dormant for a long time.

Virus writers need to choose the entry point carefully: a badly chosen entry point can either corrupt the host file or cause the virus to remain dormant long enough for the infected file to be deleted.

Virus writers use different methods to find useful entry points:

- Searching for frames and overwriting them with infected starting points
- Disassembling the host file code
- Or changing the addresses of importing functions

Companion viruses

Companion viruses do not modify the host file. Instead they create a duplicate file containing the virus. When the infected file is launched the copy containing the virus will be executed first.

This category includes viruses that re-name the host file, record the new name for future reference and then overwrite the original file. For instance, a virus might rename notepad.exe as notepad.exd and write its own code to the file under the original name. Each time the user of the victim machine launches notepad.exe, the virus code will be executed, with the original Notepad file, notepad.exd, being run afterwards.

There are other types of companion viruses which use original infection techniques or exploit vulnerabilities in specific operating systems. For instance, Path-companion viruses place their copies in the Windows system directory, exploiting the fact that this directory is first in the PATH list;

the system will start from this directory when launching Windows. Many contemporary worms and Trojans use such autorun techniques.

Other infection techniques

Some viruses do not use executable files to infect a computer, but simply copy themselves to a range of folders in the hope that sooner or later they will be launched by the user. Some virus writers give their viruses such as install.exe or winstart.bat in order to persuade the user to launch the file containing the virus.

Other viruses copy themselves to compressed files in formats such as ARJ, ZIP and RAR, while still others write the command to launch an infected file to a BAT-file.

Link viruses also do not modify host files. However, they force the operating system to execute the virus code by modifying the appropriate fields in the file system.

Boot Sector Viruses

The boot viruses which are currently known about infect the boot sectors of floppy disks and the boot sector or Master Boot Record (MBR) of the hard disk. Boot viruses act on the basis of the algorithm used to launch the operating system when the computer is switched on or rebooted. Once the necessary checks of memory, disks etc. have been carried out, the system boot program reads/ fetches the first physical sector of the boot disk (A:, C: or the CD-ROM, depending on the parameters configured/ installed in BIOS Setup, and passes control to this sector.

When infecting disks, a boot virus will substitute its code for that of a program which gains control when the system launches. In order to infect the system, the virus will force the system to read the memory and hand over control not to the original boot program, but the virus code.

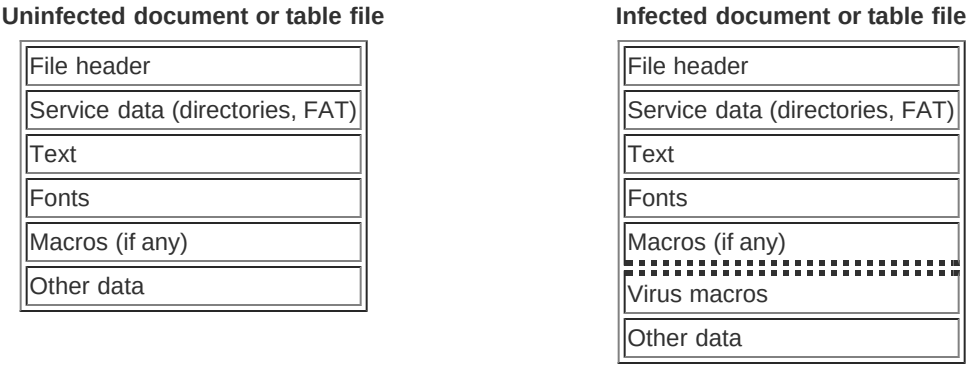
Floppy disks can only be infected in one way. The virus writes its code in the place of the original code of the boot sector of the disk. Hard disks can be infected in three ways: the virus either writes its code in place of the MBR code; the boot sector code of the boot disk, or modifies the address of the active books sector in the Disk Partition Table in the hard disk MBR.

In the vast majority of cases, when infecting a disk the virus will move the original boot sector (or MBR) to another sector of the disk, often the first empty one. If the virus is longer than the sector, then the infected sector will contain the first part of the virus code, and the remainder of the code will be placed in other sectors, usually the first free ones.

Macro Viruses

The most widespread macro viruses are for Microsoft Office applications (Word, Excel and PowerPoint) which save information on OLE2 (Object Linking and Embedding) format. Viruses for other applications are relatively rare.

The actual location of a virus with an MS Office file depends on the file format, which in the case of Microsoft products is extremely complex. Every WORD document, Office 97 or Excel table is composed of a sequence of data blocks (each of which has its own format) which are joined/ linked/ united by service data. Due to the complex format of Word, Excel and Office 97 files, it is easiest to use a diagram to show the location of a macro virus in such a file:



When working with documents and tables, MS Office carries out a number of different actions: the application opens the document, saves it, prints it, closes it etc. MS Word will search for and execute/ launch the appropriate built-in macros. For example, using the File/Save command will call the FileSave macro, the File/SaveAs command will call the FileSaveAs macro, and so on, always assuming that such macros are defined/ configured.

There are also auto macros, which will be automatically called in a range of situations. For instance, when a document is opened, MS Word will check the document for the presence for the AutoOpen macro. If the macro is found, Word will execute it. When a document is closed, Word will execute the AutoClose macro, when Word is launched, the application will execute the AutoExec macro etc. These macros are executed

automatically, without any action from the user, as are macros/ functions which are associated either with a particular key, or with a specific time or date.

As a rule, macro viruses which infect MS Office files will use one of the techniques described above. The virus will either contain an auto macro (automatic function) or one of the standard system macros (associated with a menu item) will be redefined, or the virus macro will be automatically called by a certain key stroke or key combination. Once the macro virus has gained control, it will transfer its code to other files, usually ones which are currently being edited. More rarely, the viruses will search disks for other files.

Script Viruses

Script viruses are a subset of file viruses, written in a variety of script languages (VBS, JavaScript, BAT, PHP etc.). They either infect other scripts e.g. Windows or Linux command and service files, or form a part of multi-component viruses. Script viruses are able to infect other file formats, such as HTML, if the file format allows the execution of scripts.

EICAR-Test-File

Aliases

EICAR-Test-File (Kaspersky Lab) is also known as: EICAR-AV-Test (Sophos), EICAR_Test_File (RAV), Eicar_test_file (Trend Micro), Eicar-Test-Signature (H+BEDV), EICAR_Test_File (FRISK), EICAR_Test (+356) (Grisoft), Eicar-Test-Signature (ClamAV), Eicar.Mod (Panda)

Description added Jul 07 2003

Behavior Virus

Technical details

EICAR is a short 68-byte COM file that is detected by anti-virus programs as a virus, but is actually **NOT "VIRAL"** at all. When executed it just displays a message and returns control to the host program.

Why is this harmless file detected as a virus? The file was created in order to demonstrate to users the messages and procedures that anti-virus programs display when a real virus is detected.

Some time ago researchers from several anti-virus companies were asked by users to develop a way to demonstrate what would happen in case of a real virus attack; a sort of simulation of which messages anti-virus programs will display and what actions will be recommended to perform, e.t.c.

After some time and thought toward how to best satisfy the request, the anti-virus researchers decided to release some virus-simulators that would be some harmless file that does nothing but display a message(s) and then exits to DOS (host OS). It was decided that this file could contain only ASCII characters so that users could type it or copy it from a User Guide. As a result the COM file looks as follows:

```
X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*
```

Despite having only ASCII characters, this COM file is nonetheless a legitime computer program that does work under DOS or in a DOS window under Windows, OS/2 or any other OS that is able to run DOS programs. When run or executed this COM-file simply displays a text message and exits to DOS. The displayed message looks as follows:

```
EICAR-STANDARD-ANTIVIRUS-TEST-FILE!
```

It is as simple as that, though a lot of anti-virus programs detect it as a virus named **EICAR-Test-File** or something close to this.

Virus.Boot.ABCD.a

Aliases

Virus.Boot.ABCD.a (Kaspersky Lab) is also known as: ABCD.a (Kaspersky Lab), BtDr.Tanko (McAfee), Tanko Dropper (Symantec), ABCD.dropper (Doctor Web), ABCD (Sophos), ABCD (RAV), Replicator* (Trend Micro), Tanko (Boot) (H+BEDV), BOOT SECTOR DROPPER (FRISK), ABCD (ALWIL), ABCD (Grisoft), Tanko (SOFTWIN), Tanko (ClamAV), Replicator (Panda)

Description added	Mar 07 2000
Behavior	Virus

Technical details

It's a harmless boot virus. On loading from infected disk, it hooks INT 13h and writes itself into boot sectors of floppy disks. It infects the hard drive on loading from infected floppy. It uses the ID-word ABCDh.

Virus.Boot.Amjads

Aliases

Virus.Boot.Amjads (Kaspersky Lab) is also known as: Amjads (Kaspersky Lab), Amjads (McAfee), Amjads (RAV), Amjads (FRISK)

Description added	Mar 07 2000
Behavior	Virus

Technical details

It is a very dangerous memory resident polymorphic and stealth boot virus. It infects the MBR of the hard drive and boot sector on floppy disks. While loading from infected disk it hooks INT 1Ch, waits for some time and then hooks INT 13h and completes installation into the system memory. While loading from infected floppy disk it also infects the MBR of the hard drive. Floppy disks get infected when they are accessed.

On March 6th the virus erases data on the hard drive and displays the message:

```
You PC is now Stoned!
This virus was written in the city of Taipei.
Amjads 1997.
```

Virus.Boot.Azusa.a

Aliases

Virus.Boot.Azusa.a (Kaspersky Lab) is also known as: Azusa.a (Kaspersky Lab), BtDr.Azusa (McAfee), Azusa (Symantec), Drop Azusa (Sophos), Azusa.A (RAV), Tree (H+BEDV), BOOT SECTOR DROPPER (FRISK), Azusa-A (ALWIL), Stoned (Grisoft), Dropper.Boot.Azusa.A (SOFTWIN), Tree (ClamAV), Azusa Boot (Panda)

Description added	Mar 07 2000
Behavior	Virus

Technical details

These are dangerous viruses which hit boot sectors of floppy disks and the MBR of hard disks. They save boot sector into the last sector of the floppy disk, but don't save the original MBR (contain the loader inside the own body). The viruses periodically hangs up COM and LPT ports. The viruses hook INT 13h.

Virus.Boot.Beryllium

Aliases

Virus.Boot.Beryllium (Kaspersky Lab) is also known as: Beryllium (Kaspersky Lab), BtDr.Beryllium (McAfee), Virus.Dropper (Symantec), Beryllium.dropper (Doctor Web), Beryllium (Sophos), Beryllium (RAV), BERYLLIUM.A (Trend Micro), BOO/BERYLLIU (H+BEDV), BOOT SECTOR DROPPER (FRISK), Beryllium (ALWIL), Beryllium (Grisoft), Beryllium (SOFTWIN), BOO.BERYLLIU (ClamAV), Beryllium.Boot (Panda)

Description added	Mar 07 2000
Behavior	Virus

Technical details

It's a harmless memory resident stealth boot virus. On loading from infected floppy it hits MBR of hard drive. On loading from infected sector it hooks INT 13h and writes itself into boot sectors of floppy disks on reading from them. It contains the internal text: "BERYLLIUM!".

Virus.Boot.Cannabis.a

Aliases

Virus.Boot.Cannabis.a (Kaspersky Lab) is also known as: Cannabis.a (Kaspersky Lab), BtDr.b (McAfee), Cannabis Dropper (1) (Symantec), Cannabis.dropper (Doctor Web), Cannabis (Sophos), Cannabis.A (RAV), CANNAB1-1 (Trend Micro), Drop-Boot-2 (H+BEDV), BOOT SECTOR DROPPER (FRISK), Cannabis (ALWIL), Cannabis (Grisoft), Cannabis.A.dropper (SOFTWIN), Cannabis (ClamAV), Cannabis.B.Drp (Panda)

Description added	Mar 07 2000
Behavior	Virus

Technical details

It's a not dangerous memory resident floppy boot-sectors infector. It hooks INT 13h. It contains the word "Cannabis". It also types:

```
Hey man, I don't wanna work. I'm too stoned right now...
Non-System disk or disk error
Replace and press a key when ready
```

Virus.Boot.Catman

Aliases

Virus.Boot.Catman (Kaspersky Lab) is also known as: Catman (Kaspersky Lab), Glug (McAfee), Catman (Doctor Web), Catman (Sophos), Catman (RAV), CATMAN-B* (Trend Micro), Catman (Boot) (H+BEDV), Catman (ALWIL), Catman (Grisoft), Catman (SOFTWIN), Gen.428 (ClamAV)

Description added	Mar 07 2000
Behavior	Virus

Technical details

It's a memory resident dangerous virus which hooks INT 9, 13h and infects the floppy Boot-sectors by a virus "Brain" algorithm. It moves the TSR part into the memory at a random address and does not change the system areas. It can cause the computer to hang-up. This virus checks the keyboard and beeps when the Alt-Ctrl-Enter pressed. It also erases the FAT and DIR sectors of the drives.

Virus.Boot.Cicada

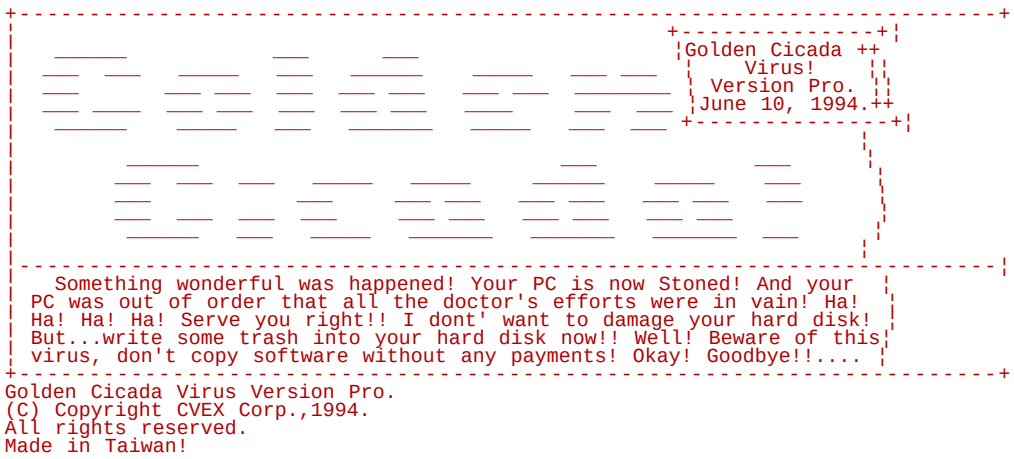
Aliases

Virus.Boot.Cicada (Kaspersky Lab) is also known as: Cicada (Kaspersky Lab), BtDr.Cicada (McAfee), Cicada Dropper (Symantec), Cicada.dropper (Doctor Web), Cicada (Sophos), Cicada (RAV), GVC3-B* (Trend Micro), VGEN/15694.0 (H+BEDV), BOOT SECTOR DROPPER (FRISK), Cicada (ALWIL), Cicada (Grisoft), Cicada (ClamAV), Cicada.Drp (Panda)

Description added	Mar 07 2000
Behavior	Virus

Technical details

It is a dangerous memory resident boot virus. It hooks INT 13h and writes itself into the MBR of hard drive and boot sectors of floppy disks. On July, 10th it erases the hard drive sectors and displays:



[Note: some characters not displayable in HTML]

Virus.Boot.DenZuk.a

Aliases

Virus.Boot.DenZuk.a (Kaspersky Lab) is also known as: DenZuk.a (Kaspersky Lab), BtDr.Denzuk (McAfee), Den Zuko Dropper (Symantec), DenZuk.dropper (Doctor Web), Den Zuk Trojan (Sophos), DenZuk.A.dr (RAV), DENZUK.A (Trend Micro), Boot-Dropper (H+BEDV), BOOT SECTOR DROPPER (FRISK), Den (ALWIL), DenZuk.D.Dropper (SOFTWIN), Boot-Dropper (ClamAV)

Description added	Mar 07 2000
Behavior	Virus

Technical details

These are dangerous viruses, 9 sectors long. They infect floppy disks Boot-sectors during access (INT 13h, ah=2,3,4,5). The viruses make no check when place their second parts on a disk, so they can destroy some information at the 40th track.

The viruses hook INT 9, 13h. On a warm reboot they display their name "Den Zuk" in big letters (graphics video mode). The viruses replace the label of the infected disk with "Y_C_1_E_R_P". They don't have a destructive function, but they are dangerous because of the possibility to erase information at the 40th track of the infected disk. The viruses contain the text: "Welcome to the C l u b --The HackerS-- Hackin' All The Time", "The HackerS".

Virus.Boot.DiskFiller

Aliases

Virus.Boot.DiskFiller (Kaspersky Lab) is also known as: DiskFiller (Kaspersky Lab), Filler (McAfee), Filler (Doctor Web), Disk Filler (Sophos), Filler (RAV), Filler.A* (Trend Micro), Filler (H+BEDV), Filler.A (FRISK), Filler (ALWIL), Filler (Grisoft), Filler.A (SOFTWIN), Filler (ClamAV), Filler Boot (Panda)

Description added	Mar 07 2000
Behavior	Virus

Technical details

This is a very dangerous stealth virus that hits Boot-sectors of floppy disks and the MBR of hard disks during access. This virus formats an additional track on the floppy disk (the 40th on 360K size and 80th on 1.2M) and then puts its code there. After that, the virus mounts its head part into the boot sector of the floppy, its original contents is practically unchanged. On a hard disk infection, the virus places its body just after the MBR. Inside the MBR, it changes the active boot sector address only and sets this address to the sector containing the beginning of the virus code.

When COMMAND.COM is started, the virus moves itself into the low address memory area. According to the system time it encrypts and displays the message: Haha,vírus van a gépben!! Ez egy eddig még nem közismert vírus. De hamarosan az lesz. A neve egyszerüen töltögetö Ezt a nevét onnan kapta, hogy feltöltögeti a FAT-táblát kölönbözö alakzatokkal. Ez már meg is történt !!!

and then "draws" in the FAT sectors the following picture:

The virus also contains the string "command.com", hooks INT 13h,1Ch,21h.

Virus.Boot.Dodgy.a

Aliases

Virus.Boot.Dodgy.a (Kaspersky Lab) is also known as: Dodgy.a (Kaspersky Lab), Dodgy (McAfee), Ravage (b) (Symantec), Dodgy (Doctor Web), Dodgy (Sophos), Dodgy.A (RAV), DOGGY* (Trend Micro), Dodgy (H+BEDV), Dodgy.B (FRISK), Rp&Murphy (ALWIL), Dodgy (Grisoft), Dodgy.A (SOFTWIN), DODGY-B (ClamAV), Dodgy (Panda)

Description added	Mar 07 2000
Behavior	Virus

Technical details

This is a very dangerous memory resident stealth boot virus. It occupies two sectors, so the virus length is 1024 (400h) bytes. It infects the MBR of the hard drive and boot sector of floppy disks. While infecting the hard drive the virus saves the original MBR sector and the rest of its code to the sectors on the first track/zero head starting from sector 14. Usually that space is not occupied by any programs/data. While infecting floppy disks the virus saves original boot sector and its code to the last sectors of root directory.

While loading from infected disk the virus decreases the size of system memory by using the word at address 0:0413h, copies itself to there, hooks INT 8, 13h, 40h and calls bootstrap loader (reboots the system). Being already installed, the virus runs its stealth engine. As a result bootstrap loader will read original boot/MBR sector instead of infected one, and virus code will not receive control and the virus will not install itself twice to the system memory. While installing the virus also accessed the MBR of the hard drive - the virus INT 13h handler intercepts that call and infects the MBR, if it is not infected yet.

While infecting the MBR the virus uses several tricks to avoid detection by BIOS anti-virus protection - the virus modifies necessary fields in the CMOS and stuffs the 'Y' key to keyboard buffer before writing to the MBR.

The virus uses INT 13h, 40h hooks to run its infection and stealth routines while reading/writing to/from floppy disks and the hard drive. By hooking INT 8 (timer) the virus intercepts DOS loading process - the virus looks for low memory area and scans it for "PEC=" text, that is the rest of "COMSPEC=" string placed in DOS programs environment blocks. If this string is found, the virus hooks DOS interrupts INT 21h, 2Fh, increases (i.e. restores) the size of system memory (the word at the address 0:0413h) and disables its INT 8 handler.

By hooking INT 21h the virus intercepts programs execution, checks their names. If a program with name RAV* is executed, the virus calls its trigger routine (see below). The virus does not calls this trigger routine under Windows, in this case the virus runs it when Windows is exiting (the virus intercepts it by INT 2Fh hook).

By hooking INT 2Fh the virus intercepts Windows installation, gets Windows' directory and deletes the SYSTEM\IOSUBSYS\HSFLOP.PDR in there. When Windows exits, the virus jumps to its trigger routine, if there was RAV* file executed during Windows seance.

In three months after infecting a disk the virus manifests itself by a trigger routine: it turns computer to graphic video mode, displays a message, disables the keyboard and erases sectors on the hard drive. The message is:

```
RAVage is wiping data!  RP&muRphy
```

Virus.Boot.EE.a

Aliases

Virus.Boot.EE.a (Kaspersky Lab) is also known as: EE.a (Kaspersky Lab), Jumper (McAfee), Jumper (Doctor Web), Viresc (Sophos), Jumper.B (RAV), JUMPER.B* (Trend Micro), Jumper (H+BEDV), Jumper.B (FRISK), Jumper (ALWIL), Jumper (Grisoft), EE.A (ClamAV), Jumper.B (Panda)

Description added Mar 07 2000

Behavior Virus

Technical details

It's a not dangerous memory resident virus. On loading from infected floppy it infects MBR of hard drive, then it hooks INT 1Ch, waits for DOS loading, then hooks INT 21h and infects floppies on DOS functions SELECT DISK and KEYBOARD INPUT calls (INT 21h, ah=0Eh,0Ah). Depending on current time it displays the 'î' character (ASCII EEh).

Virus.Boot.Ekaterinburg

Aliases

Virus.Boot.Ekaterinburg (Kaspersky Lab) is also known as: Ekaterinburg (Kaspersky Lab), Antiexe (McAfee), Ekaterinburg (Doctor Web), Junk/Ekaterin (Sophos), RussianFlag (RAV), RUSSIAN_FLAG.A* (Trend Micro), Russian Flag (Boot) (H+BEDV), Russian (ALWIL), Russian_Flag (Grisoft)

Description added	Mar 07 2000
Behavior	Virus

Technical details

It's a not dangerous memory resident boot virus. On loading from infected disk it copies itself into Interrupt Vectors Table and hooks INT 13h. Then it writes itself into boot sectors of floppy disks. MBR of hard drive is infected on loading from infected floppy. Depending on the system timer value the virus erases the screen and waits for keystroke. It contains encrypted text string "Ekaterinburg".

Virus.Boot.Flame

Aliases

Virus.Boot.Flame (Kaspersky Lab) is also known as: Flame (Kaspersky Lab), Flame (McAfee), Flame (Doctor Web), Flame (Sophos), Flame (RAV), FLAME* (Trend Micro), Fire (Boot) (H+BEDV), Flame.A (FRISK), Flame (ALWIL), Flame (Grisoft), Flame (ClamAV), Flame.A (Panda)

Description added	Mar 07 2000
Behavior	Virus

Technical details

It's a very dangerous floppy Boot and HD MBR infector. It hooks INT 13h. The old Boot-sector is saved into the sector at address 1901/01. As the result, the contents of that sector is corrupted. On MBR infection the virus overwrites it. Sometimes this infector displays the picture that looks like the tongues of flames.

Virus.Boot.Form.a

Aliases

Virus.Boot.Form.a (Kaspersky Lab) is also known as: Form.a (Kaspersky Lab), Form (McAfee), Form (Doctor Web), Form (Sophos), Form (RAV), Form* (Trend Micro), Form.A (H+BEDV), Form (ALWIL), Form (Grisoft), Form.A (SOFTWIN), Form.5 (ClamAV), Form.A (Panda)

Description added	Mar 07 2000
Behavior	Virus

Technical details

This is a very dangerous virus. It hits the boot-sector of floppy disks while accessing them and the boot-sector of the hard disk upon rebooting from an infected floppy disk. The virus acts only on the 16th of every month. It processes a dummy cycle when keys are pressed. If you are working with a hard disk, the data could be lost. The virus hooks INT 9 and INT 13h. It contains the following text:

```
The FORM-Virus sends greetings to everyone who's reading this text.
FORM doesn't destroy data! Don't panic! Fuckings go to Corinne.
```

Virus.Boot.Hob

Aliases

Virus.Boot.Hob (Kaspersky Lab) is also known as: Hob (Kaspersky Lab), Hob (McAfee), Hob (Doctor Web), Hob (Sophos), Hob (RAV), BOOT.GENERIC* (Trend Micro), BOO/Hob (H+BEDV), Hob (FRISK), Hob (ALWIL), Hob (Grisoft), Hob.B (ClamAV), Teramai.512 (Panda)

Description added	Mar 07 2000
Behavior	Virus

Technical details

This is a harmless memory resident stealth boot virus. It hooks INT 13h and infects the MBR of the hard drive and floppy disk boot sector in the A: drive. The virus checks the CMOS fields and in case of AWARD infects the MBR only in case the BIOS VirusWarning protection is disabled. The virus contains the text string:

```
h0b13BzZ
```

Virus.Boot.Incubus.a

Aliases

Virus.Boot.Incubus.a (Kaspersky Lab) is also known as: Incubus.a (Kaspersky Lab), BtDr.Incubus (McAfee), Incubus dropper (Symantec), Incubus.dropper (Doctor Web), Boot dropper (Sophos), Incubus.A (RAV), INCUBUSB-C (Trend Micro), Incubus (Boot) (H+BEDV), BOOT SECTOR DROPPER (FRISK), Incubus-B (ALWIL), Incubus.A (Grisoft), Incubus.A (SOFTWIN), Incubus (Panda)

Description added	Mar 07 2000
Behavior	Virus

Technical details

This is a harmless memory resident boot virus. On loading from infected floppy it infects MBR of hard drive, then it hooks INT 13h or INT 40h depending on the virus version, and infects boot sectors of the floppies.

It contains the internal text strings:

```
Incubus PRiEST - Phalcon/Skism
```

Virus.Boot.JindraBoot

Aliases

Virus.Boot.JindraBoot (Kaspersky Lab) is also known as: JindraBoot (Kaspersky Lab), Jindra (McAfee), Jindra.2049 (Doctor Web), Jindra (Sophos), Jindra (RAV), JINDRABOOT* (Trend Micro), BOO/JINDRA (H+BEDV), Jindra (FRISK), Pastika-2049 (ALWIL), Jindra (Grisoft), JindraBoot (ClamAV)

Description added	Mar 07 2000
Behavior	Virus

Technical details

It is a very dangerous memory resident boot virus. It hooks INT 13h and writes itself to boot sectors of floppy disks and C: drive. On 101st infection the virus erases disk sectors and the CMOS. The virus contains the text:

```
JINDRA_0
```

Virus.Boot.Joshi.a

Aliases

Virus.Boot.Joshi.a (Kaspersky Lab) is also known as: Joshi.a (Kaspersky Lab), BtDr.Joshi (McAfee), Joshi.A (Symantec), Joshi.dropper (Doctor Web), Joshi drop (Sophos), Joshi.A (RAV), JOSHI (Trend Micro), Joshi (Boot) #1 (H+BEDV), BOOT SECTOR DROPPER (FRISK), Joshi (ALWIL), Joshi (Grisoft), Trojan.Dropper.Boot.Joshi.A (SOFTWIN), Joshi Boot (Panda)

Description added	Mar 07 2000
Behavior	Virus

Technical details

These are dangerous stealth viruses. They infect floppy disks Boot-sectors and hard disk MBR during an access to them (INT 13h, ah=2,3,4,0Ah,0Bh). The viruses include two parts - the first part contains the body of the virus and is placed onto the boot sector (or MBR) of the disk, the second part contains the original first sector of the infected disk and the other eight sectors of the virus, and occupies the 40th or 80th track of the floppy disk (the virus uses nonstandard format); on the hard disks the second part of the virus body begins from the second sector of the starting track. The viruses can destroy FAT when they save their own copy on the disk.

The viruses hook INT 21h. Just after starting (rebooting of the system) they permanently check the interrupt vector 21h, and if it is changed the viruses read the new value of the vector. The viruses hook INT 9h (keyboard). When the ALT-CTRL-DEL keys are used to boot the system, the viruses will emulate rebooting: clear the screen and so on. The viruses will stay resident even if you boot the system from a clean and write-protected floppy disk.

On the 5th of January the viruses will display the message "Type `Happy Birthday, Joshi'!" and will wait for the entering "Happy Birthday, Joshi!" from the keyboard. The viruses hook the INT 8, 9, 13h, 21h.

Virus.Boot.KeyDrop

Aliases

Virus.Boot.KeyDrop (Kaspersky Lab) is also known as: KeyDrop (Kaspersky Lab), BtDr.Keydrop (McAfee), Keydrop.dropper (Doctor Web), Dropper Keydrop (Sophos), KeyDrop (RAV), KeyDrop* (Trend Micro), BOO/KEYDR-B (H+BEDV), BOOT SECTOR DROPPER (FRISK), Keydrop (ALWIL), Keydrop (Grisoft), Dropper.Boot.Keydrop (SOFTWIN), BOO.KEYDR-B (ClamAV), Pilla_Mbr.2560 (Panda)

Description added	Mar 07 2000
Behavior	Virus

Technical details

This is a nondangerous virus. It infects in a "Brain" way Boot-sectors of floppy disks during an access and MBR of the hard disk on a reboot from an infected floppy disk. The virus produces the "falling letters" effect (the code is copied from the "Cascade" virus). The virus hooks INT 13h and contains the text "(c) Copyright 1990 Keydrop inc.".

Virus.Boot.Kilroy.a

Aliases

Virus.Boot.Kilroy.a (Kaspersky Lab) is also known as: Kilroy.a (Kaspersky Lab), BtDr.Kilroy (McAfee), Trojan Horse (Symantec), Kilroy.dropper (Doctor Web), Kilroy.K.dr (RAV), KILROY.A-B* (Trend Micro), LBBCV-Kilroy (H+BEDV), BOOT SECTOR DROPPER (FRISK), Lucifer (ALWIL), Kylroy.A (SOFTWIN), LBBCV-Kilroy (ClamAV), Kilroy.DRP (Panda)

Description added	Mar 07 2000
Behavior	Virus

Technical details

This is a non memory-resident dangerous boot virus. It overwrites the boot sectors of floppies and hard drives during loading from an infected disk. This virus does not leave any TSR code and is active only during loading from infected disk. It contains the text strings:

```
KILROY
Kilroy was here!
```

Virus.Boot.Kilroy.Turd.a

Aliases

Virus.Boot.Kilroy.Turd.a (Kaspersky Lab) is also known as: Kilroy.Turd.a (Kaspersky Lab), BtDr.Kilroy (McAfee), Boot.Kilroy (Symantec), Kilroy (Doctor Web), Kilroy Turd (Sophos), Killroy.B.dr (RAV), KILLBOOT (Trend Micro), VGEN/3252.512 (H+BEDV), Kilroy.unknown? (FRISK), Kilroy-D (ALWIL), Kilroy (Grisoft), Kilroy.B (SOFTWIN), KILTURD (ClamAV)

Description added	Jul 22 2000
Behavior	Virus

Technical details

This is a non memory-resident dangerous boot virus. It overwrites the boot sectors of floppies and hard drives during loading from an infected disk. This virus does not leave any TSR code and is active only during loading from infected disk. It contains the text strings:

```
DAVIES
YOU BLACK-COATED TURD!
```

Virus.Boot.KOH.a

Aliases

Virus.Boot.KOH.a (Kaspersky Lab) is also known as: KOH.a (Kaspersky Lab), StealthBoot.KOH.a (McAfee), StealthBoot.KOH (Doctor Web), KOHv1-00 (Sophos), KOH.A (RAV), KOH.A (Trend Micro), K.O.H (Boot) (H+BEDV), Stealth_Boot.KOH.A (FRISK), Koh (ALWIL), Stealth_Boot (Grisoft), KOH v1.0 (Panda)

Description added	Mar 07 2000
Behavior	Virus

Technical details

It's a memory resident boot virus. It hooks INT 09h (keyboard) and INT 13h. On loading from infected floppy it asks user for permission to infect hard drive:

```
KOH-Encrypt your HARD DISK now (please backup first)?
```

and infects HD on 'Y' answer, in another case it returns control to normal booting. On infection of hard drive this virus encrypts its sectors, the virus asks passwords before infection:

```
Now, enter 2 passwords, 1 for HD, 1 for FD. FD PW can be changed anytime
with Ctrl/Alt-K, C/A-O stops FD infect, C/A-H uninstalls on HD. Enter HD
PW at power up. WRITE THIS DOWN!
CASUAL encryption=fast but breakable--keeps out snoops.
STRONG encryption=good but slow--keeps out all. Use disk cache.
Do you want STRONG encryption?
```

On loading from infected HD the virus asks for password and lets booting on true answer only. This virus infects/encrypts floppy disks also. It can decrypt disks and uninstall itself on Ctrl-Alt-K,O,H keyboard keys. This virus contains and displays other strings also:

```
Initial load failed... aborting.
Load successful. A: now infected with KOH.
Sure you want to uninstall?
Should change be permanent?
Enter FLOPPY PW now.
Now enter HD PW.
Enter
Password:
Verify Password:
Verify failed!
KOHv1.00
```

Virus.Boot.Lilith

Aliases

Virus.Boot.Lilith (Kaspersky Lab) is also known as: Lilith (Kaspersky Lab), Lilith (McAfee), Lillith (Doctor Web), Lilith (Sophos), Lilith (RAV), TRAP.LILITH* (Trend Micro), Lilith (FRISK), Lilith (ALWIL), Lilith (Grisoft), Lilith (Panda)

Description added	Mar 07 2000
Behavior	Virus

Technical details

It is not a dangerous memory resident polymorphic and stealth boot virus. To hook INT 13h the virus scans the BIOS code for INT 18h call (CDh 18h), sets INT 13h to that address and hooks INT 18h. Then the virus writes itself to boot sector of the floppy disks and the MBR of the hard drive. Depending on the system timer the virus also hooks INT 5 (Print Screen) and when PrintScreen key is pressed, the virus displays:

```
L · I · L · I · T · H
Tu del creato prima Donna
del Sesso Maestra infernale
accogli le Nostre dannate Carni
nel Tuo satanico Ventre
```

The virus also contains the text string:

```
Milan Italy 95
```

Virus.Boot-DOS.DAN.WMA.451

Aliases

Virus.Boot-DOS.DAN.WMA.451 (Kaspersky Lab) is also known as: DAN.WMA.451 (Kaspersky Lab), WMA.mp (McAfee), Wma.451 (Symantec), WMA.451 (Doctor Web), WMA-451 (Sophos), Wma_II.451 (RAV), WMA.MP.451-O (Trend Micro), WMA #1 (H+BEDV), Wma_II.451 (FRISK), WMA-451 (ALWIL), WMA.451 (Grisoft), PS-MPC.0450.AS.Gen (SOFTWIN), DAN.WMA.451 (ClamAV), Wma.512 (Panda)

Description added Mar 07 2000

Behavior Virus

Technical details

It is a dangerous memory resident multipartite virus. While executing an infected file the virus infects the MBR of the hard drive and returns to DOS. The virus stays memory resident while loading from infected disk (the virus also infects the MBR while loading from infected floppy). The virus hooks INT 13h, waits for DOS loading, then hooks INT 21h and writes itself to the end of COM files that are executed. While accessing to floppy disks the virus overwrites the boot sector. The virus has the bugs, and can halt the system while infecting a floppy disk. The virus contains the text string:

```
wma
```

Virus.Boot-DOS.PFS.3786

Aliases

Virus.Boot-DOS.PFS.3786 (Kaspersky Lab) is also known as: PFS.3786 (Kaspersky Lab), Pofu.mp (McAfee), PowerFul.3795 (Doctor Web), Powerful-3955 (Sophos), PFS.3795 (RAV), PFS.3786 (Trend Micro), BOO/POFU (H+BEDV), PFS.3795 (FRISK), PowerFul-3275 (ALWIL), PFS (Grisoft), PFS.3795 (SOFTWIN), PFS.3762 (Panda)

Description added Mar 07 2000

Behavior Virus

Technical details

This is a benign memory resident encrypted stealth multipartite virus. It infects the MBR of the hard drive and writes itself to the end of COM and EXE files. When an infected file is executed, the virus infects the MBR, hooks INT 21h and stays memory resident. When the system is booted from the infected disk, the virus stays memory resident, hooks INT 8 (timer), wait for DOS loading, then it releases INT 8 and hooks INT 21h.

The virus INT 21h handler hooks more than 10 DOS functions: FindFirst/Next (including long-names calls), open file, close, execute, rename, read, e.t.c. On opening, executing, renaming and file attribute access the virus infects the files. In case of other functions the virus calls its stealth routines.

Plus to file stealth ability the virus uses several quite complex tricks to hide its presence in the system. First of all the virus uses direct disk access calls to bypass BIOS anti-virus protection. To hide its TSR copy the virus leaves in the system memory just 339 bytes of its code - it copies it to the Interrupt Vectors Table. This code contains INT 21h handler that in case of needs reads the complete virus code from the first track of the hard drive and calls it. As a result the virus does not occupy the conventional system memory and is not visible by memory browsers. Depending on the system environment the virus also copies its code to the XMS memory and in case of need reads it from there, not from the hard drive.

The virus contains the text strings:

```
PowerFul Stealth v6.1 (c)'98 DK eyegabooom
```

Virus.Boot-DOS.Pieck.2016

Aliases

Virus.Boot-DOS.Pieck.2016 (Kaspersky Lab) is also known as: Pieck.2016 (Kaspersky Lab), Kaczor.mp.2016 (McAfee), Pieck.2016 (Symantec), Pieck.2016 (Doctor Web), Pieck (Sophos), Pieck_II.2016 (RAV), PIECK_II.2016 (Trend Micro), VGEN/3210.512 (H+BEDV), Pieck_II.2016 (FRISK), Pieck-2016 (ALWIL), Pieck.2016 (Grisoft), Pieck_II.2016 (SOFTWIN), Pieck_II.2016 (Panda), Pieck.2016 (Eset)

Description added Mar 07 2000

Behavior Virus

Technical details

It's a not dangerous memory resident multipartite virus. On execution it checks the DOS version and infects MBR and installs itself into the memory under DOS 5.x and 6.x only. It hooks INT 12h, 13h, 1Ch, 21h and writes itself at the end of EXE-files are executed or opened.

On March, 3th it displays the message: "Podaj haslo ?", waits for "pieck" entry and displays "Pozdrowienia dla wychowankow Pieck'a." if "pieck" is entered, in another case it displays "Blad !".

Virus.Boot-DOS.Plagiarist.2014

Aliases

Virus.Boot-DOS.Plagiarist.2014 (Kaspersky Lab) is also known as: Plagiarist.2014 (Kaspersky Lab), Plagiarist.mp (McAfee), Plagiarist.2014 (Doctor Web), Plagiarism (Sophos), Plagiarist.2xxx (RAV), Plague (Boot) (H+BEDV), Plagiarist.2xxx (FRISK), Plagiarist (ALWIL), Plagiarist.2014 (ClamAV), Plagiarist.Boot (Panda)

Description added Mar 07 2000

Behavior Virus

Technical details

It's a not dangerous memory resident multipartite virus. It infects boot sector of floppy and hard drives and writes itself at the end of COM-files (except COMMAND.COM) are executed. It hooks interrupt vectors INT 17h for trigger routine, INT 21h for COM-file infection, INT 28h for INT 21h interception, INT 08h, 13h for INT 28h interception. The trigger routine: this virus searches for text "Andy Warhol" in any text sent to printer and replaces it with "Ron English".

Virus.Boot-DOS.Playgame.1999

Other versions: .2000

Aliases

Virus.Boot-DOS.Playgame.1999 (Kaspersky Lab) is also known as: Playgame.1999 (Kaspersky Lab), Playgame.mp (McAfee), Bin.Auto.CLR (Symantec), Junk/PlayGame (Sophos), Playgame (RAV), HAPPY-B* (Trend Micro), Playgame (Boot) (H+BEDV), Playgame.1999 (FRISK), Trident-Playgame-2000 (ALWIL), Playgame (Grisoft), PS-MPC.1999.AF.Gen.Damaged (SOFTWIN), KillMbr.1999 (Panda)

Description added Mar 07 2000

Behavior Virus

Technical details

This is a benign memory-resident multipartite virus. While executing an infected file, the virus writes itself to the hard drive MBR, and returns control to the host program. The virus stays memory resident upon loading from an infected disk only. The virus hooks INT 13h and 21h, and writes itself to the end of accessed EXE files.

The virus contains the string "CO4DSCCLVSNEHTTBVIF-FIGIIMRAFEMTBR", and does not infect files if the first two bytes of the file name consist of two characters from this string (CO*.*, 4D*.*, SC*.*, ...). This virus also contains the text string:

```
[ MK / TridenT ]
```

In December, this virus starts a game, and, while playing the game, it displays the following message:

```
HAPPY VIRUS Time to play a game (Use shift keys)
You reached level Play again?
```

Virus.Boot-DOS.Playgame.2000

Other versions: .1999

Aliases

Virus.Boot-DOS.Playgame.2000 (Kaspersky Lab) is also known as: Playgame.2000 (Kaspersky Lab), Playgame.mp (McAfee), Playgame-1999 (Sophos), Playgame (RAV), HAPPY-B* (Trend Micro), Playgame (Boot) (H+BEDV), Playgame.C (FRISK), Trident-Playgame-2000 (ALWIL), Playgame (Grisoft), Playgame.1999 (Panda)

Description added Jul 22 2000

Behavior Virus

Technical details

This is a benign memory-resident multipartite virus. While executing an infected file, the virus writes itself to the hard drive MBR, and returns control to the host program. The virus stays memory resident upon loading from an infected disk only. The virus hooks INT 13h and 21h, and writes itself to the end of accessed EXE files.

The virus contains the string "CO4DSCCLVSNEHTTBVIF-FIGIIMRAFEMTBR", and does not infect files if the first two bytes of the file name consist of two characters from this string (CO*.*, 4D*.*, SC*.*, ...). This virus also contains the text string:

```
[ MK / TridenT ]
```

In December, this virus starts a game, and, while playing the game, it displays the following message:

```
HAPPY VIRUS Time to play a game (Use shift keys)
You reached level Play again?
```

Virus.Boot-DOS.PresidentB.1504

Aliases

Virus.Boot-DOS.PresidentB.1504 (Kaspersky Lab) is also known as: PresidentB.1504 (Kaspersky Lab), Pres.mp.1504 (McAfee), PresidentB.1504 (Symantec), President.1504 (Doctor Web), President-B (Sophos), President.1504 (RAV), PRESIDENT.1504 (Trend Micro), VGEN/13929.512 (H+BEDV), President.1504 (FRISK), President-1504 (ALWIL), President (Grisoft), President.1504 (SOFTWIN), PresidentB (Panda)

Description added Mar 07 2000

Behavior Virus

Technical details

This is a very dangerous memory resident encrypted multipartite virus. When an infected file is executed, the virus decrypts itself, hooks INT 13h and 21h, and returns control to the host program. While loading from an infected floppy disk, the virus hooks INT 12h and 13h, and waits for the DOS loading process and hooks INT 21h.

The virus then writes itself to the end of COM and EXE files that are executed or loaded as overlays or for debugging. Upon accessing 1.4Mb-floppy disks, the virus infects their boot sectors.

On April 26th, the virus erases the MBR of the hard drive and displays the following message:

```
** President B ][ **
```

Virus.Boot-DOS.Prowler.1543

Aliases

Virus.Boot-DOS.Prowler.1543 (Kaspersky Lab) is also known as: Prowler.1543 (Kaspersky Lab), Prowler.mp (McAfee), Bin.Auto.CFU (Symantec), Prowler-1543 (Sophos), Prowler.1543 (RAV), PROWLER.1543 (Trend Micro), PROW1727 (H+BEDV), Prowler.1543 (FRISK), Prowler-1543-B (ALWIL), Prowler.1543 (SOFTWIN), Powler.1543 (Panda)

Description added Mar 07 2000

Behavior Virus

Technical details

These are relatively harmless, memory resident encrypted multipartite viruses. They infect the MBR of the hard drive and write themselves to the end of COM (except COMMAND.COM) and EXE files that are executed, and the viruses hook INT 21h to do that. The MBR is infected when an infected file is executed. To install the TSR copy while loading from an infected MBR, the viruses also temporarily hook INT 1Ch (timer).

Upon loading from infected MBR on 13th of any month, the viruses manifest themselves as a sound and video effect and display the following message:

```
I am +he Midnigh+ Pr0wler, s0n 0f +he m00n
And I am the child 0f +he ?? genera+i0n....
```

where ?? is virus generation.

Virus.Boot-DOS.QPHS.2931

Aliases

Virus.Boot-DOS.QPHS.2931 (Kaspersky Lab) is also known as: QPHS.2931 (Kaspersky Lab), Kaczor.mp.2931 (McAfee), Kaczor.2931 (Doctor Web), QPHS (Sophos), Qpis.2931! (RAV), QBIS.2931-C (Trend Micro), VGEN/12923.256 (H+BEDV), Qpis.2931 (FRISK), Qpis-2931 (ALWIL), Pieck (Grisoft), Qpis.2931 (SOFTWIN), QPHS.2931 (ClamAV), Qpis.2931 (Panda)

Description added Mar 07 2000

Behavior Virus

Technical details

It is not a dangerous memory resident multipartite virus. While executing an infected file the virus infects the MBR of the hard drive, hooks INT 9, 13h, 21h and stays memory resident. While infecting the hard drive the virus encrypts the original Partition Table. On reading the MBR the virus calls the stealth routine and returns the Partition Table in its original form.

While loading from infected MBR the virus hooks INT 8, 9, 12h, 13h, waits for DOS loading, and then hooks INT 21h. The virus uses INT 12h to hide itself in the system memory during the DOS installation procedure.

By hooking INT 21h the virus intercepts COM and EXE files opening, execution and searching. The virus writes itself to the end of the files on A: and B: drives only, and disinfects the infected files on other disks.

The virus pays special attention to the execution of LOGIN.EXE file, and saves the command line and entered from keyboard symbols during execution of LOGIN.EXE. By using that trick the virus allows to intercept login commands (user names and passwords).

The virus intercepts the symbols entered from keyboard. On entering the "QPHS" string the virus display the intercepted login commands. On entering the "PERFECT" string the virus disinfects itself in the MBR of the hard drive.

Virus.Boot-DOS.Radom.2688

Aliases

Virus.Boot-DOS.Radom.2688 (Kaspersky Lab) is also known as: Radom.2688 (Kaspersky Lab), Vague.mp (McAfee), Radom.2688 (Doctor Web), Lupomania.2672 (RAV), BOOT.GENERIC* (Trend Micro), BOO/VAGUE (H+BEDV), Lupomania.2672 (FRISK), Vague-2688 (ALWIL)

Description added Mar 07 2000

Behavior Virus

Technical details

It is not a dangerous memory resident encrypted multipartite stealth virus. It hooks INT 13h, 21h and writes itself to the end of COM and EXE files, as well as to the MBR of the hard drive and boot sectors on floppy disks. If the system date is November 10 1999, the virus decrypts and displays the text:

```
Wirus Version 1.0 Copyright (c) 1997 Speedy
Radom - ZSE .
```

Virus.Boot-DOS.Raiden.1433

Aliases

Virus.Boot-DOS.Raiden.1433 (Kaspersky Lab) is also known as: Raiden.1433 (Kaspersky Lab), Raiden.mp.1433 (McAfee), Raiden.1433 (Doctor Web), Raiden (Sophos), Raiden.1433.dr (RAV), RAIDEN.1433 (Trend Micro), VGEN/12312.512 (H+BEDV), Raiden.1433 (FRISK), MBR-1433 (ALWIL), Raiden.1433 (SOFTWIN), Raiden.1433 (ClamAV), Raiden.1433.DRP (Panda), TSR.EXE.BOOT (Eset)

Description added Mar 07 2000

Behavior Virus

Technical details

It is not a dangerous memory resident multipartite virus. When an infected file is executed, the virus infects the MBR of the hard drive. While loading from infected MBR the virus hooks INT 13h, 1Ch, 4Fh, waits for DOS loading process and hooks INT 21h. By hooking INT 21h the virus intercepts EXE files execution and opening, and writes itself to the end of the file. By hooking INT 13h the virus intercepts accessing to infected MBR and calls stealth routine.

In some cases (depending on the command line) the virus disinfects the host file. On INT 4Fh AX=666h calls the virus displays the message:

```
+--------------------------------------+
¦ MBR VIRUS V.01  NECROSOFT CORPORATION ¦
¦ WRITEN BY RAIDEN  COPYRIGHT  (C) 1996 ¦
+--------------------------------------+
```

Virus.Boot-DOS.Rainbow.2351

Aliases

Virus.Boot-DOS.Rainbow.2351 (Kaspersky Lab) is also known as: Rainbow.2351 (Kaspersky Lab), Ginger.O/R.mp (McAfee), Ginger.Rainbow.2351 (Doctor Web), Rainbow (Sophos), Ginger.2351 (RAV), RAINBOW.2351.B-B (Trend Micro), Rainbow (Boot) (H+BEDV), Ginger.2351 (FRISK), Rainbow-2351 (ALWIL), Ginger (Grisoft), Ginger.2351 (SOFTWIN), Ginger.2351 (Panda)

Description added Mar 07 2000

Behavior Virus

Technical details

It is harmless memory resident stealth multipartite virus. It hooks INT 12h, 13h, 21h, 2Fh and writes itself at the end of COM- and EXE-files are accessed. It writes itself into MBR of the hard drive and boot sectors of the floppy disks. It contains the internal text strings:

```
HiAnMiT - roy g biv
*4U2NV*
04/12/94
```

Virus.Boot-DOS.Rajaat.518

Aliases

Virus.Boot-DOS.Rajaat.518 (Kaspersky Lab) is also known as: Rajaat.518 (Kaspersky Lab), Andropinis.mp (McAfee), Rajaat.518 (2) (Symantec), SSS/Rajaat-518 (Sophos), Rajaat.512.A (RAV), RAJA518B (Trend Micro), VGEN/3313.0 (H+BEDV), Rajaat.518.A (FRISK), Rajaat-518 (ALWIL), Andropin (Grisoft), Rajaat.518.A (SOFTWIN), Suspect File (Panda)

Description added Mar 07 2000

Behavior Virus

Technical details

Rajaat.518 is a dangerous memory resident multipartite virus. During execution of an infected file the virus hits the MBR of the hard drive. While infecting it redirects the active boot sector to the virus body (see Starship virus). On loading from infected MBR it hooks INT 13h, 21h and writes itself at the end of .COM-files on writing (INT 21h, AH=40h) to them. It hits COMMAND.COM file. It may cause the system crash on DOS loading. The virus contains the internal text string:

```
[Andropinis] by Rajaat
```

Virus.Boot-DOS.Rasek.1310

Other versions: .1489, .1489.b, .1490, .1492

Aliases

Virus.Boot-DOS.Rasek.1310 (Kaspersky Lab) is also known as: Rasek.1310 (Kaspersky Lab), Rasek.mp (McAfee), RaseK (Doctor Web), Rasek-1310 (Sophos), Rasek.1310 (RAV), RASEK.1310.A-B (Trend Micro), BOO/RAS1490 (H+BEDV), Rasek-1310-B (ALWIL), Rasek.1310 (ClamAV), Rasek.1490.Boot (Panda)

Description added Mar 07 2000

Behavior Virus

Technical details

This is a dangerous memory resident multipartite encrypted virus. While executing an infected file it writes itself to the MBR of the hard drive and hooks INT 13h, 12h. By hooking INT 13h this virus releases the stealth mechanism on reading the infected MBR. It also writes a trojan program to the floppy disk boot sectors. That program erases the hard drive FAT while loading from that floppy. Sometimes the virus also erases the FAT on loading from infected MBR.

By hooking INT 21h the virus infects COM and EXE files that are executed, it writes itself to the end of the files. The virus contains the text string "AND.COM" and does not infect the files that contains that string in their names (COMMAND.COM). The virus also contains the text strings:

```
RASEK v1.1,from LA CORUÑA(SPAIN).Jan93
```

Virus.Boot-DOS.Rasek.1489.b

Other versions: .1310, .1489, .1490, .1492

Aliases

Virus.Boot-DOS.Rasek.1489.b (Kaspersky Lab) is also known as: Rasek.1489.b (Kaspersky Lab), Rasek.mp (McAfee), RaseK.1489 (Doctor Web), Rasek-1489b (Sophos), Rasek.1489.B (RAV), RASEK.1489.B-B (Trend Micro), Rasek (Boot) #3 (H+BEDV), Rasek.1489 (FRISK), Rasek-1489-C (ALWIL), Rasek.1492.Boot (Panda)

Description added Jul 13 2000

Behavior Virus

Technical details

This is a dangerous memory resident multipartite encrypted virus. While executing an infected file it writes itself to the MBR of the hard drive and hooks INT 13h, 12h. By hooking INT 13h this virus releases the stealth mechanism on reading the infected MBR. It also writes a trojan program to the floppy disk boot sectors. That program erases the hard drive FAT while loading from that floppy. Sometimes the virus also erases the FAT on loading from infected MBR.

By hooking INT 21h the virus infects COM and EXE files that are executed, it writes itself to the end of the files. The virus contains the text string "AND.COM" and does not infect the files that contains that string in their names (COMMAND.COM). The virus also contains the text strings:

```
"RASEK" v3.0,from La Coruña(SPAIN).Ap93
```

Virus.Boot-DOS.Rasek.1489

Other versions: .1310, .1489.b, .1490, .1492

Aliases

Virus.Boot-DOS.Rasek.1489 (Kaspersky Lab) is also known as: Rasek.1489 (Kaspersky Lab), Rasek.mp.1489a (McAfee), Rasek.1489 (Symantec), RaseK.1489 (Doctor Web), Rasek-1489 (Sophos), Rasek.1310 (RAV), RASEK.1489 (Trend Micro), Rasek #1 (H+BEDV), Rasek.1489.A (FRISK), Rasek-1489 (ALWIL), Rasek (Grisoft), Rasek.1489.D (SOFTWIN), Coru.qa (Panda)

Description added Jul 13 2000

Behavior Virus

Technical details

This is a dangerous memory resident multipartite encrypted virus. While executing an infected file it writes itself to the MBR of the hard drive and hooks INT 13h, 12h. By hooking INT 13h this virus releases the stealth mechanism on reading the infected MBR. It also writes a trojan program to the floppy disk boot sectors. That program erases the hard drive FAT while loading from that floppy. Sometimes the virus also erases the FAT on loading from infected MBR.

By hooking INT 21h the virus infects COM and EXE files that are executed, it writes itself to the end of the files. The virus contains the text string "AND.COM" and does not infect the files that contains that string in their names (COMMAND.COM). The virus also contains the text strings:

```
RaseK v2.1,from LA CORUÑA(SPAIN).Mar93
```

Virus.Boot-DOS.Rasek.1490

Other versions: .1310, .1489, .1489.b, .1492

Aliases

Virus.Boot-DOS.Rasek.1490 (Kaspersky Lab) is also known as: Rasek.1490 (Kaspersky Lab), Rasek.mp.1490 (McAfee), Rasek.1490 (x) (Symantec), RaseK.1490 (Doctor Web), Rasek-1490 (Sophos), Rasek.1310 (RAV), RASEK.1490 (Trend Micro), Rasek #1 (H+BEDV), Rasek.1490.B (FRISK), Rasek-1490 (ALWIL), Rasek (Grisoft), Rasek.1490.B (SOFTWIN), Rasek.1490.B (Panda), CRYPT.TSR.COM.EXE.BOOT (Eset)

Description added Jul 13 2000

Behavior Virus

Technical details

This is a dangerous memory resident multipartite encrypted virus. While executing an infected file it writes itself to the MBR of the hard drive and hooks INT 13h, 12h. By hooking INT 13h this virus releases the stealth mechanism on reading the infected MBR. It also writes a trojan program to the floppy disk boot sectors. That program erases the hard drive FAT while loading from that floppy. Sometimes the virus also erases the FAT on loading from infected MBR.

By hooking INT 21h the virus infects COM and EXE files that are executed, it writes itself to the end of the files. The virus contains the text string "AND.COM" and does not infect the files that contains that string in their names (COMMAND.COM). The virus also contains the text strings:

```
RaseK v2.0,from LA CORUÑA(SPAIN).Mar93
```

Virus.Boot-DOS.Renegade.1176

Aliases

Virus.Boot-DOS.Renegade.1176 (Kaspersky Lab) is also known as: Renegade.1176 (Kaspersky Lab), Renegade.1176 (McAfee), Renegade.1176 (1) (Symantec), Renegade (Sophos), Renegade.1176 (RAV), RENEGADE.1176 (Trend Micro), Renegade (H+BEDV), Renegade-1176 (ALWIL), Renegade.1176 (ClamAV), Renegade.1176 (Panda)

Description added Mar 07 2000

Behavior Virus

Technical details

It is not a dangerous memory resident encrypted parasitic virus. It hooks INT 21h and writes itself into the middle of EXE files that are executed, opened or closed. On 17th of each month it displays the message:

```
(C) Renegade 1994.  Hello  Hacker`s !!!
```

Virus.Boot-DOS.Res.2879

Aliases

Virus.Boot-DOS.Res.2879 (Kaspersky Lab) is also known as: Res.2879 (Kaspersky Lab), Res.mp (McAfee), Virus.Dropper (Symantec), Res.based (Doctor Web), Res-2879 (Sophos), Res.28xx (RAV), RES.2979-B (Trend Micro), DOS/Res.2879 (H+BEDV), Res.28xx (FRISK), Res-28XX (ALWIL)

Description added Mar 07 2000

Behavior Virus

Technical details

These are harmless memory resident multipartite encrypted stealth viruses. They hook INT 13h, 21h and write themselves to the end of COM and EXE files that are accessed. The viruses also infect the MBR of the hard drive and boot sector on the 1.4Mb floppy disks.

The viruses check file names and do not infect several anti-virus programs and archivers. The viruses contain the text strings, the first strings contains the identification letters for files that are not infected by the virus (two letters per name, the viruses check two last letters of names):

```
NFEBSTTERJIPHAAR
[RES] VVS
```

"Res.4258" also embeds itself to the FIDO mails (.PKT files). While embedding the virus creates its dropper with the LIFE.COM name, converts it to ASCII data by using standard UUE method, and adds these data to the end if victim message as a block of encoded data.

Virus.Boot-DOS.Rex.1637

Aliases

Virus.Boot-DOS.Rex.1637 (Kaspersky Lab) is also known as: Rex.1637 (Kaspersky Lab), Rex.mp.1637 (McAfee), Rex.1637 (Symantec), Rex (Sophos), Rex.1637 (RAV), ROMMEI-G-1 (Trend Micro), BOO/REX (H+BEDV), Rex.1637 (FRISK), Rex-1637 (ALWIL), Rex.1637 (SOFTWIN), Rex.1637 (Panda)

Description added Mar 07 2000

Behavior Virus

Technical details

Rex.1637 is a dangerous memory resident encrypted multipartite virus. It hooks INT 16h, 21h, and on file opening it searches for COM- and EXE-files, and writes itself at their ends. In some cases it duplicates the keystrokes that are entered. The virus contains errors and may halt the computer. Rex.1637 contains the internal text strings:

```
REX
*.com *.exe
```

Virus.Boot-DOS.Samara.1536

Aliases

Virus.Boot-DOS.Samara.1536 (Kaspersky Lab) is also known as: Samara.1536 (Kaspersky Lab), Samara.mp.1536 (McAfee), SAMARA.1536 (Symantec), Samara.1536 (Doctor Web), Samara-1536 (Sophos), Win4.1536 (RAV), SAMARA.1536 (Trend Micro), VGEN/50766 (H+BEDV), Win4.1536.damaged? (FRISK), Samara-1536 (ALWIL), Musicbug (Grisoft), Win4.1536.damaged (SOFTWIN), Kill.Mbr (Panda), POLY.CRYPT.TSR.COM.EXE.BOOT (Eset)

Description added Mar 07 2000

Behavior Virus

Technical details

It is not a dangerous memory resident multipartite polymorphic virus. When an infected file is executed, the virus affects the MBR of the hard drive, then hooks INT 21h and writes itself to the end of COM and EXE files (except COMMAND.COM) that are accessed. The virus cancels anti-virus programs execution: AVPLITE, AIDSTEST, AVP, DRWEB, SCAN.

On loading from infected MBR the virus hooks INT 13h, waits for DOS loading process and hooks INT 21h. On loading from infected floppy disk the virus also infects the hard drive MBR.

While infecting the MBR and boot sectors the virus does not stores their original contents. To continue loading under infected environment the virus reads and executes the first sector on the C: drive. This sector usually contains standard OS loading routine.

Virus.Boot-DOS.Senda.4162

Aliases

Virus.Boot-DOS.Senda.4162 (Kaspersky Lab) is also known as: Senda.4162 (Kaspersky Lab), Senda.mp (McAfee), Senda.4162 (Doctor Web), Senda-4162 (Sophos), Senda (RAV), SENDA.4162.A-B (Trend Micro), BOO/SENDA (H+BEDV), Senda (FRISK), Senda-4162 (ALWIL), Senda.4162.MBR (Panda)

Description added Mar 07 2000

Behavior Virus

Technical details

It is a dangerous memory resident encrypted multipartite virus. It writes itself to the end of .COM files and infects the MBR of the hard drive and boot sector of floppy disks. To intercept system events the virus hooks INT 13h, 21h. The virus has a bug and infect Windows' COMMAND.COM. As a result the virus corrupts the COMMAND.COM and the system halts. The virus contains the text:

```
- Senda, dedicated to my love PL -
```

Virus.Boot-DOS.Shimmer.a

Aliases

Virus.Boot-DOS.Shimmer.a (Kaspersky Lab) is also known as: Shimmer.a (Kaspersky Lab), Shimmer.mp (McAfee), BAT.Shimmer.A (Symantec), Q.Shimmer (Doctor Web), Shimmer-a (Sophos), Shimmer.A (RAV), SHIMMER.A (Trend Micro), VGEN/3401.0 (H+BEDV), Shimmer.A (FRISK), New (ALWIL), Shimmer (Grisoft), Shimmer.A (SOFTWIN), Vgen.3401 (ClamAV), TPE.Poet (Panda)

Description added Mar 07 2000

Behavior Virus

Technical details

These are dangerous memory resident multipartite viruses. They infect the boot sectors of the floppy disks, and create BAT and EXE worms with the virus body inside. To install their TSR copies the viruses use HMA and video memory.

The method of infection of the BAT files is the same as used in "Winstart" virus. The "Shimmer" virus creates the WINSTART.BAT file in the C:\WINDOWS directory and writes itself into there. While executing an infected WINSTART.BAT the virus creates INSTALL.EXE file, and executes that file. INSTALL.EXE contains the virus installator, its code hooks INT 2Fh,40h and overwrites with the virus code the boot sectors of the floppy disks that are accessed.

On loading from infected floppy the virus hooks INT 1Ah, waits for DOS loading, hooks INT 21h, and creates the C:\WINDOWS\WINSTART.BAT worm during the first call to INT 21h. Then the virus disables its infection routine.

The viruses have the bugs and may halt the system. "Shimmer.b" outputs the string "ATM0L0S0=1O1" to the COM port. The viruses contain the text strings:

"Shimmer.a"

```
:yt
@echo.PKX>install.exe
@copy/b install.exe+%0.bat>nul
@install.exe
c:\windows\winstart.bat
New Shimmer
```

"Shimmer.b"

```
:y~ATM0L0S0=1O1
@ECHO PKX>INSTALL.EXE
@COPY/B INSTALL.EXE+%0.BAT>NUL
@INSTALL.EXE
C:\WINDOWS\WINSTART.BAT
```

Virus.Boot-DOS.Shrapnel.6067

Aliases

Virus.Boot-DOS.Shrapnel.6067 (Kaspersky Lab) is also known as: Shrapnel.6067 (Kaspersky Lab), Shrapnel.mp.6067 (McAfee), Shrapnel.6067 (Symantec), Shrapnel.6067 (Doctor Web), Shrapnel-1.0 (Sophos), Shrapnel.6067 (RAV), SHRAPNEL.6067 (Trend Micro), Shrapnel (Boot) (H+BEDV), Shrapnel.6067 (FRISK), Shrapnel-6067 (ALWIL), Brain (Grisoft), Shrapnel.6067 (SOFTWIN), Shrapnel.6067 (ClamAV), Shrapnel.6067 (Panda), CRYPT.TSR.COM.EXE.BOOT (Eset)

Description added Mar 07 2000

Behavior Virus

Technical details

It is a dangerous memory resident multipartite stealth virus. It writes itself to the end of COM, EXE and NewEXE files (Windows) as well as to the MBR of the hard drive and boot sector of floppy disks.

When an infected file is executed, the virus checks the presence of MS Windows. If Windows is installed, the virus searches for EXE files in the current directory and infects them. Then the virus infects the MBR of the hard drive. If Windows is installed, the virus uses direct calls to hard drive ports to write data to the disk. The virus then returns control to the host program.

While loading from an infected disk the virus hooks INT 13h, 1Ch, waits for DOS loading process and hooks INT 21h, 2Fh. The virus then writes itself to the end of files that are executed. When PKZIP or ARJ archivers are run, the virus disables its stealth routines. The virus does not infect the files (anti-viruses, utilities, and more) TBAV, COMMAND, WIN, SCAN, AVP, F-PROT, NAV and so on according to the string (two letters per name):

```
TBCOWISCVIAVVAF-NAVSIVFIFVIMQBMSDODESW
```

The virus deletes the file:

```
C:\WINDOWS\SYSTEM\IOSUBSYS\HSFLOP.PDR
```

Depending on its counters the virus creates the subdirectory SHRAPNEL on the disk.

The virus also contains the texts:

```
SHRAPNEL v1.0 by PH Made in the USA
*.EXE
```

Virus.Boot-DOS.Smile.4320.a

Aliases

Virus.Boot-DOS.Smile.4320.a (Kaspersky Lab) is also known as: Smile.4320.a (Kaspersky Lab), Yesmile.mp (McAfee), Yesmile.5504 (Symantec), Smile.5504 (Doctor Web), Smile-5504 (Sophos), Yesmile.5504.C (RAV), YESMILE (Trend Micro), Funface (Boot) (H+BEDV), Yesmile.5504.A (FRISK), Yesmile-5504 (ALWIL), Yesmile (Grisoft), Yesmile.5504.B (SOFTWIN), Smiley Boot (Panda), Smile.S (Eset)

Description added Mar 07 2000

Behavior Virus

Technical details

Smile is a not dangerous memory resident multipartite virus. On execution of infected file it writes itself into MBR of the hard drive and returns the control to the host program. On loading from infected MBR it hooks INT 1Ch and waits for DOS loading. Then it hooks INT 21h and writes itself at the beginning at the COM- and EXE-files. Sometimes it hooks INT 8 and plays something.

Virus.Boot-DOS.Snafu

Aliases

Virus.Boot-DOS.Snafu (Kaspersky Lab) is also known as: Snafu (Kaspersky Lab), Snafu.mp.cmp (McAfee), Virus.Dropper (Symantec), Snafu-1024 (Sophos), Snafu (RAV), SNAFU.A-B (Trend Micro), BOO/SNAFU (H+BEDV), Snafu (FRISK), Snafu-1024 (ALWIL), Snafu (ClamAV), Snafu.1024.B (Panda)

Description added Mar 07 2000

Behavior Virus

Technical details

It is not a dangerous memory resident multipartite virus. It infects EXE-files, the MBR of the hard drive and boot sector of 1.2Mb floppy disks. It hooks INT 13h, 21h and copies its TSR code to high memory area (HMA). While infecting EXE files the virus creates and writes itself to companion COM files. When such file is executed on non-infected PC, the virus beeps and infects the hard drive MBR.

Virus.Boot-DOS.Sphinx.2751

Aliases

Virus.Boot-DOS.Sphinx.2751 (Kaspersky Lab) is also known as: Sphinx.2751 (Kaspersky Lab), Sphinx.mp.2751 (McAfee), Sphinx (Symantec), Sphinx.2751 (Doctor Web), Sphinx (Sophos), Sphinx.2751 (RAV), Sphinx (Trend Micro), VGEN/3455.512 (H+BEDV), Sphinx.2751 (FRISK), Sphinx-2751 (ALWIL), Sphinx (Grisoft), PS-MPC.2751.AZ.Gen (SOFTWIN), Sphinix.II (Panda)

Description added Mar 07 2000

Behavior Virus

Technical details

Sphinx.2751 is dangerous memory resident multipartite virus. On execution of infected file it hits MBR of hard drive. On loading from infected MBR it hooks INT 1Ch, then INT 13h, 21h and on termination of programs it searches for COM- and EXE-files and writes itself at their ends. It contains the bugs and in some cases corrupts the files instead of infection. Depending on system time it displays the messages:

```
Bonjour, je suis le SPHINX de la légende.  Tu veux jouer avec moi ?
Mauvaise réponse...
Bonne réponse...
Tant pis, tu jouras quand même...
Qui marche à quatres pattes le matin ,
à deux pattes le midi et sur trois pattes le soir ?
Donne la réponse en cinq lettres :
```

waits for input string "homme" and erases the disk sectors.

Virus.Boot-DOS.Starship

Aliases

Virus.Boot-DOS.Starship (Kaspersky Lab) is also known as: Starship (Kaspersky Lab), Starship.mp (McAfee), Starship (Doctor Web), Starship (Boot) (H+BEDV), Starship (FRISK), Starship-2632 (ALWIL), Starship.Boo (Panda)

Description added Mar 07 2000

Behavior Virus

Technical details

This is a memory resident and not dangerous stealth polymorphic virus. It infects only newly created COM- and EXE-files on the A: and B: drives. The virus also infects MBR of the hard disk if an infected file is started. As a result of this policy the virus stays resident in memory and can be moved to other computers with the minimum of the infected objects. So it is more difficult to find the virus. There is one more reason to use such a policy: when only newly created files are infected there is no need to control the DOS fatal errors (INT 24h).

The virus infects files in a standard way using the polymorphic mechanism. To infect a disk the virus puts itself into the last sectors of it, replaces the active boot sector address in the Partition Table with its own starting address. During an access to MBR or to the last sectors the virus uses stealth mechanism.

The virus infects the memory during rebooting from an infected disk. It places some part of its TSR copy into the interrupt vectors table (0000:02C0) and into BIOS Data Area (0000:04B0); the main part of the code is placed into the video RAM (BB00:0050). When the operating system is loaded the virus looks for other programs. If some program has been swapped from the memory (Exit - INT 20h, INT 21h and ah=0 or 4Ch) the virus moves from the video RAM to the place of the program. If a program remains resident (Keep - INT 27h, INT 21 and ah= 31h) the virus "attaches" its code to the program body. The virus recovers its main part in the video RAM if this part has been corrupted, and does this from the disk.

Depending on the internal counters the virus "beeps" using Morse code and shows "stars" on the screen. It contains the string ">STARSHIP_1<". The virus hooks INT 13h, 20h, 21h, 27h.

Virus.Boot-DOS.SVC.4644.a

Aliases

Virus.Boot-DOS.SVC.4644.a (Kaspersky Lab) is also known as: SVC.4644.a (Kaspersky Lab), SVC.mp (McAfee), SVC.4644 (Doctor Web), SVC-4644 (Sophos), SVC (RAV), SVC-4677 (Trend Micro), SVC-6.0 (Boot) #2 (H+BEDV), SVC.46xx.B (FRISK), SVC-4644 (ALWIL), SVC (Grisoft)

Description added Mar 07 2000

Behavior Virus

Technical details

These are harmless memory-resident viruses. They hit the MBR of the hard disk as soon as an infected file is started. The viruses also affect COM-, EXE-, OVL- and SYS-files (except COMMAND.COM and IBM*.*) whenever they are accessed. These viruses cure the infected files if they are debugged. The infectors contain the texts:

```
"SVC.4644,.4677":  /* (c) 1990-91 by SVC, Vers. 6.0 */
"SVC.4661":        /* (c) 1990-91 by Moscow SVC, Vers. 6.0 */
```

and hook INT 8, 13h, 21h. The viruses writes into CMOS from address 34h the string like a "SVC 6.0".

Virus.Boot-DOS.TD.1536

Other versions: .V.1253, .V.1526, .V.1536

Aliases

Virus.Boot-DOS.TD.1536 (Kaspersky Lab) is also known as: TD.1536 (Kaspersky Lab), Bap.mp.1536 (McAfee), TD.1536 (Symantec), Baphometh.1536 (Doctor Web), Baph TD-1536 (Sophos), Baphometh.1536.A (RAV), BAPHTOME.1536-E (Trend Micro), BOO/BAP (H+BEDV), Baphometh.1536.A (FRISK), Baphometh-1536 (ALWIL), Baphometh (Grisoft), Baphometh.1536.A (SOFTWIN), TD.1536 (ClamAV), Baphometh.1536 (Panda), Bap.1536.A (Eset)

Description added Mar 07 2000

Behavior Virus

Technical details

It is not a dangerous memory resident multipartite virus. It writes itself to the end of COM and EXE files, to the MBR of the hard drive and to the boot sector of floppy disks. The virus does not manifest itself by any sound or video effect. It was named after its ID-text "TD" that presents in infected files, boot and MBR sectors.

When an infected file is executed, the virus infects the MBR of the hard drive, hooks INT 21h and stays memory resident. It then affects files that are executed. The virus pays attention to Windows self-checking signature ENUNS that presents at the end of Windows COM files and patches it. While installing memory resident the virus also infects the C:\WINDOWS\WIN.COM file and deletes the C:\WINDOWS\SYSTEM\IOSUBSYS\HSFLOP.PDR file, if they exist.

On loading from infected disk the virus hooks INT 13h, 1Ch, waits for DOS loading process and then hooks INT 21h. By hooking INT 13h the virus infects floppy disks, INT 13h handler also has stealth routine that is activated on accessing to already infected disks.

Virus.Boot-DOS.TeaForTwo.1024

Aliases

Virus.Boot-DOS.TeaForTwo.1024 (Kaspersky Lab) is also known as: TeaForTwo.1024 (Kaspersky Lab), Tea.mp (McAfee), TeaForTwo (Sophos), TeaForTwo (RAV), TEAFORTWO.1024-B (Trend Micro), BOO/Tea (H+BEDV), Tea for (ALWIL), Tea (Grisoft), TeaForTwo.1024 (ClamAV)

Description added Mar 07 2000

Behavior Virus

Technical details

It is harmless memory resident multipartite virus. It hooks INT 13h, 21h and writes itself at the end of COM-files are executed or opened, and boot sectors of floppy disks are accessed. It contains the internal text string:

```
T42 Tea for two !
```

Virus.Boot-DOS.Telefonica.3429

Aliases

Virus.Boot-DOS.Telefonica.3429 (Kaspersky Lab) is also known as: Telefonica.3429 (Kaspersky Lab), Kampana.mp.b (McAfee), Kampana (Doctor Web), Span Tel-c (Sophos), Kampana.B (RAV), GENB* (Trend Micro), VGEN/1400.37 (H+BEDV), Kampana.B (FRISK), Anti-Telefonica 2 (ALWIL), Kampana (Grisoft), Kampana.B (SOFTWIN), Telefonica.3429 (ClamAV), Telefonica.H (Panda)

Description added Mar 07 2000

Behavior Virus

Technical details

These are very dangerous viruses. They hit .COM- and .EXE-files being started or opened (by standard way), MBR of hard disk while an infected file is started and Boot-sectors of floppies while DOS access to them. The viruses are encoded in an infected files. During installation the infectors traces INT 13h, 21h, 40h and hooks INT 21h. The viruses contain more than 10 handlers of INT 21h into their bodies. The viruses contain the texts like a:

```
"(C) 1990 Grupo HOLOKAUSTO (Barcelona, Spain) Kampaña Anti-TELEFONICA:
Mejor
servicio, Menores tarifas...";
"Virus Anti - C.T.N.E. (c)1990 Grupo Holokausto.
Kampanya Anti-Telefonica.
Menos tarifas y mas servicio.
Programmed in Barcelona (Spain).
23-8-90. - 666 -"
```

The part of viruses is wrote to MBR infects after only sectors and have no possibility to infect files. After 190hth booting from infected disk the infector erases the disk sectors and then type: "Campaña Anti-TELEFONICA (Barcelona)".

Virus.Boot-DOS.Tequila.5volt.2659

Aliases

Virus.Boot-DOS.Tequila.5volt.2659 (Kaspersky Lab) is also known as: Tequila.5volt.2659 (Kaspersky Lab), FiveVolts.2659 (McAfee), Bin.Auto.BCO (Symantec), Tequila.5volt (Doctor Web), Tequila 5volt (Sophos), Tequila.2659 (RAV), 5VOLT (Trend Micro), 5-Volt (H+BEDV), Tequila.2659 (FRISK), 5 (ALWIL), Mururoa (Grisoft), Tequila.2659 (SOFTWIN), Tequila.5Volt.2659 (Panda), 5Volt (Eset)

Description added Jun 16 2000

Behavior Virus

Technical details

It's a parasitic (not multipartite) variant of "Tequila" virus. It hooks INT 21h only and does not hit MBR of hard drive. It tries to install itself into UMB. This virus checks the file name and does not hit the files WIN*.*, CHKDSK*.*, BACK*.*. It contains the internal text:

> This is a beta version of the '-5 Volt' virus. A final and error free one will never follow because I've got enough of viruses. Now a message to the programmers of Turbo Anti Virus: You do a dangerous play with INT 21h in your TSAFE utility. It took me quite a long time to make the virus compatible with TSAFE. Please use clean programming technics in your next version. Today it's a Saturday and a big party with a lot of TEQUILA takes place! Wow!! Greetings to the U.S. Army in Iraq.

Virus.Boot-DOS.Tequila.a

Aliases

Virus.Boot-DOS.Tequila.a (Kaspersky Lab) is also known as: Tequila.a (Kaspersky Lab), Tequila.mp.2468a (McAfee), Tequila (Symantec), Tequila.2468 (Doctor Web), Tequila (Sophos), Tequila.2468.A (RAV), TEQUILA-1 (Trend Micro), Tequila (H+BEDV), Tequila.2468.G (FRISK), Tequila-2468 (ALWIL), Tequila (modified) (Grisoft), Tequila.2468.E (SOFTWIN), Tequila File (Panda)

Description added Mar 07 2000

Behavior Virus

Technical details

These are memory resident harmless stealth polymorphic multipartite viruses. They write themselves at the end of EXE files are executed or closed. These infectors hit MBR on execution of infected files, save the old MBR in the last sectors of C: drive and reduce its size in the Disk Partition Table. The viruses infect RAM on a reboot from the infected MBR only. They hook INT 13h, 1Ch, 21h. According to their internal counters the viruses display a colorful picture (Mandelbrot fractal set) and the message:

```
Execute: mov ax, FE03 / INT 21. Key to go on!
```

After executing this instruction the viruses display:

```
Welcome to T.TEQUILA's latest production.
Contact T.TEQUILA/P.o.Box 543/6312 St'hausen/Switzerland.
Loving thoughts to L.I.N.D.A
BEER and TEQUILA forever !
```

Virus.Boot-DOS.Terminator.3490

Aliases

Virus.Boot-DOS.Terminator.3490 (Kaspersky Lab) is also known as: Terminator.3490 (Kaspersky Lab), Term.mp (McAfee), Terminator.3490 (Doctor Web), Terminator-3490 (Sophos), AusTerm.3490 (RAV), BOOT.GENERIC* (Trend Micro), Italian-Generic (H+BEDV), AusTerm.3490 (FRISK), Ping-Pong (ALWIL), Ping-Pong (Grisoft), Italian-Generic (ClamAV)

Description added Mar 07 2000

Behavior Virus

Technical details

It's a dangerous memory resident multipartite encrypted virus. It hooks INT 21h and writes itself at the end of COM- (except COMMAND.COM) and EXE-files are accessed. Sometimes it fills the disk sectors by string "TERMINATED".

It tries to infect disk boot-sectors, but it contains error and fails. This virus contains the internal text strings:

```
THE TERMINATOR
TERMINATED
COMMAND.COM
Non-system disk or disk error
Replace and strike any key when ready
Disk boot failure
The TERMINATOR -- Boot virus version.
Released 15 May  5-15-91, 7.15 pm
.COM .EXE
The TERMINATOR -- Full virus version.
Released 15 May  5-15-91, 7.15 pm
```

Virus.Boot-DOS.Theta.527

Aliases

Virus.Boot-DOS.Theta.527 (Kaspersky Lab) is also known as: Theta.527 (Kaspersky Lab), Theta.mp (McAfee), Theta.527 (Symantec), Theta.527 (Doctor Web), Theta (Sophos), Theta.527 (RAV), THETA.527-O (Trend Micro), VGEN/957.3 (H+BEDV), Theta.527 (FRISK), Theta-527 (ALWIL), PS-MPC.0527.AF.Gen (SOFTWIN), Theta.527 (ClamAV), Theta.527 (Panda)

Description added Mar 07 2000

Behavior Virus

Technical details

These are harmless memory resident multipartite viruses. While executing an infected file the viruses infect the MBR of the hard drive. While loading from infected disk they hook INT 13h, intercept the first execution of an EXE file, hook INT 21h and then write themselves to the end of COM files that are executed. The viruses do not manifest themselves in any way.

Virus.Boot-DOS.Tiso.1279

Other versions: .846, .940

Aliases

Virus.Boot-DOS.Tiso.1279 (Kaspersky Lab) is also known as: Tiso.1279 (Kaspersky Lab), Tiso.mp (McAfee), Tiso.864 (Doctor Web), Tiso-940 (Sophos), Tiso.1279 (RAV), BOOT.GENERIC* (Trend Micro), BOO/Tiso (H+BEDV), Tiso.940 (FRISK), Tiso-940/1279 (ALWIL), Tiso.940 (Grisoft), Tiso.1279.B (ClamAV), Tiso.940.MBR (Panda)

Description added Jul 23 2000

Behavior Virus

Technical details

This is a harmless memory resident multipartite encrypted (in files) virus. It infects both COM and EXE files. On execution of infected file it hits MBR of hard drive. On loading from infected disk it hooks INT 08h, waits for DOS loading and then hooks INT 21h. It writes itself at the end of files that are executed.

This is a stealth virus on accessing to infected hard drive, it hooks INT 13h to use that function.

Sometimes this virus decrypts and displays:

```
Nech zije Jozef Tiso, prvy slovensky prezident !
```

Virus.Boot-DOS.Tiso.846

Other versions: .1279, .940

Aliases

Virus.Boot-DOS.Tiso.846 (Kaspersky Lab) is also known as: Tiso.846 (Kaspersky Lab), Tiso.mp.846b (McAfee), Tiso.846 (Symantec), Tiso.846 (Doctor Web), Tiso (Sophos), Tiso.846 (RAV), TISO.846 (Trend Micro), Tiso #2 (H+BEDV), Tiso.846 (FRISK), Tiso-846 (ALWIL), Tiso.846 (Grisoft), Tiso.846 (SOFTWIN), Tiso.2 (ClamAV), Tiso.846 (Panda)

Description added Mar 07 2000

Behavior Virus

Technical details

This is a harmless memory resident multipartite encrypted (in files) virus. The virus infects COM files only. On execution of infected file it hits MBR of hard drive. On loading from infected disk it hooks INT 08h, waits for DOS loading and then hooks INT 21h. It writes itself at the end of files that are executed.

Sometimes this virus decrypts and displays:

```
Nech zije Jozef Tiso, prvy slovensky prezident !
```

Virus.Boot-DOS.Tiso.940

Other versions: .1279, .846

Aliases

Virus.Boot-DOS.Tiso.940 (Kaspersky Lab) is also known as: Tiso.940 (Kaspersky Lab), Tiso.mp.940 (McAfee), Tiso.940 (Symantec), Tiso.846 (Doctor Web), Tiso-940 (Sophos), Tiso.940 (RAV), TISO.940 (Trend Micro), Tiso-940 (H+BEDV), Tiso.940 (FRISK), Tiso-940 (ALWIL), Tiso.940 (Grisoft), Tiso.940 (SOFTWIN), Univ (Panda)

Description added Jul 23 2000

Behavior Virus

Technical details

This is a harmless memory-resident multipartite encrypted (in files) virus. It infects COM files only. On execution of infected file it hits MBR of hard drive. On loading from infected disk it hooks INT 08h, waits for DOS loading and then hooks INT 21h. It writes itself at the end of files that are executed.

This virus is a stealth virus on accessing to infected hard drive, it hooks INT 13h to use that function.

Sometimes this virus decrypts and displays:

```
Nech zije Jozef Tiso, prvy slovensky prezident !
```

Virus.Boot-DOS.Ugly.4575

Aliases

Virus.Boot-DOS.Ugly.4575 (Kaspersky Lab) is also known as: Ugly.4575 (Kaspersky Lab), Noker.mp.4575.dam (McAfee), Junk/Noker-4575 (Sophos), UGLY.4575 (Trend Micro), VGEN/32459.512 (H+BEDV), NoKrenel-4575 (ALWIL)

Description added Mar 07 2000

Behavior Virus

Technical details

These are very dangerous memory resident polymorphic and stealth multipartite viruses. They infect COM and EXE files as well as the MBR of the hard drive and boot sectors of floppy disks. ("Ugly.6047,6048" fail to infect floppy disks). The viruses are encrypted in files and the MBR, they do not encrypt themselves in boot sector on floppy disks.

While infecting a file the viruses write themselves to the end of the file. While infecting a disk the viruses overwrite its first sector (boot or MBR), the original sector and virus code are saved on the last disk sectors. In case of floppy disk the virus formats an extra track.

When an infected file is executed or the system is loading from infected floppy disk, the virus infects the MBR of the hard drive and return control to the host program/boot sector. While writing data to the hard drive the virus uses direct calls to HD ports.

While loading from infected disk the virus allocates a block of system memory by decreasing the size of memory (the word at address 0000:0413), hooks INT 1Ch, waits for DOS loading process, hooks INT 8, 16h, 17h, 20h, 21h, 25h, 26h, 27h and completes its installation by restoring the size of system memory (the word at 0000:0413). As a result the virus leaves its TSR code in separated block of DOS memory. The virus then infects the files and floppy disks that are accessed. Depending on its counter (INT 8) the virus also searches for COM and EXE files in current directory and infects them.

They check the file names and do not infect the files: COMMAND.COM, GDI.EXE, DOSX.EXE, WIN386.EXE, KRNL286.EXE, KRNL386.EXE, USER.EXE, WSWAP.EXE, CHKDSK.EXE.

Depending on their internal counters and under a debugger the viruses erase the CMOS and the hard drive sectors.

The viruses use a complex algorithm allowing the virus to stay memory resident after cold reboot and loading from a clean DOS floppy disk. On installation the virus stores the CMOS memory that keeps the information about floppy drives and sets that info to zero (i.e. the virus emulates situation when no floppy drives are installed). On accessing to disks the virus temporary restores the CMOS and then erases these fields again. On any (cold or warm) reboot the system checks the CMOS, does not detect the floppy disks and passes the control to the MBR of hard drive. As a result the virus in the MBR receives the control, installs itself into the memory and then passes the control to the floppy disk loader. As a result the virus stays memory resident after loading from a clean write-protected disk.

Virus.Boot-DOS.Uranus.2048

Aliases

Virus.Boot-DOS.Uranus.2048 (Kaspersky Lab) is also known as: Uranus.2048 (Kaspersky Lab), Sailor-Uranus.mp.2048 (McAfee), Sailor.2048 (Doctor Web), Uranus-2048 (Sophos), Uranus.2048 (RAV), URANUS.2048-C (Trend Micro), BOO/URANUA (H+BEDV), Uranus.2048 (FRISK), Sailor-Uranus (ALWIL), Uranus.2048 (SOFTWIN), Uranus.2048 (ClamAV), Uranus.2048 (Panda)

Description added Mar 07 2000

Behavior Virus

Technical details

It is a harmless memory resident multipartite virus. It infects COM, EXE, NewEXE (NE) files and disk boot sectors. When an infected file is executed, the virus writes its code to the first hard drive track (unused sectors) and writes its loader to the boot sector of C: drive. The virus then returns to the host program.

When the system is loaded from infected disk, the virus hooks INT 13h, waits for DOS loading process, hooks INT 21h and writes itself to the end of COM, EXE and NewEXE (NE) files that are executed or accessed by FindFirst/Next ASCII DOS calls. When 1.4Mb floppy disks are accessed, the virus infects their boot sectors.

The virus checks the file names - it compares two last letters of file name with pairs of letters of the string:

```
ANOT86AVVPUSILEDOPNDLPGRPLRKYRRE
```

and does not infect these files (anti-viruses and utilities SCAN, F-PROT, KRNL386, NAV, AVP, FINDVIRUS, MSMAIL and so on).

The virus also contains the string:

```
Sailor_Uranus
```

Virus.Boot-DOS.USTC.7680

Aliases

Virus.Boot-DOS.USTC.7680 (Kaspersky Lab) is also known as: USTC.7680 (Kaspersky Lab), USTC.mp (McAfee), Virus.Dropper (Symantec), USTC.7680 (Doctor Web), USTC7680 (Sophos), Ustc.7680 (RAV), USTC.7680 (Trend Micro), BOO/USTC (H+BEDV), Ustc.7680 (FRISK), Ustc.7680 (SOFTWIN), Ustc.7680 (Panda)

Description added Mar 07 2000

Behavior Virus

Technical details

It is a very dangerous memory resident multipartite polymorphic virus. The virus infects the MBR of the hard drive and writes itself to the end of COM and EXE files. It is encrypted not only in files and MBR, but in the system memory also. Most of virus routines are encrypted, the virus decrypts them in case of need, executes and then encrypts.

While infecting the MBR the virus saves the original MBR sector to 16th sector on the first disk track and writes its main code from the MBR sector till 15th sector of first track. While infecting files the virus writes several blocks of junk code to the middle of file. It does it similar to "OneHalf" multipartite virus, but "USTC" virus' polymorphic engine is more complex. In that junk code the virus also uses anti-debugging tricks.

When an infected file is executed, the virus decrypts its code, infects the MBR if the hard drive, hooks INT 13h, 21h and stays memory resident. On loading from infected MBR the virus hooks INT 8, 13h, waits for some time (until DOS is installing itself) and then releases INT 8 and hooks INT 21h.

By hooking INT 13h the virus realizes its stealth routine that hides virus code on the first track. By hooking INT 21h the virus intercepts files that are copied or modified and infects them, i.e. the virus does infect new files or when file's data/code are changed. As a result the virus fools anti-virus CRC-checkers. The virus has a bug - it does not checks file name extension, but internal file format only, and infects not only COM and EXE but also data files.

Depending on its internal counter the virus pauses booting from infected MBR and waits for "CAPSL" input. The virus contains the text string:

```
3.0 1996.10 USTC
```

Virus.Boot-DOS.V.1253

Other versions: .TD.1536, .V.1526, .V.1536

Aliases

Virus.Boot-DOS.V.1253 (Kaspersky Lab) is also known as: V.1253 (Kaspersky Lab), Thanksgiving.mp (McAfee), Thanksgiving.1253 (Doctor Web), V-1 (Sophos), V1 (RAV), V.1253-B (Trend Micro), V-1 (A) (H+BEDV), Thanksgiving.1253 (FRISK), Thanksgiving-1253 (ALWIL), Thanksgiving.MBR (Grisoft), V-1.A (ClamAV), V1 (Panda)

Description added Mar 07 2000

Behavior Virus

Technical details

It is a memory resident very dangerous multipartite virus. It hooks INT 8, 13h, 21h and infects .COM files that are executed, boot sectors of the floppy disks and the MBR of the hard drive. It erases some sectors on the hard drive.

Virus.Boot-DOS.V.1526

Other versions: .TD.1536, .V.1253, .V.1536

Aliases

Virus.Boot-DOS.V.1526 (Kaspersky Lab) is also known as: V.1526 (Kaspersky Lab), Unapt.mp.1526 (McAfee), V.1526 (Symantec), Unapt.1526 (Doctor Web), 1526 (Sophos), _1526 (RAV), ZEALA_ET-C (Trend Micro), V-1526 (Boot) (H+BEDV), _1526 (FRISK), Unapt-1526 (ALWIL), BehavesLike:Dos.FileInfector (SOFTWIN), V.1526 (ClamAV), Denzuko.1526.A (Panda)

Description added Mar 07 2000

Behavior Virus

Technical details

It is a harmless memory resident multipartite virus. When an infected file is executed, it hooks INT 21h, infects the MBR of the hard drive and stays memory resident. When the system is loading from infected MBR, the virus hooks INT 1Ch, waits for DOS loading procedure and then hooks INT 21h.

When a .COM or .EXE file is executed, the virus writes itself to the end of the file. When the DOS command GetDiskSpace is executed, the virus searches for executable files and infects them.

The virus does not manifest itself in any way.

Virus.Boot-DOS.V.1536

Other versions: .TD.1536, .V.1253, .V.1526

Aliases

Virus.Boot-DOS.V.1536 (Kaspersky Lab) is also known as: V.1536 (Kaspersky Lab), Varna.mp (McAfee), V-1536 (Sophos), Varna (RAV), VARNA-B* (Trend Micro), BOO/VARNA (H+BEDV), Varna.1536 (FRISK), Varna-1536 (ALWIL), V.1536 (ClamAV), Varna.1536 (Panda)

Description added Mar 07 2000

Behavior Virus

Technical details

It is a dangerous memory resident multipartite virus. While executing an infected file the virus infects the MBR of the hard drive, as well as while loading from infected floppy disk.

While loading from infected disk (MBR, boot) the virus hooks INT 13h, waits for DOS loading, and hooks INT 21h. Then the virus writes itself to the end of EXE files that are opened, and to boot sectors of the floppy disks that are accessed. On 8th of any month the virus erases the hard drive sectors.

Virus.Boot-DOS.Vecna

Aliases

Virus.Boot-DOS.Vecna (Kaspersky Lab) is also known as: Vecna (Kaspersky Lab), Vecna.mp (McAfee), Vecna.512 (Doctor Web), Vecna (Sophos), Vecna.512 (RAV), VECNA.512-O (Trend Micro), Vecna (Boot) (H+BEDV), Vecna.512.A (FRISK), Vecna (ALWIL), Vecna (Grisoft), Vecna (ClamAV), Vecna (Panda)

Description added	Mar 07 2000
Behavior	Virus

Technical details

It is a very dangerous memory resident multipartite stealth virus. It writes itself to the MBR of the hard drive, to boot sectors of floppy disks and overwrites EXE files on floppy disks. While executing an infected EXE file the virus infects the MBR, decrypts and displays the message and then returns to DOS. The message is:

```
Out of memory.
```

While loading from infected disk (HD or floppy) the virus hooks INT 13h, stays memory resident and infects disks and files.

Under debugger and on Pentium computers the virus displays the message:

```
Vecna Live ...
```

The virus has quite a serious bug - it may continue INT 13h flow with wrong AX register. That may cause damage for disks, including disk formatting.

Vecna.313

It is not a dangerous memory resident stealth multipartite virus. It hooks INT 21h and writes itself to the end of COM files that are executed. The virus writes itself to the MBR sector when an infected COM file is started, it then returns control back to the host file. On loading from the MBR sector the virus hooks INT 13h that then hides virus code in the MBR sector and hooks INT 21h.

Vecna.Outsider

It is a very dangerous memory resident encrypted multipartite virus. It infects .EXE files and boot sector on floppy disks. EXE files get infection in "DirII" virus way. The virus hooks INT 13h, 28h.

In three month after infecting the computer, or under debugger the virus corrupts the CMOS (writes a password?) and displays the message:

```
[OUTSIDER]
Esta , minha vingan‡a contra esta sociedade injusta
E eu ainda n|o estou satisfeito
Espere e ver|o...
```

The virus also contains the text strings:

```
Written by Vecna/SGWW in Brazil 1997
```

Vecna.Tron

It is a harmless memory resident boot virus. It hooks INT 1, 8, 13h and writes itself to the MBR of the hard drive and boot sectors of floppy disks. The virus contains the text:

```
[ORGASMATRON] by Vecna/SGWW in Brazil 1997
```

To hook INT 13h the virus uses i386 debug registers DR0, DR6 and DR7. By using these registers it sets break point on BIOS INT 13h handler. When this handler takes control the processor generates INT 1, and control is passed to virus INT 1 handler. The virus disables debug break point, checks registers and calls its infection and stealth routines in case of need and then returns to original BIOS INT 13h handler. To reset break point and to keep INT 1 hook the virus uses INT 8 hook (timer).

Virus.Boot-DOS.VLAD.Hemlock.a

Aliases

Virus.Boot-DOS.VLAD.Hemlock.a (Kaspersky Lab) is also known as: VLAD.Hemlock.a (Kaspersky Lab), Hemlock.mp (McAfee), Hemlock-3168 (Sophos), Hemlock.3183 (RAV), Hemlock-2* (Trend Micro), Hemlock (H+BEDV), Hemlock.3168.unknown? (FRISK), VLAD-Hemlock-3168 (ALWIL), Hemlock (Grisoft), Hemlock.Boot (Panda)

Description added Mar 07 2000

Behavior Virus

Technical details

It's not dangerous memory resident polymorphic stealth multipartite virus. It hooks INT 9, 13h, 21h and writes itself at the end of COM-, EXE, and SYS-files are accessed. On execution of infected files it hits MBR of hard drive. On accessing to floppy disks it overwrites their boot sectors.

On Alt-Ctr-Del it emulates rebooting and stays memory resident. On execution of some programs it disables its stealth routine. It contains the internal text strings:

```
TBSCAN WIN CHKDSK PKZIP ARJ NDD SCANDISK LHA
co nm  /d:f
Hemlock by [qark/VLAD]
OSDATA
```

VLAD.MegaStealth

It's a not dangerous memory resident stealth multipartite virus. It hooks INT 13h, 21h, 76h and writes itself at the end of .COM-files, MBR of hard and floppy boot sectors are accessed. It displays '' character on each INT 21h calls. Interrupts 13h, 76h are used by stealth routine. It contains the internal test string:

```
[MegaStealth] by qark/VLAD
```

Virus.Boot-DOS.Yang.2528

Aliases

Virus.Boot-DOS.Yang.2528 (Kaspersky Lab) is also known as: Yang.2528 (Kaspersky Lab), Cancer.mp (McAfee), Cancer.2528 (Doctor Web), Yang (Sophos), Yang.2528 (RAV), BOOT.GENERIC* (Trend Micro), BOO/CANC (H+BEDV), Good_Doctor (FRISK), Good (ALWIL), Yang.2528.B (ClamAV), GoodDoctor.Boot (Panda)

Description added Mar 07 2000

Behavior Virus

Technical details

Yang.2528 is a dangerous memory resident multipartite virus. On execution of infected program it hits active boot sector of hard drive. Then (as well as on loading from infected disk) it hooks INT 8, 21h and writes itself at the end of COM- and EXE-files (except COMMAND.COM) are executed. In some cases it encrypts MBR of hard drive, slows down the computer, displays the messages:

```
Cancer -- Version 1.0  by  Mr. Yang  Sep/1990...
Hard disk has been demaged !!!
You can cure hard disk if you has a good Doctor !
I wish you luck !  Ha! Ha! Ha!
I am tired. Please give me a rest.
```

Virus.Boot-DOS.Yosha.440

Other versions: .512

Aliases

Virus.Boot-DOS.Yosha.440 (Kaspersky Lab) is also known as: Yosha.440 (Kaspersky Lab), Yosha.mp.440 (McAfee), Yosha.440 (Symantec), Yosha-440 (Sophos), Yosha.442 (RAV), YOSHA.440* (Trend Micro), Yosha-440 (H+BEDV), Yosha.440 (FRISK), Yosha-440 (ALWIL), Yosha (Grisoft), Yosha.440 (ClamAV), Yosha.440.MBR (Panda)

Description added Mar 07 2000

Behavior Virus

Technical details

It is a harmless memory resident multipartite virus. While executing an infected file the virus writes itself to the MBR of the hard drive and returns to the host program. While loading from infected MBR the virus hooks INT 13h, waits for DOS loading process, hooks INT 21h and then writes itself to the end of COM files that are executed. By hooking INT 13h the virus also realizes the stealth routine while accessing to the infected MBR. The virus contains the text string:

```
ELDOB1X by Yosha/DC
```

Virus.Boot-DOS.Yosha.512

Other versions: .440

Aliases

Virus.Boot-DOS.Yosha.512 (Kaspersky Lab) is also known as: Yosha.512 (Kaspersky Lab), Yosha.mp.cav.447 (McAfee), Yosha.512 (Symantec), Sly (Doctor Web), Yosha-512 (Sophos), Yosha.447 (RAV), YOSHA.512 (Trend Micro), Yosha (Boot) #2 (H+BEDV), Yosha.447 (FRISK), Parvir-512 (ALWIL), Yosha.512 (ClamAV), Suspect File (Panda), TSR.EXE.BOOT (Eset)

Description added Aug 04 2000

Behavior Virus

Technical details

It is a very dangerous stealth virus that infects EXE files and the MBR of the hard drive. When an infected EXE file is executed, the virus infects the MBR and reboots the computer. While loading from infected MBR the virus cuts a block of the system memory by decreasing RamSize word at the address 0000:0413, hooks INT 13h and then writes itself to the beginning of EXE files that are accessed.

While infecting a file the virus saves the original EXE header to the random selected sector on the disk and stores that address in the EXE header. While accessing to an infected EXE file the virus gets the address of the sector that keeps the original EXE header and reads it from the disk to the read/write buffer. This routine realizes the complete stealth algorithm, but the disk sectors at the random selected addresses may be corrupted by the virus.

Virus.Boot-DOS.Yosha.Novacane.271.a

Aliases

Virus.Boot-DOS.Yosha.Novacane.271.a (Kaspersky Lab) is also known as:
Yosha.Novacane.271.a (Kaspersky Lab), Yosha.mp (McAfee), Yosha.Novacane.271 (Symantec), BootExe.Yosha.271 (Doctor Web), Yosha-271 (Sophos), Yosha.271 (RAV), YOSHA.271-B* (Trend Micro), BOO/YOSHA271 (H+BEDV), Yosha.271 (FRISK), Yosha-NovaCane-271 (ALWIL), Yosha (Grisoft), Yosha.Novacane.271.A (ClamAV), Muzik (Panda)

Description added Aug 04 2000

Behavior Virus

Technical details

It is a harmless stealth virus that infects EXE files and the MBR of the hard drive. When an infected EXE file is executed, the virus infects the MBR and reboots the computer. While loading from infected MBR the virus cuts a block of the system memory by decreasing RamSize word at the address 0000:0413, hooks INT 13h and then writes itself into the header of EXE files that are accessed. The virus contains the string:

```
NovaCane by Yosha/DC
```

Virus.Boot-DOS.ZhengZhou.3576.a

Other versions: .3576.b, .3584.a, .3584.b, .3584.c

Aliases

Virus.Boot-DOS.ZhengZhou.3576.a (Kaspersky Lab) is also known as: ZhengZhou.3576.a (Kaspersky Lab), ZhengZhou.mp (McAfee), ZhengZhou.3576 (Doctor Web), ZhengZhou-3576 (Sophos), ZhengZhou.3571 (RAV), ZHENGZHOU.B-B (Trend Micro), ZHE (Boot) (H+BEDV), ZhengZhou.3571.A (FRISK), ZhengZhou-3576-A (ALWIL), Musicbug (Grisoft), ZhengZhou.3576.A (ClamAV), ZhengZhou.3584.Boot (Panda)

Description added Mar 07 2000

Behavior Virus

Technical details

This is a dangerous memory resident multipartite DOS virus.

ZhengZhou hooks INT 13h, 21h and first writes itself to the end of COM and EXE files that are executed, and to the MBR of the hard drive when infected files are executed. It then infects the boot sector of the floppy drive. Under a debugger ZhengZhou will also reboot the computer.

ZhenZhou may also infect files that are accessed by FindFirst/Next FCB function (DIR command). It may also erase hard drive sectors.

Virus.Boot-DOS.ZhengZhou.3576.b

Other versions: .3576.a, .3584.a, .3584.b, .3584.c

Aliases

Virus.Boot-DOS.ZhengZhou.3576.b (Kaspersky Lab) is also known as: ZhengZhou.3576.b (Kaspersky Lab), ZhengZhou.mp.3576b (McAfee), Chang.3576 (Symantec), ZhengZhou-3576b (Sophos), ZhengZhou.3571.B (RAV), ZHENGZHO.3571B (Trend Micro), Zheng (H+BEDV), ZhengZhou.3571.B (FRISK), ZhengZhou-3576-B (ALWIL), Musicbug (Grisoft), ZhengZhou.3571.B (SOFTWIN), ZhengZhou.3576.B (ClamAV), Zhengzhou.3571.B (Panda)

Description added Mar 07 2000

Behavior Virus

Technical details

This is a dangerous encrypted memory resident multipartite DOS virus.

ZhengZhou hooks INT 13h, 21h and first writes itself to the end of COM and EXE files that are executed, and to the MBR of the hard drive when infected files are executed. It then infects the boot sector of the floppy drive. Under a debugger ZhengZhou will also reboot the computer.

ZhenZhou may also infect files that are accessed by FindFirst/Next FCB function (DIR command). It may also erase hard drive sectors.

Virus.Boot-DOS.ZhengZhou.3584.a

Other versions: .3576.a, .3576.b, .3584.b, .3584.c

Aliases

Virus.Boot-DOS.ZhengZhou.3584.a (Kaspersky Lab) is also known as: ZhengZhou.3584.a (Kaspersky Lab), ZhengZhou.mp (McAfee), ZhengZhou.3584 (Doctor Web), ZhengZhou-3584 (Sophos), ZhengZhou.3584.A (RAV), ZHENGZHOU.D-B (Trend Micro), Chang #1 (Boot) (H+BEDV), ZhengZhou.3584.B (FRISK), ZhengZhou-3584-B (ALWIL), Musicbug (Grisoft), ZhengZhou.3584.A (ClamAV), Zhengzhou.3584.BOO (Panda)

Description added Mar 07 2000

Behavior Virus

Technical details

This is a dangerous memory resident multipartite DOS virus.

ZhengZhou.3584.a hooks INT 13h, 21h and first writes itself to the end of COM and EXE files that are executed, and to the MBR of the hard drive when infected files are executed. It then infects the boot sector of the floppy drive.

ZhenZhou.3584.a may also infect files that are accessed by FindFirst/Next FCB function (DIR command). It may also erase hard drive sectors.

ZhenZhou.3584.a contains the following text strings:

```
Zheng Zhou, China. 1993

Thank for your helping, Good-bye !
```

Under a debugger ZhengZhou.3584.a tries to format the hard disk (but fails), and displays the messages:

```
Do not turn OFF the computer when WOLF is working !
Insert DOS diskette in drive A:
Strike any key when ready ...
```

Virus.Boot-DOS.ZhengZhou.3584.b

Other versions: .3576.a, .3576.b, .3584.a, .3584.c

Aliases

Virus.Boot-DOS.ZhengZhou.3584.b (Kaspersky Lab) is also known as: ZhengZhou.3584.b (Kaspersky Lab), ZhengZhou.mp.3584b (McAfee), Chang.3576 (Symantec), ZhengZhou-3584b (Sophos), ZhengZhou.3584.B (RAV), V0214-E (Trend Micro), Avalanche #4 (H+BEDV), ZhengZhou.3584.B (FRISK), ZhengZhou-3584-B (ALWIL), Musicbug (Grisoft), ZhengZhou.3584.B (SOFTWIN), ZhengZhou.3584.B (ClamAV), Zhengzhou.3584.B (Panda)

Description added Mar 07 2000

Behavior Virus

Technical details

This is a dangerous memory resident multipartite DOS virus.

ZhengZhou.3584.b hooks INT 13h, 21h and first writes itself to the end of COM and EXE files that are executed, and to the MBR of the hard drive when infected files are executed. It then infects the boot sector of the floppy drive.

ZhenZhou.3584.b may also infect files that are accessed by FindFirst/Next FCB function (DIR command). It may also erase hard drive sectors.

ZhengZhou.3584.b does not infect the SCAN.EXE and CLEAN.EXE files, and deletes the WMSET.COM file.

ZhenZhou.3584.b contains the following text string:

```
wolf
```

Virus.Boot-DOS.ZhengZhou.3584.c

Other versions: .3576.a, .3576.b, .3584.a, .3584.b

Aliases

Virus.Boot-DOS.ZhengZhou.3584.c (Kaspersky Lab) is also known as: ZhengZhou.3584.c (Kaspersky Lab), ZhengZhou.mp.3584c (McAfee), Chang.3576 (Symantec), ZHENGZHOU.3584.C (Trend Micro), ZhengZhou-3584-A (ALWIL), ZhengZhou.3584.C (SOFTWIN), ZhengZhou.3584.A (Panda)

Description added Mar 07 2000

Behavior Virus

Technical details

This is a dangerous memory resident multipartite DOS virus.

ZhengZhou.3584.c hooks INT 13h, 21h and first writes itself to the end of COM and EXE files that are executed, and to the MBR of the hard drive when infected files are executed. It then infects the boot sector of the floppy drive. Under a debugger it may reboot the computer.

ZhenZhou.3584.c may also infect files that are accessed by FindFirst/Next FCB function (DIR command). It may also erase hard drive sectors.

BWME.Gangi.1130

Description added	Jun 15 2000
Behavior	Virus
Technical details	

It is a dangerous memory resident parasitic virus. It hooks INT 21h and writes itself to the end of EXE files that are executed. The virus has a bug and can halt the system. It was created with Biological Warfare Mutation Engine - it is a polymorphic engine, like the MtE and TPE engines.

This virus writes itself to the end of the files. It contains the text strings:

```
[BWME]
[NCSA] Gangi is a dweeb
```

BWME.GSD.1145

Description added Jun 15 2000
Behavior Virus
Technical details

It is a harmless memory resident virus. It hooks INT 21h and infects EXE files that are executed or opened. It was created with Biological Warfare Mutation Engine - it is a polymorphic engine, like the MtE and TPE engines.

This virus writes itself to the end of the files. It contains the text strings:

```
[BWME]
[BW] Glycogen Storage Disease
```

BWME.Test.1287

Description added	Mar 07 2000
Behavior	Virus
Technical details	

It is a harmless memory resident virus. It hooks INT 21h and infects COM and EXE files that are executed or opened. It was created with Biological Warfare Mutation Engine - it is a polymorphic engine, like the MtE and TPE engines.

This virus writes itself to the end of the files. It contains the text strings:

```
[BWME]
[BW] Test virus #1
```

BWME.Twelve.1378

Description added	Jun 15 2000
Behavior	Virus
Technical details	

It is a harmless nonmemory resident parasitic virus. It searches for COM and EXE files and infects them. It was created with Biological Warfare Mutation Engine - it is a polymorphic engine, like the MtE and TPE engines.

This virus writes itself to the end of the files. It contains the text strings:

```
[BWME]
[BW] Twelve Toes Virus
```

Devices.2000

Description added	Mar 07 2000
Behavior	Virus
Technical details	

It is a harmless memory resident parasitic polymorphic virus. It writes itself to beginning of SYS and to the end of EXE files. While executing an infected EXE file the virus opens the C:\CONFIG.SYS file, scans it for the names of device drivers, infects them and returns to the host program. While infecting a SYS file the virus creates the temporary file DEVICES.$$$, writes its code to that file, appends the code of the SYS file, then deletes the SYS file and renames DEVICES.$$$ to the original name of infected SYS file.

While loading an infected SYS file the virus installs itself into the system memory as device driver, hooks INT 1Ch, waits for some time, then hooks INT 21h and while accessing to floppy disks searches and infects EXE files.

The virus contains the text strings:

```
XMSXXXX0
:\devices.$$$ \ config.sys *.exe
```

Happy_II.506

Description added	Mar 07 2000
Behavior	Virus
Technical details	

It is a harmless nonmemory resident parasitic virus. It searches for COM files (except COMMAND.COM), then writes itself to the end of the file. The virus does not manifests itself in any way, it contains the text strings:

```
*.com COMMAND.
HAPPY v1.03 (C) PROFESSOR,KPI
```

Joke.1068

Description added Mar 07 2000
Behavior Virus
Technical details

This is not a dangerous nonmemory resident parasitic virus. It searches for .COM files (except COMMAND.COM) of current directory and writes itself to the end of the file. Sometimes it display:

```
At last ...... ALIVE !!!!!
I guess your computer is infected by the Big Joke Virus.
Release 4/4-91
Lucky you, this is the kind version.
Be more careful while duplicating in the future.
The Big Joke Virus, killer version, will strike harder.
The Big Joke rules forever
```

Kot.b

Aliases

Kot.b (Kaspersky Lab) is also known as: Kot (McAfee), Kot (Doctor Web), Kot-B (Sophos), Kot.B (RAV), BOOT.GENERIC* (Trend Micro), DOS/Kot.B (H+BEDV), Kot_II.B (FRISK), Kot-B (ALWIL), Kot-II.B (Panda)

Description added	Jun 10 2000
Behavior	Virus
Technical details	

This is a dangerous memory resident boot virus. It hooks INT 13h, and writes itself to the BOOT sectors of floppy disks and to the MBR sector of the hard drive. On the 15th day of each month, the virus stops booting in a computer. The virus contains the text string:

```
Kot
```

Lemena.3544

Description added Mar 07 2000
Behavior Virus
Technical details

It is not a dangerous memory resident parasitic polymorphic virus. It copies itself to the video memory at address BC00:0000, hooks INT 22h (Terminate call), returns control to host program, waits for termination and hooks INT 21h. To hook INT 21h the virus patches the DOS kernel. The virus then writes itself to the end of COM and EXE files that are executed, opened or accessed by Get/Set File Attributes DOS call.

To hide itself in the system memory the virus uses a quite complex way. When any program is executed, the virus allocates a block of XMS memory, moves its code to there, then copies its INT 22h handler to DOS kernel (the virus looks for a cave in there). The virus then releases INT 21h, hooks INT 22h, erases its TSR copy in the video memory and releases control. As a result, when any program (including anti-viruses) are active, there are no virus code in the DOS memory. The main part of virus code (encrypted) is placed in the XMS memory, and INT 22h handler is "waiting" for the Terminate call to restore "status quo" (move virus code from XMS to the video memory and to re-hook INT 21h).

The virus also uses anti-debugging tricks as well as on-the-fly encryption: the virus decrypts its subroutines before calling them, and encrypts after return from subroutine.

The virus does not infect anti-virus programs -V.EXE, ADINF, AIDSTEST, AVP, CPAV, and so on according to the string (two letters per name):

```
-VADAIAVCPDRF-FIGUIMIVMSNAPCSCSPSSSVTBTOV-VAVSWE
```

The virus deletes the anti-virus databases: ANTI-VIR.DAT, AVP.CRC, CHKLIST.CPS, CHKLIST.MS, CHKLIST.TAV, CRC.SVS, FILES.VVL FINGERP.VVF IM.PRM IVB.INI, IVB.NTZ, MSAV.CHK, SMARTCHK.CPS, \AV.CRC, \BOOT.CPS, \BOOT.MS, \BOOT.NTZ, \BOOT.TAV, \IV.INI, \PART.NTZ

According to its random counter the virus displays the texts:

```
LEMENA'97
BOKEPH'97
```

The virus also contains the text strings:

```
TBDRVXXX
[LEMENA'97] by Bokeph from Batavia, Indonesia
[MENA]
```

MidInfector.765

Description added	Jul 15 2000
Behavior	Virus
Technical details	

This is a harmless memory resident parasitic virus. It hooks INT 21h and writes itself to the end of COM files that are executed.

The virus contains the text string:

```
MidInfector by Dark Slayer of [TPVO]
```

The virus writes "JMP VirusCode" instruction to the file middle. While infecting the virus reads the file into the system memory, and disassembles the file code instruction-by-instruction (the virus contains primitive disassembler). The disassembler stops at interrupt calls (CD), jumps on condition (Jcc), FAR JMP/CALL, and some other instructions, and the virus overwrites that instruction with "JMP VirusCode".

Natas.4744

Aliases

Natas.4744 (Kaspersky Lab) is also known as: Natas.mp (McAfee), Natas-b (Sophos), Natas (RAV), Natas-7* (Trend Micro), Natas.4774 (H+BEDV), Natas (FRISK), Natas-4744 (ALWIL), Natas (Grisoft), Natas.A (SOFTWIN), VGEN.47937 (ClamAV), 4744.MBR (Panda)

Description added Jul 15 2000

Behavior Virus

Technical details

This is a dangerous memory resident multipartite polymorphic virus. It hooks INT 13h, 21h and writes itself into MBR of hard drive, boot sectors of floppy disks and at the end of COM and EXE files that are accessed. It does not infect the files that are opened by PKZIP/PKUNZIP, LHA and ARJ archivators. Depending on its internal counters the virus formats disk sectors. It contains the internal text strings:

```
BACK MODEM

Natas
```

Pcvrs.1904

Description added	Mar 07 2000
Behavior	Virus
Technical details	

This is a very dangerous memory-resident parasitic virus. It hooks INT 21h and 16h (keyboard), and writes itself to the beginning of .COM (except COMMAND.COM) and to the end of .EXE files that are executed or opened.

Some time after activation, the virus starts to delete files that are opened. On Monday 23, the virus formats the hard disk and displays:

```
PcVrsDs Version 1.00 Copyright (C) VirOP 1990.
```

and changes every 13th key that is pressed. The virus also contains the ID-string:

```
PcDos
```

Poss.2110

Description added	Mar 07 2000
Behavior	Virus
Technical details	

There are memory resident dangerous parasitic viruses. They hook INT 8, 21h and write themselves to the end of COM and EXE files (except COMMAND.COM). Sometimes they delete the files. They manifest themselves by the face picture which is drawn on the screen. They also contain the text strings:

```
COMMAND.COM
POSSESSED! Bwa! ha! ha! ha! ha!
Author: JonJon Gumba of AdU
:*.COM :*.EXE
```

Search.437

Description added	Jul 13 2000
Behavior	Virus
Technical details	

This is nonmemory resident parasitic virus. It searches for COM files and writes itself to the end of the file.

On Friday, 13th the virus erases the the C: drive.

Seneca.392

Description added	Mar 07 2000
Behavior	Virus
Technical details	

It is a very dangerous nonmemory resident parasitic virus. Being executed it searches for .EXE files and overwrites them. On November, 25th it displays:

```
HEY EVERYONE!!!
Its Seneca's B-Day!  Let's Party!
```

and erases the sectors of the current drive. Sometimes it also displays:

```
You shouldn't use your computer so much,
its bad for you and your computer.
```

and erases the sectors.

Slovakia.II.3584.b

Description added	Jul 14 2000
Behavior	Virus
Technical details	

This is a harmless memory resident parasitic polymorphic virus. It hooks INT 21h and writes itself to the end of COM and EXE files that are executed. It contains the text strings:

```
I'am SLOVAKIA virus Version 1.1 Copyright (c) 29.1.1994 SVL
chklist.ms chklist.cps smartchk.cps
svl.svl
scan avg vir asta alik rex msav cpav nod clean f-pro tbav tbuti avast nav
vshie dizz vsafe
```

It displays the first (and second) strings, deletes the files from third (second) string. The fourth (third) string contains the file name which is used on infection (the virus renames the file into that name on infection and then renames back). The next string contains the file names which are not infected by this virus.

Slow.1716

Description added	Mar 07 2000
Behavior	Virus
Technical details	

This is a relatively harmless memory resident encrypted virus. It hooks INT 21h, and infects COM and EXE files that are executed. On Friday, it sets the date stamp to zero for files that are closed.

Stoned.a

Aliases

Stoned.a (Kaspersky Lab) is also known as: Tiebud (McAfee), Boot.Stoned.family (Symantec), NewZealand-2 (Sophos), Stoned (RAV), Stoned-B* (Trend Micro), Stoned #2 (H+BEDV), Stoned.A (FRISK), Stoned (ALWIL), Stoned.Standard.Dropper (Grisoft), Trojan.Dropper.Boot.Stoned.AE (SOFTWIN), Stoned.2 (ClamAV), Stoned.NOP (Panda)

Description added Mar 07 2000

Behavior Virus

Technical details

"Stoned" family. At midnight, this virus displays the following message:

```
IT'S MID NIGH
```

Stoned.Military

In November, this virus tries to format hard drive sectors.

Stoned.Million

This virus does not save the original floppy Boot sector and types "Non-System disk" while booting from an infected floppy. It overwrites the OEM message of the floppy Boot sector with the string "1000000".

Stoned.Near.a,b

These are stealth viruses. With the probability of 1/16 they will erase the MBR and displays the text:

```
Near Dark
```

Stoned.Nichols

Sometimes this virus displays:

```
[Nichols] by Apache
```

Stoned.Nov7

In October, this virus types a face symbol (01h ASCII) while booting, and on November 7, it erases the MBR.

Stoned.PC-AT

This is an encrypted virus containing the non-encrypted text string:

```
 PC AT
  = "heart" symbol
```

Stoned.Rostov

While booting from an infected floppy disk, this virus has the probability of 1/32 of eraseing eight sectors on the hard disk.

Stoned.Satria

Stoned family. It displays a picture.

Stoned.Scale

"Stoned" family. It saves the Boot sector of floppies and the MBR hard drive at the address 0/0/9 (track/cylinder/sector). Sometimes it plays a tune (scale).

Stoned.Scrlock

These viruses disable writing to the hard drive if the ScrollLock key is pressed.

Stoned.Scroll

It scrolls the screen if NumLock is pressed and ScrollLock is released.

Stoned.Sex.a,b

These viruses infect disks while accessing them (INT 13h, AH=2,3). They save the original sectors (boot and MBR sectors) at the addressed 1/0/3 (head/track/sector) for a floppy disk and 0/0/8 (or 0/0/7 according to its version) for the hard disk. While loading from an infected floppy disk, the viruses, with the probability of 1/8, display the messages:

```
"Stoned.Sex.a":  EXPORT OF SEX REVOLUTION ver. 1.1
"Stoned.Sex.b":  EXPORT OF SEX REVOLUTION ver. 2.0
```

Stoned.Spook

While infecting the hard drive, this virus writes 8 sectors to 1--9 sectors of the hard drive, and as a result, it can erase the system information. It contains a texts:

```
Spook 1.0
LIM
```

Stoned.Swedish

This virus displays the message "The Swedish Disaster".

Stoned.Torm

While booting from an infected disk, this virus, with the probability of 1/8, displays:

```
Repent for ye shall be tormented...
Tormentor B - RABID Int'nl Dev. Corp. '91
```

Stoned.TurboManiac

On October 19, it displays:

```
The Turbo Maniac was here..
```

Stoned.WXYC

It infects boot sectors of the floppy disks and first boot sector (not MBR) of the hard drive. It contains the

strings:

```
JAM WXYC
WXYC rules this roost!
```

Sometimes it displays the latter string.

Stoned.YMP

On the 1st of every month, it displays the message "HAVE A NICE DAY (c)YMP".

Stoned.Zappa

On December 4, it erases the disk sectors and displays:

```
Dedicated to ZAPPA...
```

Stoned.Zapped

This virus erases the disk sectors and displays the message:

```
ZAPPED YOU!
```

Tucuman.1408

Description added	Mar 07 2000
Behavior	Virus
Technical details	

This is a dangerous memory resident parasitic virus. It hooks INT 21h and writes itself to the end of EXE files that are executed or opened.

In some cases the virus corrupts files while infecting them. On June 10th, October 28th and November 21st it also hooks INT 1Ch and tries to run a video effect, but halts the computer.

The virus contains the text strings:

```
El procesador se quema!!! Inserte 586 cm3 de agua por el drive
A
[Wild Boy] UTN-FRT Tucumán, Argentina by Mr. Bithead - 1995
```

Network Worms

Today everyone has heard of computer worms.

Worms can be classified according to the propagation method they use, i.e. how they deliver copies of themselves to new victim machines. Worms can also be classified by installation method, launch method and finally according to characteristics standard to all malware: polymorphism, stealth etc.

Many of the worms which managed to cause significant outbreaks use more then one propagation method as well as more than one infection technique. The methods are listed separately below.

Email worms

Email worms spread via infected email messages. The worm may be in the form of an attachment or the email may contain a link to an infected website. However, in both cases email is the vehicle.

In the first case the worm will be activated when the user clicks on the attachment.In the second case the worm will be activated when the user clicks on the link leading to the infected site.

Email worms normally use one of the following methods to spread:

- Direct connection to SMTP servers using a SMTP API library coded into the worm
- MS Outlook services
- Windows MAPI functions

Email worms harvest email addresses from victim machines in order to spread further. Worms use one or more of the following techniques:

- Scanning the local MS Outlook address book
- Scanning the WAB address database
- Scanning files with appropriate extensions for email address-like text strings
- Sending copies of itself to all mail in the user's mailbox (worms may even 'answer' unopened items in the inbox)

While these techniques are the most common, some worms even construct new sender addresses based lists of possible names combined with common domain names.

Instant Messaging (ICQ and MSN) Worms

These worms have a single propagation method. They spread using instant messaging applications by sending links to infected websites to everyone on the local contact list. The only difference between these worms and email worms which send links is the media chosen to send the links.

Internet Worms

Virus writers use other techniques to distribute computer worms, including:

- Copying the worm to networked resources
- Exploiting operating system vulnerabilities to penetrate computers and/or networks
- Penetrating public networks
- Piggy-backing: using other malware to act as a carrier for the worm.

In the first case, the worms locate remote machines and copy themselves into folders which are open for read and write functions. These network worms scan all available network resources using local operating system services and/or scan the Internet for vulnerable machines. They will then attempt to connect to these machines and gain full access to them.

In the second case, the worms scan the Internet for machines that have not been patched, i.e. have operating systems with critical vulnerabilities

still open to exploitation. The worm sends data packets or requests which install either the entire body of the worm or a section of the worm's source code containing downloader functionality. If this code is successfully installed the main worm body is then downloaded. In either case, once the worm is installed it will execute its code and the cycle continues.

Worms that use Web and FTP servers fall into a separate category. Infection is a two-stage process. These worms first penetrate service files on the file server, such as static web pages. Then the worms wait for clients to access the infected files and attack individual machines. These victim machines are then used as launch pads for further attacks.

Some virus writers use worms or Trojans to spread new worms. These writers first identify Trojans or worms that have successfully installed backdoors on victim machines. In most cases this functionality allows the master to send commands to the victim machine: such zombies which have backdoors installed can be commanded to download and execute files - in this case copies of the new worm.

Many worms use two or more propagation methods in combination, in order to more efficiently penetrate potential victim machines.

IRC Worms

These worms target chat channels, although to day IRC worms have been detected. IRC worms also use the propagation methods listed above - sending links to infected websites or infected files to contacts harvested from the infected user. Sending infected files is less effective as the recipient needs to confirm receipt, save the file and open it before the worm is able to penetrate the victim machine.

File-sharing Networks or P2P Worms

P2P worms copy themselves into a shared folder, usually located on the local machine. Once the worm has successfully placed a copy of itself under a harmless name in a shared folder, the P2P network takes over: the network informs other users about the new resource and provides the infrastructure to download and execute the infected file.

More complex P2P worms imitate the network protocol of specific file-sharing networks: they respond affirmatively to all requests and offer infected files containing the worm body to all comers.

Email-Worm.Win32.Eyeveg.b

Other versions: .f, .g

Aliases

Email-Worm.Win32.Eyeveg.b (Kaspersky Lab) is also known as: Worm.Win32.Eyeveg.b (Kaspersky Lab), Uploader-H (McAfee), W32.Lorac (Symantec), Win32.HLLW.Eyeveg (Doctor Web), Troj/Mimail-E (Sophos), Win32/HLLW.Eyeveg.A (RAV), WORM_LORAC.A (Trend Micro), Worm/Eyeveg.B (H+BEDV), W32/Eyeveg.C (FRISK), Win32:Trojan-gen. (ALWIL), Worm/Lorac.B (Grisoft), Win32.Eyeveg.B@mm (SOFTWIN), Worm Generic (Panda), Win32/Eyeveg.C (Eset)

Description added	May 23 2005
Behavior	Internet Worm

Technical details

This worm is written in Visual C++ and packed using UPX. The file is 41480 bytes in size.

Installation

The worm copies itself to the system directory under a random name which consists of six characters. It then registers this file in the system registry:

```
[HKLM/Software/Microsoft/Windows/CurrentVersion/Run]
```

This process will not be visible on Win9x systems.

Payload

It will act as a key logger, collecting details of shared folders, passwords which have been saved in Internet Explorer, email passwords and other confidential data. It then uses http POST to send this information to www.melan******oll.biz/u2.php.

Propagation via networks

The worm is also able to copy itself to open shared files.

Email-Worm.Win32.Eyeveg.f

Other versions: .b, .g

Aliases

Email-Worm.Win32.Eyeveg.f (Kaspersky Lab) is also known as: Worm.Win32.Eyeveg.f (Kaspersky Lab), W32/Eyeveg.worm.gen (McAfee), W32.Lanieca.A@mm (Symantec), Win32.HLLW.Eyeveg.2 (Doctor Web), W32/Wurmark-J (Sophos), Worm:Win32/Eyeveg.E (RAV), WORM_WURMARK.J (Trend Micro), Worm/Cipie (H+BEDV), W32/Eyeveg.H@mm (FRISK), PSW.Agent.5.V (Grisoft), Trojan.Spy.Agent.AJ (SOFTWIN), Trojan.W32.PWS.Prostor.A (ClamAV), W32/Eyeveg.F.worm (Panda), Win32/Eyeveg.I (Eset)

Detection added	May 09 2005 08:21 GMT
Description added	May 23 2005
Behavior	Internet Worm

Technical details

This worm is written in Visual C++ and is made up of two files, an executable file (EXE) and a dynamic link library (DLL), which is found within the EXE file. The EXE file is packed using UPX, and it is 80384 bytes in size. The DLL file is 77824 bytes in size.

Installation

The worm copies itself to the system directory under a random name composed of 6 letters. THe DLL file will be saved to the same place. On Win9x systems, this process will be hidden.

Payload

The worm will deactivate the Windows XP internal firewall.

It will act as a key logger, collecting details of shared folders, passwords which have been saved in Internet Explorer, email passwords and other confidential data. It then uses http POST to send this information to www.melan******oll.biz/n.php.

Propagation via email

The worm sends itself to email addresses harvested from files with extensions such as html, eml, sht, asp, mbx.

Attachment names:

```
love.jpg                    ...scr
resume.doc                    ...scr
details.doc                   ...scr
news.doc                    ...scr
image.jpg                    ...scr
message.txt                   ...scr
pic.jpg                   ...scr
girls.jpg                    ...scr
photo.jpg                    ...scr
video.avi                    ...scr
music.mp3                    ...scr
song.wav                    ...scr
screensaver                   ...scr
```

The attachment may also arrive as a ZIP file, using the names shown above.

Propagation via networks

The worm also copies itself to open shared folders.

Email-Worm.Win32.Eyeveg.g

Other versions: .b, .f

Aliases

Email-Worm.Win32.Eyeveg.g (Kaspersky Lab) is also known as: Worm.Win32.Eyeveg.g (Kaspersky Lab), W32/Eyeveg.worm.k (McAfee), W32.Lanieca.B@mm (Symantec), Win32.HLLW.Eyeveg.3 (Doctor Web), W32/Bugbear-B (Sophos), WORM_WURMARK.J (Trend Micro), Worm/Eyeveg.g (H+BEDV), W32/Eyeveg.J (FRISK), Worm/Eyeveg.H (Grisoft), Win32.Wurmark.K@mm (SOFTWIN), Trojan.W32.PWS.Prostor.A (ClamAV), W32/Eyeveg.D.worm (Panda), Win32/Eyeveg.K (Eset)

Detection added	May 23 2005
Description added	May 23 2005
Behavior	Internet Worm

Technical details

This worm spreads via the Internet as an attachment to infected emails. It also spreads via open network resources. It sends itself to email addresses harvested from the infected computer.

It is written in Visual C++ and packed using UPX. The program has two files: an executable (EXE) file and a dynamic link library (DLL) which is saved within the exe file.

In terms of functionality, Eyeveg.g is identical to the previous version, Eyeveg.f

This latest version differs only in the size of the executable file - 78336 bytes -and the version of the packing program used.

IRC-Worm.BAT.Spth

Aliases

IRC-Worm.BAT.Spth (Kaspersky Lab) is also known as: IRC-Worm.Spth (Kaspersky Lab), MIRC/Generic (McAfee), IRC/Generic* (RAV), mIRC/Gen (Panda)

Description added	Dec 04 2002
Behavior	IRC Worm

Technical details

This is a polymorpic worm is written in Batch script with the extensions Windows 2000/XP (cmd.exe). The worm contains two parts: polymorphic generator and main body. The polymorphic generator reconstruces the main body on each start of batch file. The worm creates its droppers with the files: SPTH.BAT and C:\MIRC\SATURN.BAT. It also creates the script file C:\MIRC\SCRIPT.INI. The script sends worm dropper (SATURN.BAT) to each user who joins the infected channel. The worm also rewrites batch files into WINDOWS directory. The worm contains the comments:

```
------------ BatXP.Saturn ********** by Second Part To Hell ------------
                                                                        |
I think, you are looking at the code and think: "What the hell is this?"|
The answer is: A Windows XP Batch polymorph virus :D                     |
WinXP is using a program named CMD.EXE instate of COMMAND.COM for DOS    |
You're able to make the really nice things with CMD which you wasn't     |
able to do it with COMMAND.COM.                                          |
                                                                        |
Information about the virus:                                            |
Virusname.....................: BatXP.Saturn                             |
Virusauthor...................: Second Part To Hell                       |
Size..........................: The poly-engine has 1.301 Bytes          |
                                The whole virus has 4.158 Bytes          |
Encrypted.....................: Yes, but only the virus part.            |
                                I'll crypt also the poly engine in       |
                                next versions.                           |
Polymorphic...................: Yes                                      |
                                                                        |
written from 20.11.2002 to 22.11.2002                                    |
in Austria                                                              |
------------------------------------------------------------------------
```

Modifications

IRC-Worm.Spth.b

The worm's droppers are: SPISSTOM.BAT, C:\PROGRA~1\MIRC\MIRC.BAT
The script file name is: C:\PROGRA~1\MIRC\SCRIPT.INI

IRC-Worm.Spth.c

The worm's droppers are: SPISSTOM.BAT, C:\MIRC\INSTALL.BAT
The script file name is: C:\MIRC\SCRIPT.INI

IRC-Worm.Spth.d

The worm's droppers are: DRRA.BAT, C:\PROGRA~1\MIRC\SATURN.BAT
The script file name is: C:\PROGRA~1\MIRC\SCRIPT.INI

IRC-Worm.DOS.Banishing.2373

Aliases

IRC-Worm.DOS.Banishing.2373 (Kaspersky Lab) is also known as: IRC-Worm.Banishing.2373 (Kaspersky Lab), Banish (McAfee), Banishing.2373 (Symantec), Banish-2417 (Sophos), Ban.2404 (RAV), MEMA-1217 (Trend Micro), Banishing.2373 (FRISK), Dark (ALWIL), Dei (Grisoft), BehavesLike:Dos.IRC-Worm (SOFTWIN), Dark_Banishing.2404 (Panda)

Description added	Feb 13 2002
Behavior	IRC Worm

Technical details

This is an mIRC worm combined with a memory resident parasitic stealth DOS virus. The DOS instance, when run, hooks INT 21h, and writes itself to the end of DOS COM and EXE files that are executed or opened. The virus is encrypted in COM and EXE files.

To spread its worm component via mIRC channels, it overwrites the SCRIPT.INI file in the C:\MIRC directory with a set of instructions that send this SCRIPT.INI file to the channel upon file sending and receiving as well as to users that are leaving the channel. The worm does not send the infected DOS file to the channel, only to the SCRIPT.INI file.

The infected script also manifests itself with messages: when an infected client connects to a channel, it joins the "virus" channel and sends the following text there:

```
Will not the mountains quake and hills melt at the coming of the darkness?
Dark Banishing V1.0
```

If the text "virus" is found in the channel, the worm sends the same message to this channel.

The worm also contains the text strings:

```
Dark Banishing Version 1.0
Dark Banishing V1.0 By VxFaeRie
```

IRC-Worm.DOS.Claw.2513

Aliases

IRC-Worm.DOS.Claw.2513 (Kaspersky Lab) is also known as: IRC-Worm.Claw.2513 (Kaspersky Lab), IRC/Claw.2513 (McAfee), Warfair.2513 (Symantec), Clawfinger.2513 (Doctor Web), Clawfinger-2513 (Sophos), mIRC_Worm/Clau.2513 (RAV), CLAWFINGER-C (Trend Micro), INI/Claw (H+BEDV), Warfair.2513 (FRISK), Puddings-2513 (ALWIL), IRC-Worm/Claw (Grisoft), Claw.2513.A (Panda)

Description added	Feb 13 2002
Behavior	IRC Worm

Technical details

This is a very dangerous memory resident encrypted parasitic virus. It hooks INT 21h, and writes itself to the end of COM and EXE files when they are accessed. Then it looks for COM and EXE files in the current directory and infects them. The virus also creates a hidden file in the root directory on the C: drive, writes its copy to there and adds to the AUTOEXEC.BAT an instruction to execute this file. The virus then infects WIN.COM and COMMAND.COM in the Windows directory.

To infect mIRC and spread via IRC channels, the virus creates two files in the C:\MIRC directory: the MIRC_SYS.INI virus script file and DOS COM virus dropper CYBER.COM. Then it patches the MIRC.INI file with an instruction to load infected MIRC_SYS.INI file on IRC client start-up. The virus script switches off mIRC security (warning messages) and sends the virus dropper into the IRC channel at the moment a user disconnects from the channel.

On September 1st, depending on a random value, the virus erases the FLASH BIOS. To do this, the virus calls extended BIOS functions.

When the virus dropper starts, it displays the texts:

```
Clawfinger
```

The virus also contain encrypted strings:

```
Do you know how it feels to be down in the dirt with a bullet
in yer breast and blood on yer shirt Lying in a bloodpool down
in a pit covered with the corpse and the blood and the shit
How does it feel to have a gun at yer head when ya know that
you'd be much better off dead Freedom has a price and that price
is blood so chase the motherfucker right down in da mud
[ WARFAIR - CLAWFINGER ]
```

IRC-Worm.DOS.ElSpy.2278

Aliases

IRC-Worm.DOS.ElSpy.2278 (Kaspersky Lab) is also known as: IRC-Worm.ElSpy.2278 (Kaspersky Lab), Elspy.worm (McAfee), BAT.Trojan (Symantec), BAT/Elspy.2278* (RAV), BAT_ELSPY.2278 (Trend Micro), MIRC/WormElSpy.2278 (H+BEDV), BAT/Elspy.2278 (FRISK), BAT.Elspy.2278 (SOFTWIN), Worm.IRC.ElSpy.2278 (ClamAV), Univ.ES (Panda)

Description added	Feb 19 2002
Behavior	IRC Worm

Technical details

This is an IRC worm that spreads through IRC channels using the mIRC client for spreading. The worm appears on a computer as the EL15_BMP.EXE DOS program. When this file is executed by a user, the worm installs itself into the system, and creates a temporary DOS batch helper that copies the worm file to the C:\Windows\System directory and overwrites the mIRC SYSTEM.INI script file with new instructions.

The commands that are written to SYSTEM.INI mIRC script intercept several events:

- when a new user enters the infected channel, (s)he is sent by the worm copy (the C:\WINDOWS\SYSTEM\EL15_BMP.EXE file).
- on connection to a channel, the worm informs a user with a "EL15_SPY" nick about an infected client sends the IP address of an infected user the name of the IRC server the user is logged on to, and the port address.
- if the word "EL15" appears on the channel, the worm opens the C:\ drive on an infected computer as a file server (shares C: drive).
- on text "are_u" the worm sends the message: "EL15_send_kisses_to_U_:)__come_on!" followed with an IP address of an infected user.

The worm contains the following text strings:

```
Designed by Del_Armg0____26 Juin 1999____Keep It Load!
MagicÇ%Software (c) 1999
```

IRC-Worm.DOS.Godog.a

Aliases

IRC-Worm.DOS.Godog.a (Kaspersky Lab) is also known as: IRC-Worm.Godog.a (Kaspersky Lab), IRC/GDog (McAfee), IRC.Family.Gen (Symantec), IRC.GhostDog (Doctor Web), mIRC/Worm-GDOG (Sophos), IRC/GhostDog* (RAV), TROJ_GHOSTDOG (Trend Micro), Worm/Generic.Ini (H+BEDV), GhostDog (ALWIL), IRC-Worm/GDog (Grisoft), IRC-Worm.GhostDog.A (SOFTWIN), Worm.Generic.Ini (ClamAV), IRC/Ghostdog (Panda)

Description added	Nov 20 2000
Behavior	IRC Worm

Technical details

This is a virus worm that spreads via IRC channels. It is a DOS program, and when run, it copies itself to the MIRC directory (if MIRC software is installed) with the "GhostDog.exe" name, and creates the SCRIPT.INI mIRC script file here. This script contains instructions that send a worm copy to users that enter the infected IRC channel. The script also hides messages if they contain the "virus" or "worm" words.

The main worm feature is the fact that it generates polymorphic instructions in the SCRIPT.INI file. These instructions are mixed in order; characters are randomly uppper and lower-cased; there are a random number of random comment-lines here, for example:

```
n0=$40Yw840RIGlx6Amlp7G0JaZ4QTs840N
n1=On 1^tExt^*WoRm*^*^{ /Ignore $nick | /closeMsg $NiCk }
n2=$HyX5NMq840KBAfrpTGfj7Z0DuT5J6m840GXWb1lQcbe7V0ZpT5F5j840CTRwihMYW
```

Despite the strange appearance, the script commands maintain their functionality.

IRC-Worm.DOS.Kazimas

Aliases

IRC-Worm.DOS.Kazimas (Kaspersky Lab) is also known as: IRC-Worm.Kazimas (Kaspersky Lab), Bat/kazi (McAfee), IRC.Kazimas.worm (Symantec), mIRC/Kazimas (Sophos), BAT/Kazimas.A* (RAV), BAT_KAZIMAS.A (Trend Micro), BAT/Kazimas (H+BEDV), BAT/Kazimas.A (FRISK), BV:Qt (ALWIL), BAT.Kazimas.A (SOFTWIN), Worm.IRC.Kazimas (ClamAV), BAT/Kazimas (Panda)

Description added	Feb 19 2002
Behavior	IRC Worm

Technical details

This is an IRC virus-worm that spreads itself via mIRC channels. It appears as a MILBUG_A.EXE DOS EXE file about 10Kb in length. When it is executed, it copies itself to several disk directories under different names:

```
C:\WINDOWS\KAZIMAS.EXE
C:\WINDOWS\SYSTEM\PSYS.EXE
C:\ICQPATCH.EXE
C:\MIRC\NUKER.EXE
C:\MIRC\DOWNLOAD\MIRC60.EXE
C:\MIRC\LOGS\LOGGING.EXE
C:\MIRC\SOUNDS\PLAYER.EXE
C:\GAMES\SPIDER.EXE
C:\WINDOWS\FREEMEM.EXE
```

The worm then infects the installed mIRC client in the C:\MIRC directory: it creates a new script file SCRPT.INI and overwrites the MIRC.INI configuration file. If the mIRC client is installed in any other path, the worm fails to infect it.

The worm modifies the MIRC.INI files that customize the mIRC client. There are several options set, for instance a user's identity is set to "kazimas", and the additional script file SCRPT.INI is included in auto-run scripts.

The SCRPT.INI file, that is dropped by the worm, contains several instructions that switch a user to the "Chat2K" channel, send messages to there, and the most important: send to the channel the worm copy (the C:\WINDOWS\KAZIMAS.EXE file).

The worm also overwrites the C:\AUTOEXEC.BAT file with instructions that restore worm's copies (if they are erased) and execution:

```
@copy c:\windows\system\psys.exe c:\windows\kazimas.exe >nul
@copy c:\windows\kazimas.exe c:\kazimas.exe >nul
@c:\kazimas.exe >nul
@cls
```

IRC-Worm.DOS.Loa

Aliases

IRC-Worm.DOS.Loa (Kaspersky Lab) is also known as: IRC-Worm.Loa (Kaspersky Lab), IRC/Loa (McAfee), IRC.Family.Gen (Symantec), IRC/Generic* (RAV), IRC_LOA (Trend Micro), IRC/Loa.A (FRISK), IRC-Worm/Loa (Grisoft), Worm.IRC.Loa (ClamAV), mIRC/Gen (Panda)

Description added	Feb 19 2002
Behavior	IRC Worm

Technical details

This is an IRC worm that spreads via mIRC channels. The worm code itself is a randomly named DOS EXE file. When it is executed, the worm copies itself with the LOA.EXE name to the Windows directory and registers this file in the system registry in the auto-run section:

```
LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices:
"Life of Agony"="loa.exe"
```

When the worm locates the MIRC.INI file, it writes to there several instructions that disable the mIRC security settings and creates its script file that contains commands that send the worm's EXE file to the channel.

The worm manifests itself as anti-virus programs that searche and delete the DM-Setup mIRC worm (the worm actually does delete DM-Setup files if they present on disks). It then displays the following messages:

```
You are about to scan your harddrive for the DMSetup virus, it is
crucial that you run this program without mIRC active, so if you
are still in mIRC at the moment, type /EXIT before you continue.
Press any key if mIRC is not active...
```

The worm also displays other messages that depend on the current date:

```
PowerBit anti-virus v3.34, (C)opyrighted 1999 by PB Systems.
SHAREWARE - REGISTER?
YES!
Scan completed, no viruses were found.
The Ultimate Chaos Website 2 - http://sourceofkaos.com/homes/ultchaos
Visit me...
NOW!
Not detected.
WaReZ SCaNNeR bY oDELiOFiLThY [SuCK]... ViSiT #warez !
SeLF CHeCK:
oKeY
nO WaReZ wErE FoUnD aT DRiVe C: !!!
DrSolomon Anti-Virus Toolkit v10.00 - SPECIAL EDITION -
Scanning memory (DOS\UMB\HMA\XMS)...
No viruses found in memory
No viruses were found.
ScanDisk 2.00, (C)Copyright Microsoft Corp 1981-1998.
Checking critical areas...
OK
No errors were detected.
Anti-Back-Orifice II.A, detects/removes all BO-instances from your system.
Checking registry...
BO was not found in the registry
System clean, visit http://sourceofkaos.com/homes/ultchaos for updates.
TERA SPOOF-INSTALLER VERSION 6.66
Checking shadow-RAM...
located at x0FA56D6A4h
Failed to install spoof, SPSOCK64.DLL missing.
WinGater by Terminatius [Finds installed WinGates at your system].
Locating registry:
REGISTRY.REG
No WinGates found, go to Undernet, #wingater for help.
Thunderbyte virus-detector v9.24, - (C) Copyright 1989-1999 Thunderbyte B.V.
SANITY CHECK:
OK!
No viruses were found.
Anti-Nuke written by cDc - Cult of the Dead Cow.
Checking V86 interrupts...
No polling detected
No nuke-programs found.
LOA''s Kill-DMSetup version 2.2, - SHAREWARE
Checking memory...
OK
Completed!
KILL-CIH v2.0. --> kills all known CIH-strains! <--
Memory check...
passed
CIH has not been detected at your system.
```

When the worm is started with the /SECRET argument, it displays the following message:

```
=[ Life of Agony 1.30, (c) 1998 by T-2000 / Immortal Riot ]=
Hi! I am the [LIFE OF AGONY] worm, and I''m gonna fuck you up REAL bad!
```

LIFE OF AGONY

IRC-Worm.DOS.Mabra.a

Aliases

IRC-Worm.DOS.Mabra.a (Kaspersky Lab) is also known as: IRC-Worm.Mabra.a (Kaspersky Lab), IRC/Mabra.worm (McAfee), IRC.Family.Gen (Symantec), IRC.Mabra.14396 (Doctor Web), mIRC/Mabra-A (Sophos), HLLW.Mabra.A (RAV), TROJ_MABRA.A (Trend Micro), VGEN/24338.512 (H+BEDV), HLLW.Mabra.A (FRISK), IRC:Mabra (ALWIL), IRC-Worm/Mabra (Grisoft), HLLW.Mabra.A (SOFTWIN), Worm.IRC.Mabra.A (ClamAV), IRC/Mabra.A (Panda)

Description added	Feb 19 2002
Behavior	IRC Worm

Technical details

This is a silly IRC worm that spreads through IRC channels using mIRC client for spreading. The worm appears on a computer as the DOS EXE file with MABRA.EXE, CDMAN.EXE, or GLADYS.EXE filename (depending on the worm's version), and about 14K in file size. When this file is executed by a user, the worm copies itself into C:\WINDOWS, C:\WINDOWS\SYSTEM or C:\WINDOWS\SYSTEM32 directory (depending on worm version), and overwrites the mIRC script file SCRIPT.INI in the C:\MIRC directory. The new script sends the worm copy to any user that enters an infected channel.

Depending on the system time, the worm erases the C:\WINDOWS\WIN.COM file.

IRC-Worm.DOS.Milbug.a

Aliases

IRC-Worm.DOS.Milbug.a (Kaspersky Lab) is also known as: IRC-Worm.Milbug.a (Kaspersky Lab), IRC/Milbug.a (McAfee), IRC.Family.Gen (Symantec), IRC.Milbug (Doctor Web), mIRC/Milbug-A (Sophos), HLLW.Milbug.A (RAV), WORM_MILLBUG.A (Trend Micro), IRC:Milbug (ALWIL), IRC-Worm/Milbug (Grisoft), IRC-Worm.Milbug.A (SOFTWIN), W32/Milbug.A (Panda)

Description added	Feb 20 2002
Behavior	IRC Worm

Technical details

This is an IRC virus-worm that spreads itself via mIRC channels. It appears as a MILBUG_A.EXE or MILBUG_B.EXE DOS EXE file about 10Kb in length. The file name depends on the worm version. When the worm file is executed, it overwrites the SCRIPT.INI file in the C:\MIRC directory with its own script program that has just two instructions. The first one sends the following message to any new user in the channel:

```
I'm testing my millenium bug fix program. Receive it and test it
```

The second one sends the MILBUG EXE file to this user.

The worm does not have any dangerous payload and does not manifest itself in any other way.

IRC-Worm.DOS.MrWormy.1198

Aliases

IRC-Worm.DOS.MrWormy.1198 (Kaspersky Lab) is also known as: IRC-Worm.MrWormy.1198 (Kaspersky Lab), IRC/Mypic (McAfee), MrWormy.1200 (Doctor Web), mIRC/MrWormy (Sophos), Mypic.1198 (RAV), WORM_MRWORMY (Trend Micro), MIRC/CeydaDemet.B (H+BEDV), Mypic.1198 (FRISK), Trivial (Grisoft), BehavesLike:Dos.IRC-Worm (SOFTWIN)

Description added	Feb 19 2002
Behavior	IRC Worm

Technical details

This is a harmless encrypted parasitic virus-worm that spreads via mIRC and PIRCH chat channels. To install itself into the system, the virus patches chat-client scripts and creates the infected DOS COM file MYPIC.COM in the \WINDOWS directory, and this file has Hidden and Read-only attributes set. The infected chat clients then will send this infected file to the chat channels.

To infect chat clients, the virus first of all checks and creates the EVENTS.INI file in the \PIRCH98 directory. New EVENTS.INI sends the infected file C:\WINDOWS\MYPIC.COM, when a user enters the IRC channel.

If the PIRCH client was not found, the virus attacks the mIRC client. It checks and creates the SCRIPT.INI file in the \MIRC directory. New SCRIPT.INI sends to channel the files C:\WINDOWS\MYPIC.COM and C:\MIRC\MIRC.INI.

The virus then appends to the end of a C:\AUTOEXEC.BAT file the instruction that will activate the virus dropper C:\WINDOWS\MYPIC.COM each time the system reboots.

The EVENTS.INI script file in the infected PIRCH directory has just one instruction that sends to the channel that infected file. The SCRIPT.INI file in the infected mIRC is more complex and runs more actions:

- on entering any new person to the channel, he/she is sent by the virus dropper (the C:\WINDOWS\MYPIC.COM file)

- when "why me" appears in the channel (a user sends it), the script runs the mIRC timer that runs an attack on CTCP protocol to this user.

- when joining with a IRC server, the script sends the message to the user with "TPhunk" name on the same server:

```
I am alive
```

- on receiving the CTCP commands "blah", the script quits mIRC with the message:

```
I am Owned - TP ownes me
```

- on receiving the CTCP command "bye", the script starts the mIRC timer that once per second executes the COMMAND.COM file.

- on receiving the CTCP command "give", the script sends to this user the MIRC.INI file from the C:\MIRC directory.

- on receiving the CTCP command "unf", the script runs on the computer a file that is specified in the command parameters.

- on receiving the CTCP commands "ya", the script sends a message to a user. Both the user and message are specified in the command's parameters.

- on receiving the CTCP commands "own", the script changes the window title to the following text:

```
You've been hax0red
```

- on receiving the text "mypic" from a user, the script in 30 seconds runs and attacks this user by CTCP protocol.

- on receiving the CTCP command "giveme", the script sends out a file that is specified in the command's parameter, i.e., the worm is able to steal data from remote computers.

IRC-Worm.DOS.Pron.576

Aliases

IRC-Worm.DOS.Pron.576 (Kaspersky Lab) is also known as: IRC-Worm.Pron.576 (Kaspersky Lab), Pron.gen (McAfee), mIRC/Pron-576 (Sophos), BAT/Pron.B (RAV), BAT_PRON.B (Trend Micro), MIRC/Pron (H+BEDV), BAT/Pron.B (FRISK), BV:Pron-576 (ALWIL), IRC-Worm/Pron (Grisoft), BehavesLike:Dos.IRC-Worm (SOFTWIN), IRC/Pron.576 (Panda), Pron.576 (Eset)

Description added	Feb 19 2002
Behavior	IRC Worm

Technical details

This is an IRC worm that spreads through IRC channels using mIRC client for spreading. The worm is encrypted and has a very short size - just about 600 bytes, and appears as the PR0N.BAT file. When this file is executed on a computer, it copies itself with the PR0N.COM file and executes it as a DOS program. The worm code is built so that it can be executed as a DOS COM file as well as a DOS Batch, so the main worm routine (as a COM program) gains control and installs the worm into the system.

To infect the system, the worm uses a very silly way: it just copies its BAT file with the same name to the Windows system directory by using its direct name C:\WINDOWS\SYSTEM. If Windows is installed in any other directory, the worm fails to install itself. The worm then creates the WINSTART.BAT file and overwrites its with worm's code.

To spread itself via IRC channels, the worm overwrites SCRIPT.INI in the mIRC directory. The worm searches for this directory by four variants:

```
C:\MIRC
C:\MIRC32
C:\PROGRA~1\MIRC
C:\PROGRA~1\MIRC32
```

The worm's script is very short and just sends the worm's BAT file to all users joining an infected channel.

The worm also contains the "copyright" text:

```
IRC-pr0n.bat v1.0 (c) nUcLeii 1999
```

IRC-Worm.DOS.Readme.1077

Aliases

IRC-Worm.DOS.Readme.1077 (Kaspersky Lab) is also known as: IRC-Worm.Readme.1077 (Kaspersky Lab), Readme.1077 (McAfee), Readme.1077 (Doctor Web), Readme-1077 (Sophos), mIRC_Worm/Readme.1077 (RAV), TROJ_README.A (Trend Micro), VGEN/45109 (H+BEDV), Dark_matter.1077 (FRISK), Readme-1077 (ALWIL), Dark_matter.1077 (Panda)

Description added	Feb 20 2002
Behavior	IRC Worm

Technical details

This is an IRC worm spreading through IRC channels and using the mIRC client for spreading. The worm appears on a computer as the README.EXE DOS program. When this file is executed by a user, the virus installs itself resident into DOS memory and infects DOS COM files (except COMMAND.COM) that are executed. The virus is encrypted in infected files, and its code is placed at the end of files.

The virus also creates its "dropper" README.EXE on the C: drive (this file has a "hidden" attribute) and "registers" it in the C:\AUTOEXEC.BAT in the very first lines: they contain an instruction to execute virus the dropper upon each rebooting.

To spread through mIRC channels, the virus searches for the C:\INTERNET\MIRCdirectory and creates a SCRIPT.INI file there that contains just one command for sending the README.EXE dropper to anybody joining the infected channel.

The worm contains the following text strings:

```
;-)x
whose name means dark matter vir-L
```

IRC-Worm.DOS.Septic

Aliases

IRC-Worm.DOS.Septic (Kaspersky Lab) is also known as: IRC-Worm.Septic (Kaspersky Lab), Messiah.bat (McAfee), BAT/Septic.4535.A* (RAV), BAT_SEPTIC.A (Trend Micro), BAT/Septic.4535.A (FRISK), BV:Porn (ALWIL), Univ.EO (Panda)

Description added	Feb 19 2002
Behavior	IRC Worm

Technical details

This is a virus-worm that spreads through mIRC channels by using an mIRC script program, and attempting to affect HTML files to infect remote computers when an Internet browser reads infected HTML pages.

The virus manifests itself on the 1st and 2nd of each month. It displays messages and then runs a video effect. By using VGA functions, the virus changes colors of the monitor turning it from white-on-black to black-on-white and back. The messages are as follows:

```
Day 1st:
Only in your dreams you can be truly free!
~+DarK.MeSsiAh+~ written by SeptiC [TI]
Day 2nd:
Pure evil comes from within! ~+DarK.MeSsiAh+~
Written by SeptiC [TI]
```

The virus also supports a "protection" that disables virus infection routines. When a virus copy is executed, it looks for the C:_VAC.TXT file and immediately returns to the host program if such a file exists. The virus also displays the message here:

```
You are protected by a devine power
~+DarK.MeSsiAh+~ will not touch your files
```

DOS COM and EXE infector

The main part of the virus is an ordinary parasitic DOS file infector. The virus is encrypted, and when an infected file is executed, the decryption loop restores the virus code to non-encrypted form and jumps to the main virus routine. The virus then searches for DOS COM and EXE files and infects them. While infecting, the virus encrypts and writes its code to the end of the file and modifies the file header.

The virus searches for files and infects them in the current directory, in the parent directories, and in the directory tree on all drives from C: to G:. The virus checks file names and does not infect: COMMAND, ?GA*, ??NP*, ???GW* files; runs mIRC script infection routine if MI* (MIRC.EXE, MIRC32.EXE) file is found; corrupts anti-virus files: F-*, TO*, TB*, SC*, AV* (F-PROT, TBAV, SCAN, AVP) - the virus overwrites them with a code that displays the message and returns to DOS when an infected file is executed:

```
~+DarK.MeSsiAh+~ a Digital Touch of DarKness! Written by SeptiC [TI]
```

The virus also deletes the ANTI-VIR.DAT file if it exists.

Infecting BAT files

The virus also searches for BAT and HTML files and infects them in the same directories. While infecting BAT files, the virus writes to the end of the file DOS commands that replace the DOS "dir" command with a set of two instructions: the first runs a virus dropper PORNO.COM, the second executes the DOS "dir" instruction. As a result, on any "dir" instruction the virus dropper is executed.

The virus creates its dropper file PORNO.COM in the Windows Command directory. To locate this directory the virus tries three variants:

```
C:\WINDOWS\COMMAND
C:\WIN95\COMMAND
C:\WIN98\COMMAND
```

If not one of them is valid, the virus drops this file in the current directory. The virus then opens the C:\AUTOEXEC.BAT file and infects it in the same way as for other BAT files.

Infecting HTML files

While infecting an HTML file, the virus creates, in the same directory, the infected dropper with the PATCH.COM name and appends to the end of the HTML file a short set of HTML commands that display the message:

```
Download The Latest Patch!
Click Here!
```

The "Click Here!" is a link that downloads and runs the PATCH.COM virus dropper, when this link is activated. As a result, infected HTML pages are "continued" with a virus text that offers to download an upgrade, but spreads the virus code instead.

mIRC script

The virus looks for an mIRC client installed in the system and creates a new SCRIPT.INI file in the same directory. The virus looks for mIRC in six directories and does not drop its mIRC component if none of the directories is found:

```
C:\MIRC
C:\MIRC32
C:\PROGRAM\MIRC
C:\PROGRAM\MIRC32
C:\PROGRA~1\MIRC
C:\PROGRA~1\MIRC32
```

While infecting the mIRC client, the virus uses the same trick as other mIRC viruses do: it overwrites the standard mIRC script file SCRIPT.INI with an infected one. When an mIRC client starts with an infected script, it accepts this file and follows its instructions.

The infected SCRIPT.INI contains several commands. The main one is the virus-sending instruction: when any user sends/receives any files, the virus sends to this user its infected dropper file, PORNO.COM.

The virus also sends messages to the channel and users on the channel. When an infected client connects to an IRC server, the virus sends the message to a user with the "SeptiC_dm" nickname:

```
I am your servant! I have been turned into a zealot of darkness
```

If the "D.Messiah" string appears in a message in the channel the, virus sends its own message to all users on the channel:

```
Only in your dreams you can be truly free!
~+DarK.MeSsiAh+~ Written by SeptiC [TI]
```

On the "666" string, the virus changes the topic of the channel (that is displayed in the header of the channel window), if the infected user has enough privileges. The new topic string appears as follows:

```
~+DarK.MeSsiAh+~ a Digital Touch of DarKness! Written by SeptiC [TI]
```

On the "pray" text, the virus sets the channel operator mode to a user who posts this text, and sends the message to the channel:

```
I Obey my master! long live satan
```

On the "sacrifice" text all infected users are kicked out of the channel with the message:

```
Your word is my command, Power to satan!
```

IRC-Worm.IRC.Edoc

Aliases

IRC-Worm.IRC.Edoc (Kaspersky Lab) is also known as: IRC-Worm.Edoc (Kaspersky Lab), IRC/Edo (McAfee), IRC.Family.Gen (Symantec), mIRC/Edoc-A (Sophos), IRC/Edoc* (RAV), TROJ_MAKEOP.A (Trend Micro), Worm/Edoc (H+BEDV), VBS:Malware (ALWIL), Backdoor.IRC.Edoc (SOFTWIN), Worm Generic (Panda), mIRC/Edoc.A (Eset)

Description added	Jan 15 2002
Behavior	IRC Worm

Technical details

This is a simple network worm that replicates in IRC channels. The worm sends the following message to all channel users, except channel operators, that connect to the channel where an infected user is connected:

```
hey  to get OPs use this hack in the chan but SHH!
//$decode(d3JpdG.....................................................
.....................................................................
.....................................................................
.....................................................................
...................SkgLG0p,m) | $decode( Lmxv........IMQ= ,m)
```

(dots are placed instead of the virus)

This message contains a line starting from "//", which is a script command and contains the worm's body, encoded with MIME base64 encoding.

If a user receiving the infected message starts the script, the worm creates a file that is then distributed through IRC channels, and adds a link to the infected file in the "mirc.ini" file.

IRC-Worm.IRC.Radex

Aliases

IRC-Worm.IRC.Radex (Kaspersky Lab) is also known as: IRC-Worm.Radex (Kaspersky Lab), JS/Radex@MM (McAfee), JS.Radex.mirc (Symantec), BAT/Radex* (RAV), JS_RADEX.A (Trend Micro), Worm/Radex.1 (H+BEDV), BAT/Radex (FRISK), BAT.Radex.A (SOFTWIN), Worm.IRC.Radex (ClamAV), Radex.A (Eset)

Description added	Oct 18 2001
Behavior	IRC Worm

Technical details

This is a virus-worm that spreads via IRC channels. The worm itself is a batch-script file about 3 Kb in length.

The worm copies itself to the following batch files:

C:\Windows\winstart.bat
C:\Windows\LINUX_SH_DOS_BAT_WIN_JS.bat
C:\Win95\LINUX_SH_DOS_BAT_WIN_JS.bat
C:\Win98\LINUX_SH_DOS_BAT_WIN_JS.bat
C:\WinME\LINUX_SH_DOS_BAT_WIN_JS.bat

The batch file drops and executes the JS file LINUX_SH_DOS_BAT_WIN_JS.JS. This JS file displays a dialogue window with the following Title/Subject:

Radix16/SMF
SH-BAT-JS

After this, the worm creates and sends the new e-mail message to the following address:

Radix16@atlas.cz

The infected messages contain the following:

Subject: SHBATJS
Body: crazzy bat :) testing MS OTLOOK in the (WORLD)
Attach: LINUX_SH_DOS_BAT_WIN_JS.bat

The virus-worm also creates the file C:\MIRC\SCRIPT.INI. This INI file sends the batch file to the IRC channels.

Installing

While installing, the worm copies its JS component to the Windows directory with the name C:\WINDOWS\LINUX_SH_DOS_BAT_WIN_JS.JS, and registers this file in the WIN.INI run section.

The worm also contains the following text strings:

/bin/sh
-=LINUX START=-
-=DOS/WIN START=-
ONLY SAMPLE (TEST) LINUX SH DOS BAT WIN JS .....
WoRID iS mY

IRC-Worm.IRC.Sonne

Aliases

IRC-Worm.IRC.Sonne (Kaspersky Lab) is also known as: IRC-Worm.Sonne (Kaspersky Lab), VBS/Sunflower.gen (McAfee), VBS.Onnet (Symantec), VBS.Warlus (Doctor Web), VBS/Sonnet-A (Sophos), VBS/VBSWG.dr.gen* (RAV), VBS_SONNET.A (Trend Micro), Worm/Sonnet (H+BEDV), VBS/Sonnet.A (FRISK), VBS:Malware (ALWIL), VBS/Sonnet (Grisoft), VBS.Sonne.A (SOFTWIN), Worm.IRC.Sonne (ClamAV), Worm Generic (Panda), VBS/Sonne (Eset)

Description added	Feb 15 2002
Behavior	IRC Worm

Technical details

This is an IRC worm that spreads through IRC channels using mIRC client for spreading. The worm appears on a computer as the "Sonnet.vbe" VBE program. When this file is executed by a user, the worm installs itself into the Windows directory and overwrites the mIRC SYSTEM.INI script file with new instructions.

The commands that are written to the SYSTEM.INI mIRC script intercept several events:

- when a new user enters the infected channel, (s)he is sent by the worm copy (the C:\WINDOWS\SONNET.VBE file).

IRC-Worm.MSWord.Anumps

Aliases

IRC-Worm.MSWord.Anumps (Kaspersky Lab) is also known as: IRC-Worm.Anumps (Kaspersky Lab), W97M/Generic (McAfee), W97M.Anumps.A (Symantec), W97M.Belyash (Doctor Web), WM97/Anumps-A (Sophos), W97M/Furio.D (RAV), W97M/Furio.D (FRISK), MW97:Furio (ALWIL), W97M/Furio (Grisoft), W97M/Generic (Panda), STEALTH.MACRO (Eset)

Description added	Sep 17 2003
Behavior	IRC Worm

Technical details

This worm spreads via IRC channels and infects MS Word documents. The virus itself is a Word document containing a macro named Mumps.

Installation

When opened, the file will:

- attempt to disable the Security menu in the Macro menu
- disable the ban on activating macros in the Windows system registry
- create a file named Mumps.drv in C:\Windows\ directory and writes the code of the macro to this file. This file is then used to infect all open Word documents
- save the active document to the hard drive under the following names:

```
C:\Windows\FAQ.doc
C:\Program Files\Microsoft Office\Office\STARTUP\Mumps.dot
```

- commences propagation via IRC.

Propagation via IRC

The worm modifies a file named script.ini file. This means the file C:\Windows\FAQ.doc will automatically be sent to all users of the channel used by the infected computer.

Signs of infection

When the user tries to open the Help\About menu, the worm changes the background colour of the document to dark blue. Letters will appear in white. It also open notepad.exe displaying the following text:

```
"Windows has low memory resources. Please restart your Windows....."
```

If the user tries to print the current document and the system clock is showing 59 seconds, a Message Box with the following text will be displayed:

```
"Your printer driver is not compatible with Windows. Please
install another printer drivers."
```

If the user tries to view the code of the Macros or open the Tools\Macro menu, a Message Box with the following text will be displayed:

```
"There is something a trouble with this function..."
```

Other

The worm attempts to register C:\Windows\FAQ.doc in the system registry as the default signature for Microsoft Outlook 5.0. The file will then automatically be added to all outgoing mail.

IRC-Worm.VBS.Evion

Aliases

IRC-Worm.VBS.Evion (Kaspersky Lab) is also known as: IRC-Worm.Evion (Kaspersky Lab), VBS/Waterworks.worm (McAfee), VBS.Waterworks.Worm (Symantec), VBS/Evion-A (Sophos), VBS/Evion.gen* (RAV), VBS_EVION.A (Trend Micro), VBS/Evion.1 (H+BEDV), VBS/Evion.A (FRISK), VBS:Malware (ALWIL), VBS/Envion (Grisoft), VBS.Evion.A (SOFTWIN), Worm.VBS.Evion (ClamAV), VBS/Evion (Panda), VBS/Evion.A (Eset)

Description added	Feb 28 2003
Behavior	IRC Worm

Technical details

IRC-Worm.Evion **Evion** is an IRC worm spreading via IRC channels. The virus is written in Visual Basic Script (VBS). It overwrites .vbs and .html files on all local and mapped drives.

Installing:
When the worm is executed it does the following:

Evion creates copies of itself in the root directory of disk C: in the file "Win32 Strt.exe.vbs " and in the system directory file "BootLoader.exe.vbs" as well as in the root Windows directory in the files"Jokes.htm" and "Winupdate.exe"

Evion overwrites these existing files with a copies of itself:

```
%Windir%\Readme.htm
%Windir%\Htmlhelp.htm
%System%\Winhelp32.exe
%Mirc%\script.ini
```

Evion registers the files "BootLoader.exe.vbs" and "Win32 Strt.EXE" in the automatic launch string of the system registry:

```
HKEY_LOCAL_MACHINE\Microsoft\Windows\CurrentVersion\Run - (BootLoader.exe.vbs)
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices - (Win32
Strt.EXE)
```

Spreading
Evion searches for the all .vbs files and overwrites the existing .vbs files with a copies of itself. Files that have the extensions .htm, .html, .asp, .htx, and .hta are replaced with the .HTML version of the worm.

The "Script.ini" file is a short mIRC program that sends the **%Windir%\Jokes.htm** file to everybody who enters an infected channel.

Payload
The worm activates its payload three different days (October 15th, November 23rd and December 25th), and displays a Message Box with the following respective texts:

```
with Message box title "my b-day" and text "happy birthday kefi" - 15 october
with Message box title "11/23!" and text "holy sh*t! it's 11/23" - 23 november
with Message box title "kefi [rRlf]" and text "Organized religion controls the
world" - 25 december
```

On these payload activation days the worm also creates 16 text files in the Windows Startup folder. The file name uses the format: Startup\Evion(n).txt, where n is between 0 and 15 (inclusive). These files contain 50 text strings of randomly generated text that is selected from these three lines:

You've done and gotten your self infected with Vbs.Evion by kefi [rRlf] [rRlf] ownz joo bitch Catfish_VX are lamers. This virus was constructed for them to steal

On days other than the ones on which the payload runs, a text document is created in the Desktop Windows directory. The file name uses the format "Desktop\%day% - %month%.vir.txt".

These files contain the following text:

```
today you did not experience the payload of Vbs.Evion
sorry..
kefi [rRlf]
```

IRC-Worm.VBS.Lara

Aliases

IRC-Worm.VBS.Lara (Kaspersky Lab) is also known as: IRC-Worm.Lara (Kaspersky Lab), IRC/Theme.worm.a (McAfee), IRC.Forca.Worm (Symantec), mIRC/Lara (Sophos), VBS/Lara* (RAV), VBS_LARA.A (Trend Micro), Worm/Lara.1 (H+BEDV), VBS/Lara.B (FRISK), IRC:Generic (ALWIL), VBS/Forca (Grisoft), VBS.Theme.B (SOFTWIN), VBS/LaraCroftTheme (Panda), Lara (Eset)

Description added	Sep 04 2001
Behavior	IRC Worm

Technical details

This is a silly IRC worm spreading through IRC channel and using mIRC client for spreading.

This is the first known modern Internet worm that spreads "Desktop Themes" files.

The worm appears on computer as the "LaraCroft.theme" filename.

On start this file the worm looks for mIRC-client, creates subsidiary VBS file in Windows directory and starts it. This file overwrites the mIRC script file SCRIPT.INI. The new script sends the worm copy to any user that enters infected channel.

IRC-Worm.Win32.Adrenaline

Aliases

IRC-Worm.Win32.Adrenaline (Kaspersky Lab) is also known as: IRC-Worm.Adrenaline (Kaspersky Lab), W32/Scrambler.c@MM (McAfee), W32.HLLP.Scrambler.D (Symantec), Win32.HLLW.Bugfix.34816 (Doctor Web), W32/Bugfix (Sophos), IRC/Adrenaline (RAV), PE_BUGFIX.A (Trend Micro), W95/Adrenaline (H+BEDV), W32/Adrenaline (FRISK), Win32:BugFix (ALWIL), IRC-Worm/Adrenaline (Grisoft), Win32.HLLW.Adrenaline.34816 (SOFTWIN), IRC-Worm.Adrenaline (ClamAV), IRC-Worm.Adrenaline.A (Eset)

Description added	Feb 06 2002
Behavior	IRC Worm

Technical details

This is a virus-worm that infects Windows systems and spreads via IRC channels. The worm itself is a Windows executable file, written in MS Visual C++ and compressed by PECompact (compressed size is about 35K, uncompressed size is about 65K).

When an infected file is run, it looks for EXE files in the Windows directory and infects them. While infecting, the virus moves the file body down by 35K, and then writes itself to the top of the file. To release control to host file, the virus "disinfects" the host file to HOSTFILE.EXE, spawns it and then deletes it. The virus pays attention to the file names and does not infect a file if its name begins with 'E', 'P', 'R', 'T', 'W', or 3rd letter is 'D', or 5th letter is 'R'.

The virus also infects EXE files in the C:\MIRC\DOWNLOAD directory, without paying attention to file names.

To spread via IRC channels, the virus drops its "pure" image to the Windows system directory with the BUGFIX.EXE name, and overwrites the SCRIPT.INI file in the mIRC client directory. The infected SCRIPT.INI file contains just one instruction that sends the BUGFIX.EXE file to everybody joining the infected IRC channel.

The virus looks for the mIRC client in directories \MIRC\ and \PROGRA~1\MIRC\ on all drives from C: to F:.

The virus then runs another routine that sends messages by using MS Outlook. The virus does not spread itself in infected messages, but just spams the address "Rhape79@ultimatechaos.demon.co.uk" with messages that have a randomly generated Subject and Body. Upon each run, the virus sends 15 messages to that address.

IRC-Worm.Win32.Crack.a

Aliases

IRC-Worm.Win32.Crack.a (Kaspersky Lab) is also known as: IRC-Worm.Crack.a (Kaspersky Lab), W32/Insomnia (McAfee), IRC Worm Generic (Symantec), Win32.Crack (Doctor Web), mIRC/Insomnia (Sophos), Win32/Insomnia.A (RAV), TROJ_CRACK.B (Trend Micro), MIRC/Crack.A1 (H+BEDV), Win95:mIRCrack (ALWIL), IRC-Worm/Crack (Grisoft), IRC-Worm.Insomnia.A (SOFTWIN), Worm.W32.IRC.Crack.B (ClamAV), Worm Generic (Panda), Win32/Crack.A (Eset)

Description added	Jan 12 2001
Behavior	IRC Worm

Technical details

This is a silly IRC worm spreading through IRC channels by using mIRC client. The worm itself is Win32 executable file about 3K of length (that is compressed executable file, being decompressed it gets about 10K of size).

When the worm file is run, it copies itself to Windows directory with CRACK.EXE name and affects mIRC client. The worm looks for mIRC client in two directories:

> C:\MIRC\
> D:\MIRC\

While affecting the worm overwrites the SCRIPT.INI file with a set of commands that send the CRACK.EXE file (worm code) to users that join infected channel.

The SCRIPT.INI file on connecting to IRC server also joins "vxers" and "cservice" channels and sends the messages to there:

To "vxers":

> I'm wide awake in my kitchen, it's dark and I'm lonely, oh if I could
> only get some sleep.. Creeky noises make my skin creep. I need to get
> some sleep.. I can't get no sleep....

To "cservice":

> PLEASE join #vxers, and visit http://www.shadowvx.com/4Q and
> http://www.shadowvx.com/fun4vxers .. We're the best!

IRC-Worm.Win32.Hellfire.a

Aliases

IRC-Worm.Win32.Hellfire.a (Kaspersky Lab) is also known as: IRC-Worm.Hellfire.a (Kaspersky Lab), W32/Hellfire (McAfee), W32.Hellfire.Mirc (Symantec), Win32.IRC.Hellfire.32768 (Doctor Web), W32/Hellfire (Sophos), IRC/Hellfire (RAV), TROJ_HELLFIRE (Trend Micro), Worm/Hellfire.IRC.A (H+BEDV), Win95:HellFire (ALWIL), IRC-Worm/Hellfire (Grisoft), IRC-Worm.Hellfire.A (SOFTWIN), Worm.IRC.Hellfire.A (ClamAV), IRC/Hellfilre (Panda), IRC/Hellfire.A (Eset)

Description added	Aug 09 2007
Behavior	IRC Worm

Technical details

This worm spreads via IRC. It is a Windows PE EXE file. It is 11,264 bytes in size. It is packed using UPX. The unpacked file is approximately 50KB in size.

Installation

When launched, the worm copies its executable file as follows:

```
c:\mirc32\dirtysexsluts.scr
```

Payload

The worm writes the following strings:

```
[rfiles]
n100=safe.ini
```

to the following file:

```
c:\mirc32\mirc.ini
```

It creates a file and writes its script to the file:

```
c:\mirc\safe.ini
```

This script performs the following actions:

when the user "uncahellmang" enters the channel, the worm will transmit the following information about the infected machine to the user: IP address, version and type of operating system, current system data and time, and email address (from mIRC configuration).

All users entering the IRC channel are sent the following message:

```
http://hammer.prohosting.com/~nemo2k/freesex.htmlVisit this great NEW site now for 100% FREE Sex Pics And Movies.
No Strings Attached
```

The worm then uses DCC to send a copy of itself:

```
c:\mirc32\dirtysexsluts.scr
```

The worm then opens a large number of TCP ports on the victim machine and informs "uncahellmang" about attempts to connect to these open ports.

Removal instructions

If your computer does not have an up-to-date antivirus, or does not have an antivirus solution at all, follow the instructions below to delete the malicious program:

1. Use Task Manager to terminate the backdoor process.
2. Delete the original worm file (the location will depend on how the program originally penetrated the victim machine).
3. Delete the following files:

```
c:\mirc32\dirtysexsluts.scr
c:\mirc\safe.ini
```

4. Update your antivirus databases and perform a full scan of the computer (download a trial version of Kaspersky Anti-Virus).

IRC-Worm.Win32.Kromber

Aliases

IRC-Worm.Win32.Kromber (Kaspersky Lab) is also known as: IRC-Worm.Kromber (Kaspersky Lab), W32/Kromber!irc (McAfee), W32.Kromber (Symantec), W32/Kromber-A (Sophos), Win32/HLLW.Kromber.A (RAV), WORM_KROMBER.A (Trend Micro), Worm/Kromber (H+BEDV), W32/Kromber.A (FRISK), IRC-Worm/Kromber.A (Grisoft), Win32.HLLW.Kromber.A (SOFTWIN), Worm.Kromber.A (ClamAV), Trj/Kromber.A (Panda), Win32/Kromber.A (Eset)

Description added	Sep 30 2003
Behavior	IRC Worm

Technical details

This worm Trojan spreads via IRC channels, and is 3584 bytes in size.

Propagation

When launching, the worm checks for an active IRC client on the victim machine. If it finds this, the worm will send a link to a remote site to all accessible IRC channels by using the /amsg command:

```
 http://www.kromberg.at/[censored]/show.php?f=drunkchicks.jpg
LOL
```

It also attempts to install this link as the name of a channel and comments to it.

If another user clicks on this link, the remote site will be contacted. This site contains a malcious VBS script (which will be detected by Kaspersky Anti-Virus as TrojanDropper.VBS.Inor.h). This will install and launch the worm's executable file, named browsercheck.exe on the victim machine.

IRC-Worm.Win32.Lucky

Aliases

IRC-Worm.Win32.Lucky (Kaspersky Lab) is also known as: IRC-Worm.Lucky (Kaspersky Lab), IRC/Clickit.gen (McAfee), Backdoor.Trojan (Symantec), Win32.Bumblebee.4096 (Doctor Web), W32/Nbc (Sophos), Win32/Locky.worm (RAV), PE_WORM.NETBUS (Trend Micro), TR/IRC-Worm.Lucky (H+BEDV), IRC/Lucky.C (FRISK), Win32:NetBus-17 (ALWIL), IRC-Worm/Lucky (Grisoft), IRC-Worm.Lucky.A (SOFTWIN), Trojan.Netbus.KeyHook170 (ClamAV), IRC/Lucky (Panda), IRC-Worm.Lucky (Eset)

Description added	Feb 19 2002
Behavior	IRC Worm

Technical details

This is a IRC worm that spreads through the IRC channel using mIRC and PIRCH clients for spreading. The worm appears on a computer as the LK7.EXE Windows program about 500K in length. When this file is executed by a user, the worm installs itself into the system, copies the LK7.EXE to the C:\WINDOWS directory, then searches for mIRC and PIRCH clients in current, C:\MIRC, C:\MIRC32, C:\PIRCH98 directories, and modifies IRC scripts there.

The worm also installs the ""Backdoor.NetBus" Trojan to the system. To do this, the worm keeps the Trojan's code in its body, extracts it from there, copies to the C:\WINDOWS directory with IRCPATCH.EXE name, and executes it.

The worm contains the "copyright" text:

> LUCKY B.R.D 1994-99 [LK-7]...

To spread through mIRC channel the worm creates the new script file LK7.INI and sets a reference to this file in the mIRC system script file MIRC.INI. The worm's script intercepts a set of events and uses them to spread its copy to channels and manifest itself:

- on a new user joining infected channel, or on files transfer the worm sends its copy (the C:\WINDOWS\LK7.EXE file) to this user.
- if the text "leave!!!" appears in channel, the worm sends to the channel the message "Your will is my command" and leaves the channel.
- on "LUCKY !!" text the worm sends to the channel the message "I am a Lamer !!" and changes affected user's nick to "Lamer".
- on "Die!!!" text the worm reacts with the "Be sure, I will commit suicide now .. RIP" message and leaves chat.
- on "virus" and "virii" strings the virus sends to the channel the text I am infected with [LK-7]..By LUCKY B.R.D 1994-99.Win32 VIRUS".

and so on.

To spread its copy to mIRC channels, the worm also modifies the system registry keys that are responsible for mIRC events, and in some events, the worm also sends its copy to channels.

To spread to PIRCH, the worm creates the new script file EVENTS.INI that contains a command that sends a worm copy to all users that enter the infected channel.

Variants

There are several known variants of the original worm. They are crippled (infect only the mIRC client, for instance) and do not install backdoor files. They spread as files with the names:

> **"Lucky.b"**: CLICK-IT.EXE
> **"Lucky.c"**: APPOLO.EXE

IRC-Worm.Win32.Tetris

Aliases

IRC-Worm.Win32.Tetris (Kaspersky Lab) is also known as: IRC-Worm.Tetris (Kaspersky Lab), VBS/Wally.worm (McAfee), W32.Tetris.Worm (Symantec), VBS/Wally-A (Sophos), VBS/Tetris* (RAV), VBS_WALLY_TRIS (Trend Micro), Worm/IRC.Tetris.2 (H+BEDV), VBS/Tetris.A (FRISK), VBS:Malware (ALWIL), VBS.Tetris.A (SOFTWIN), IRC/Tetris.A (Panda), VBS/Tetris (Eset)

Description added	Feb 06 2002
Behavior	IRC Worm

Technical details

This is an IRC worm that spreads via IRC channels. The worm itself is a Win32 application about 70Kb in size. It has two main routines: infection and game, both of which are activated upon infected-program running. The first one infects a computer so that it will spread the worm copies further to IRC chats; the second one displays a "Tetris" game that is used to mask the worm's activity: this routine emulates real and complete "Tetris"-like game.

To spread itself, the worm looks for an mIRC client in four directories:

C:\Mirc
C:\Program Files\mirc
D:\mirc D:\Program Files\mirc

If one is found, the worm creates additional files:

C:\Windows\script.bak - mIRC script program
C:\backup.vbs - VBS program that later will complete installation
C:\Windows\system.exe - copy of worm EXE file

The "C:\backup.vbs" is then registered in the auto-run registry key as:

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run
SysFile = C:\Backup.vbs

As a result, it is run each time the system starts up, and then copies files:

C:\Windows\script.bak to mIRC directory with "script.ini" name
C:\Windows\system.exe to C:\tetris.exe

The "script.ini" file is a short mIRC program that sends C:\tetris.exe file to everybody who enters infected channel.

Net-Worm.Linux.Adm

Aliases

Net-Worm.Linux.Adm (Kaspersky Lab) is also known as: Worm.Linux.Adm (Kaspersky Lab), Linux/Adm.worm (McAfee), Unix/AdmWorm (Sophos), SH/Admworm.A* (RAV), UNIX_ADMWORM.A (Trend Micro), Unix/Admworm.A (FRISK), UNIX:Malware (ALWIL), Worm Generic (Panda)

Description added	May 31 2001
Behavior	Internet Worm

Technical details

This is the worm infecting Linux systems. The worm was discovered in spring 1998. It spreads itself from system to system by using a Linux security breach (so called "buffer overrun" breach) that allows to upload to remote system and run there a short piece of code that then downloads and activates the main worm component.

The worm uses a security breach in the program package BIND (Berkeley Internet Name Domain), which is distributed in many popular UNIX packages and provides name service for the internet.

The Worm Itself

This is multi-component worm that consist of 8 files. These files are script programs and executable files. The script programs are ".sh" files that are run by Linux command shell. The executable files are standard Linux ELF executables.

The main components of the worm are script ".sh" files that are run as hosts, and then run the rest files (additional ".sh" files and ELF executables) to perform necessary actions.

The list of components looks as follows:

```
ADMw0rm            Hnamed
gimmeIP            remotecmd
gimmeRAND          scanco
incremental        test
```

Spreading

The spreading (infecting a remote Linux machine) is done by "buffer overrun" attack. That attack is performed as a special packet that is sent to a machine being attacked. The packet has a block of specially prepared data. That block of packet's data is then executed as a code on that machine. That code opens a connection to infected machine, gets the rest of worm code and activates it. At that moment the machine is infected, and starts to spread worm further.

The worm is transferred from a machine to machine as a "tgz" archive (standard UNIX archive) with "ADMw0rm.tgz" name, with 8 worm components inside. While infecting a new machine the worm unpacks that package in there, and runs the main "ADMw0rm" file that then will activate other worm's components.

Details

To get IP addresses of remote machines to attack them the worm scans the available global network for IP addresses with computers and DNS installed servers on it.

To attack remote system the worm uses security vulnerabilities in Linux demon: "named".

To upload and activate its copy on remote machine the worm "buffer overrun" code contains the instructions that switch to "root" privileges, runs command shell and follows the commands:

- runs the deamon "/usr/sbin/named"
- creates the directory to download the worm "tgz" file, the directory name is "/tmp/.w0rm0r"
- runs "ftp" (standart Linux program) that downloads worm "tgz" file from host machine (machine the worm is spreading from)
- unpacks all worm components from "tgz" archive
- runs the worm startup component: the "ADMw0rm" file

Misc.

The worm has several payload and other non-infection routines.

First of all it finds on local machine starting from root directory all "index.html" files (Web servers start pages) and replaces them with its own "index.html" file that contains the text:

> The ADM Inet w0rm is here !

The worm deletes the "/etc/hosts.deny" file. That file contains the list of hosts (addresses and/or Inet names) that are denied to access this system (in case so-called TCP wrapper is used). As a result any of restricted machines can access affected system.

When a new system is infected, the worm sends "notification" messages to the e-mail address "admsmb@hotmail.com".

Net-Worm.Linux.Cheese

Aliases

Net-Worm.Linux.Cheese (Kaspersky Lab) is also known as: Worm.Linux.Cheese (Kaspersky Lab), Linux/Cheese.worm (McAfee), Linux.Cheese.Worm (Symantec), Linux/Cheese (Sophos), Worm:Linux/Cheese* (RAV), PERL_CHEESE.A (Trend Micro), Linux/Cheese.CHEESE (H+BEDV), Unix/Cheese (FRISK), UNIX:Malware (ALWIL), Worm.Linux.Cheese (SOFTWIN), Worm Generic (Panda), Linux/Cheese.A (Eset)

Description added	May 28 2001
Behavior	Internet Worm

Technical details

Text written by Costin Raiu, Kaspersky Lab, Romania

This is an Internet worm that replicates between systems that were previously hacked by the "Ramen" Linux worm, and not the "Lion" or "Adore" worms as it is stated in other various descriptions, or the worm itself. (see the text below) "Cheese" will also act as a "security patch" that removes the backdoors added by previous attacks, but it will not remove or patch the vulnerabilities used to hack the respective systems; thus, the machines will still remain vulnerable to the original attack(s) used to compromise them. The worm contains the following text:

> # removes rootshells running from /etc/inetd.conf
> # after a l10n infection... (to stop pesky haqz0rs
> # messing up your box even worse than it is already)
> # This code was not written with malicious intent.
> # Infact, it was written to try and do some good.

No matter how good the original intention of the author was, "Cheese" remains a piece of replicative "malware" that eats up resources such as CPU, memory, disk space or Internet bandwidth from infected systems; thus, remaining a "bad thing".

Technical details

The worm consists of three program files named "cheese", "go" and "psm". "go" is the worm's "entrypoint", that basically executes the main worm body, "cheese", in such a way that makes it immune to signals, which might attempt to halt it. "cheese", a 2Kylobytes-long Perl script, is the main part of the worm, the one responsible for the replication.

When run, it will first scan "/etc/inetd.conf" for services attempting to execute "/bin/sh", mostly root-shell backdoors, and remove them. Obviously, if a root shell has been added to the newer-style "/etc/xinetd.conf", the worm will not notice it, and leave it untouched.

Next, it will generate a random 16-bit IP base, such as "a" and "b" in the "a.b.x.y", then it will use an external Linux ELF program to scan the respective Internet IP class for hosts listening on port 10008. Usually, these are hosts that have been previously hacked by the "Ramen" worm, hosts that run an open root shell on the respective port.

So, when such a host is found, the worm will execute a small installation script on the remote host that will create a directory named "/tmp/.cheese", and it will launch an instance of the popular Lynx browser to download a copy of the worm from the infected system. The worm itself will listen for the connection attempt on the source system, and forward an UUE-encoded copy of itself to the remote caller. The installation script running on the target system will decode the worm body, unpack it in the "/tmp/.cheese" directory, and eventually execute the "go" script to launch the worm, which propagates the infection further.

Net-Worm.Linux.Lupper.a

Detection added	Nov 07 2005 04:54 GMT
Description added	Aug 21 2006
Behavior	Net-Worm

Technical details

This malicious program spreads as an ELF format file and represents a threat to Linux web servers.

The worm spreads via the following vulnerabilities:

- AWStats Rawlog Plugin Logfile Parameter Input Validation Vulnerability (Bugtraq 10950);
- XML-RPC for PHP Remote Code Injection Vulnerability (Bugtraq ID 14088);
- Darryl Burgdorf Webhints Remote Command Execution Vulnerability (Bugtraq ID 13930).

The following applications contain the vulnerabilities:

```
b2evolution
Drupal
PHPGroupWare
PostNuke
TikiWiki
WordPress
Xoops
```

These vulnerabilities were corrected in later versions of the programs.

A range of commands will be executed on the server via the vulnerabilties. First, a copy of the worm will be downloaded using wget from a fixed address. This copy of the worm will be saved to the /tmp directory as "lupii". Then an executable bit will be set using the chmod command, and the executable file itself will be launched.

In addition to the above, a backdoor will be installed on UDP port 7222 on the compromised server in order to receive commands.

The worm generates a list of URLs which contain the following strings:

```
/awstats/
/b2/xmlsrv/xmlrpc.php
/b2evo/xmlsrv/xmlrpc.php
/blog/xmlrpc.php
/blog/xmlsrv/xmlrpc.php
/blogs/xmlrpc.php
/blogs/xmlsrv/xmlrpc.php
/blogtest/xmlsrv/xmlrpc.php
/cgi/awstats/
/cgi/hints.cgi
/cgi/hints.pl
/cgi/includer.cgi
/cgi-bin/
/cgi-bin/awstats/
/cgi-bin/hints.cgi
/cgi-bin/hints.pl
/cgi-bin/hints/hints.cgi
/cgi-bin/hints/hints.pl
/cgi-bin/inc/includer.cgi
/cgi-bin/include/includer.cgi
/cgi-bin/includer.cgi
/cgi-bin/stats/
/cgi-bin/webhints/hints.cgi
/cgi-bin/webhints/hints.pl
/cgi-local/includer.cgi
/community/xmlrpc.php
/drupal/xmlrpc.php
/hints.cgi
/hints.pl
/hints/hints.cgi
/hints/hints.pl
/includer.cgi
/phpgroupware/xmlrpc.php
/scgi/awstats/
/scgi/hints.cgi
/scgi/hints.pl
/scgi/includer.cgi
/scgi-bin/
/scgi-bin/awstats/
/scgi-bin/hints.cgi
/scgi-bin/hints.pl
/scgi-bin/hints/hints.cgi
/scgi-bin/hints/hints.pl
/scgi-bin/inc/includer.cgi
/scgi-bin/include/includer.cgi
/scgi-bin/includer.cgi
/scgi-bin/stats/
/scgi-bin/webhints/hints.cgi
```

```
/scgi-bin/webhints/hints.pl
/scgi-local/includer.cgi
/scripts/
/stats/
/webhints/hints.cgi
/webhints/hints.pl
/wordpress/xmlrpc.php
/xmlrpc.php
/xmlrpc/xmlrpc.php
/xmlsrv/xmlrpc.php
```

This list is used to infect other hosts.

Net-Worm.Linux.Mighty

Aliases

Net-Worm.Linux.Mighty (Kaspersky Lab) is also known as: Worm.Linux.Mighty (Kaspersky Lab), Linux/Mighty.worm (McAfee), Linux.Slapper.D (Symantec), Linux.Slapper.19050 (Doctor Web), Linux/Devnull-A (Sophos), Linux/Mighty.worm (RAV), ELF_MIGHTY.A (Trend Micro), Unix/Mighty.A (FRISK), ELF:Malware (ALWIL), Linux/Mighty.A (Grisoft), Linux.Worm.Slapper.D (SOFTWIN), Linux/Slapper.D (Panda), Linux/Mighty.A (Eset)

Description added	Oct 04 2002
Behavior	Internet Worm

Technical details

"Mighty" is an Internet worm that infects Linux machines running the popular "Apache" web server software. It does that by exploiting a vulnerability in the "Secure Sockets Layer" SSL "mod_ssl" interface code of the server which was originally reported on July 30, 2002, and listed by the Computer Emergency Response Team (CERT) as the Vulnerability Note VU#102795.

The configurations vulnerable to the specific exploit implementation used by the worm are Intel x86 Linux Apache installations with OpenSSL older than 0.9.6e and 0.9.7-beta. Updating to one of these two versions or other more recent releases will patch the vulnerability and prevent the worm from infecting the system.

The main worm replication component is about 19KB in size, and uses the exploit code from the popular "Slapper" worm.

Besides infecting more computers to spread further, the worm will also act as a backdoor on the victim system, connecting to an IRC server and joining a special channel from where it receives the orders. It's worth noticing the backdoor component of the worm is based on the popular 'Age of Kaiten' IRC bot source, used in many other IRC malware.

At the time of writing of this description, the worm is reported to have infected around 1600 systems worldwide.

Net-Worm.Linux.Ramen

Aliases

Net-Worm.Linux.Ramen (Kaspersky Lab) is also known as: Worm.Linux.Ramen (Kaspersky Lab), Linux/Lion.worm.a (McAfee), Linux.Lion.Worm (Symantec), Linux.Ramen (Doctor Web), Linux/Ramen-A (Sophos), Worm:Linux/Ramen (RAV), ELF_RAMEN.10 (Trend Micro), Linux/LionWorm.2 (H+BEDV), Unix/Lion (FRISK), ELF:Malware (ALWIL), Linux/Ramen.F (Grisoft), Worm.Linux.Ramen (SOFTWIN), Worm.Linux.Ramen (ClamAV), Lion (Panda), Ramen (Eset)

Description added	Jan 22 2001
Behavior	Internet Worm

Technical details

This is the first known worm infecting RedHat Linux systems. The worm was discovered in the middle of January 2001. The worm spreads itself from system to system by using a RedHat security breach (a so-called "buffer overrun" breach) that allows for uploading to a remote system and running a short piece of code there that then downloads and activates the main worm component.

The worm has not been tested in VirusLab, so all information below should be read as "the worm could do, if it really does work." We also have no confirmed reports about infected servers from our customers.

The worm uses three security breaches in RedHat versions 6.2 and 7.0, these breaches were discovered in summer-autumn 2000, at least three monthes before the worm was discovered.

The worm also contains routines that intend to attack FreeBSD and SuSE machines, but these routines are neither activated, nor used in worm code.

The Worm Itself

This is a multi-component worm that consists of 26 files about 300K in total length. These files are script programs and executable files. The script programs are ".sh" files that are run by a Linux command shell (like DOS BAT files and Windows CMD files). The executable files are standard Linux ELF executables.

The main components of the worm are script ".sh" files that are run as hosts, and then run the rest of the files (additional ".sh" files and ELF executables) to perform necessary actions.

The list of components appears as follows:

```
asp         hackl.sh     randb62     start62.sh  wh.sh
asp62       hackw.sh     randb7      start7.sh   wu62
asp7        index.html   s62         synscan62
bd62.sh     l62          s7          synscan7
bd7.sh      l7           scan.sh     w62
getip.sh    lh.sh        start.sh    w7
```

The "62" components are activated under RedHat 6.2 systems, the "7" components are activated under RedHat 7.0. The "wu62" file is not used at all.

Spreading

Spreading (infecting a remote Linux machine) is done by a "buffer overrun" attack. This attack is performed as a special packet that is sent to a machine being attacked. The packet has a block of specially prepared data. That block of packet data is then executed as a code on that machine. This code opens a connection to an infected machine, obtains the rest of the worm's code, and activates it. At this moment, the machine is infected, and starts to spread the worm further.

The worm is transferred from machine-to-machine as a "tgz" archive (standard UNIX archive) with a "ramen.tgz" name, with 26 worm components inside. While infecting a new machine, the worm unpacks the package there, and runs the main "start.sh" file that then activates other worm components.

The worm components then scan the global network for other Linux machines and upload the worm there if the "buffer overrun" attack is performed successfully.

The worm also appends a command to run its starting ".sh" file to a "/etc/rc.d/rc.sysinit" file, and as a result, the worm's components are activated upon each followed system start.

The worm also closes security breaches that have been used to infect the system. So, an infected machine cannot be attacked by the worm twice.

Details

To obtain IP addresses of remote machines in order to attack them, the worm scans the available global network for IP addresses; i.e., operates similar to standard "sniffer" utilities.

To attack a remote system, the worm uses security vulnerabilities in three RedHat Linux demons: "statd", "lpd", and "wu-ftp".

To upload and activate its copy on a remote machine, the worm "buffer overrun" code contains instructions that switch to "root" privileges, runs a command shell, and follows the ensuing commands:

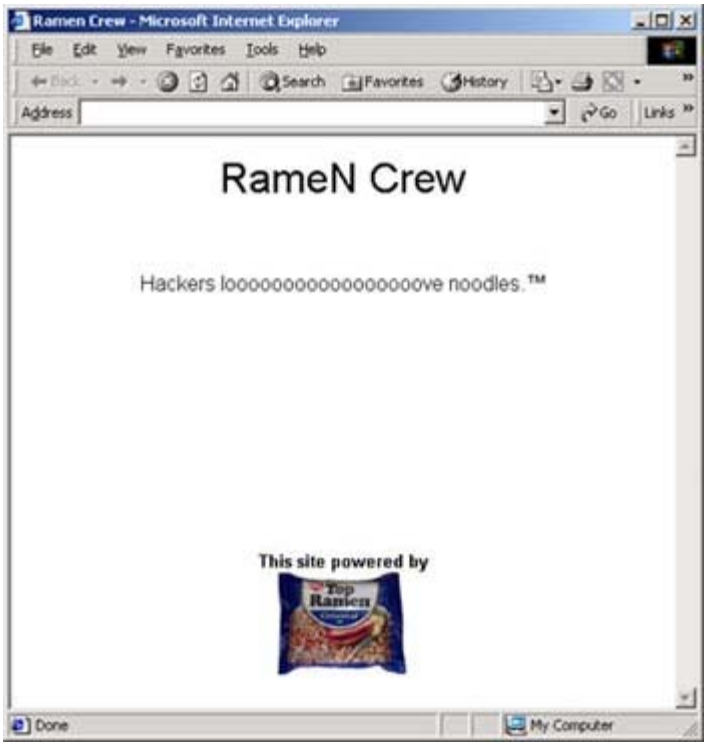
- creates a directory to download the worm "tgz" file, the directory name is "/usr/src/.poop"
- exports a "TERM=vt100" variable that is necessary for the next step
- runs "lynx" (simply WWW browser) that downloads a worm "tgz" file from a host machine (the machine from which the worm is spreading)
- unpacks all worm components from a "tgz" archive
- runs the worm startup component: the "start.sh" file

To send a "ramen.tgz" archive, the worm runs an additional server "asp" that sends the worm's "tgz" archive by request from a worm "buffer overrun" component.

Misc.

The worm has several payload and other non-infectious routines.

First of all, it finds all "index.html" files (a Web server's starting pages) on a local machine starting from the root directory and replaces them with its own "index.html" file that contains the following text:



The worm deletes the "/etc/hosts.deny" file. This file contains a list of hosts (addresses and/or Internet names) that are denied access to this system (in case a so-called TCP wrapper is used). As a result, any of the restricted machines can access an affected system.

When a new system is infected, the worm sends "notification" messages to three e-mail addresses:

1. the address of just the infected machine
2. gb31337@hotmail.com

3. gb31337@yahoo.com

The message Subject is IP address of infected machine, the message body contains the text:

> Eat Your Ramen!

Net-Worm.Linux.Slapper.a

Aliases

Net-Worm.Linux.Slapper.a (Kaspersky Lab) is also known as: Worm.Linux.Slapper.a (Kaspersky Lab), Linux/Slapper.worm.a (McAfee), Linux.Slapper.Worm (Symantec), Linux/Slapper-A (Sophos), Worm:Linux/Slapper* (RAV), ELF_SLAPPER.A (Trend Micro), UNIX/Slapper.A (FRISK), SRC:Malware (ALWIL), Linux.Worm.Slapper.A (SOFTWIN), Linux.Slapper-A (ClamAV), Linux/Slapper (Panda), Linux/Slapper.A (Eset)

Description added	Sep 18 2002
Behavior	Internet Worm

Technical details

"Slapper" is an Internet worm that infects Linux machines running the popular "Apache" web server software. It does that by exploiting a vulnerability in the "Secure Sockets Layer" SSL "mod_ssl" interface code of the server which was originally reported on July 30, 2002, and listed by the Computer Emergency Response Team (CERT) as the Vulnerability Note VU#102795. (http://www.kb.cert.org/vuls/id/102795)

The configurations vulnerable to the specific exploit implementation used by the worm are Intel x86 Linux Apache installations with OpenSSL older than 0.9.6e and 0.9.7-beta. Updating to one of these two versions or other more recent releases will patch the vulnerability and prevent the worm from infecting the system.

The worm source is approximately 68.4KBytes in size, and has some similarities with the "I-Worm.Scalper" reported earlier this year, which also hit Apache servers through a buffer overflow exploit.

Besides infecting more computers to spread further, the worm will act as a backdoor on the victim, and allow any potential attacker to run commands as well for launch various types of Denial-Of-Service attacks through a distributed network aintained between the infected machines.

Technical details of the "Slapper" worm

Like in the case of the older "Scalper" worm, the attacks are mounted against randomly-generated IP address classes of the format a.b.x.x, where "a" is selected from an array of 162 possible choices, "b" is a full 1-byte long random choice, and "x.x" are scanned incrementally from "0.0" up to "255.255". For each random IP address, the worm checks if it doesn't loop back to the local machine (eg. addresses of the form 127.x.x.x), then it tries to connect on port 80 and send a simple "GET /" request to check if the server runs an Apache version. Next, the worm will check if the specific Apache version reported in the HTTP headers match any of the versions it knows to infect, and if so, proceed further. In the case an Apache server was detected, but the apparent version returned is unknown to the worm, the selection for "Red-Hat 1.3.26" will be tried anyway.

The complete list of Linux distributivs with Apache versions the worm knows how to "correctly" infect is the following:

> (Apache): "Gentoo", "Debian 1.3.26", "Red-Hat 1.3.6", "Red-Hat 1.3.9", "Red-Hat 1.3.12", "Red-Hat 1.3.12", "Red-Hat 1.3.19", "Red-Hat 1.3.20", "Red-Hat 1.3.26", "Red-Hat 1.3.23", "Red-Hat 1.3.22", "SuSE 1.3.12", "SuSE 1.3.17", "SuSE 1.3.19", "SuSE 1.3.20", "SuSE 1.3.23", "SuSE 1.3.23", "Mandrake 1.3.14", "Mandrake 1.3.19", "Mandrake 1.3.20", "Mandrake 1.3.23", "Slackware 1.3.26" and "Slackware 1.3.26".

So, if the web server reply includes the "Apache" string, the worm will attempt to exploit the SSL vulnerability by first "shaking hands" with the SSL server on port 443, then if the exploit was successful, it will UUENCODE a copy of its source, upload it through the hacked connection in the victim server, compile and then run it. During this process, the UUENCODED copy of the worm will be saved as "/tmp/.uubugtraq", the clear-text source of the worm as "/tmp/.bugtraq.c", and the compiled binary will be stored as "/tmp/.bugtraq".

When run on the victim server, the worm will again enter the replication cycle, looking for more hosts, and activating the backdoor component on the UDP port 2002. No provision is taken against server reboots, as the worm doesn't try to set itself up so that it would receive control every time the system is restarted.

The backdoor accepts a rather large set of commands, between them, flooding remote systems with UDP, TCP, DNS or RAW packets, running local commands, downloading a binary from a remote machine via HTTP and running it, sending mails, providing information on the configuration of the hacked machine, etc... All the communication with the backdoor is encrypted, however, the encryption is static and is probably performed only to prevent direct analysis of the traffic.

As an interesting detail, the worm will attempt to create and maintain a communication network between infected machines, each node having the ability to receive and forward commands. This allows a malevolent "master" to mount a distributed DoS attack in which the single "order" of attack

is executed and passed along by all the network participants.

Another interesting detail is that the worm contains a "version" tag, which in this version of "Slapper" is set to "12.09.2002". A similar tag in the previous "Scalper" worm was "26.04.2002".

The following comments, presumably from the author can be seen inside the worm source:

```
 /*****************************************************************************
 *
 *           Peer-to-peer UDP Distributed Denial of Service (PUD)
 *
 *                         by contem@efnet
 *
and

 *         I am not responsible for any harm caused by this program!
 *
 *  I made this program to demonstrate peer-to-peer communication and  *
 *  should not be used in real life.  It is an education program that
 *
 *  should never even be ran at all, nor used in any way, shape or
 *
 *  form.  It is not the authors fault if it was used for any purposes
 *
 *  other than educational.
 *
```

Net-Worm.Perl.Santy.a

Aliases

Net-Worm.Perl.Santy.a (Kaspersky Lab) is also known as: Perl.Santy (Symantec), Perl/Santy-A (Sophos), Perl/Santy.A.worm* (RAV), PERL_SANTY.A (Trend Micro), Perl/Santy.A.2 (H+BEDV), Unix/Santy.A (FRISK), PERL/Santy (Grisoft), Worm.PhpBB.Santy.A (SOFTWIN), PHP/Santy.gen (Panda), Perl/Santy.A (Eset)

Detection added	Dec 21 2004
Description added	Dec 21 2004
Behavior	Net-Worm

Technical details

This worm uses a vulnerability in phpBB, which is used to create forums and web sites, to spread via the Internet. phpBB versions lower than 2.0.11 are vulnerable.

The worm is written in Perl, and is 4966 bytes in size.

Propagation

The worm creates a specially formulated Google search request. This request will give a list of sites running vulnerable versions of phpBB. The worm then sends a request to all sites found, which contains an exploit for the vulnerability. When the server under attack processes the exploit, the worm penetrates the site and gains control. This process is then repeated.

The worm scans all site directories, and overwrites files with the following extensions:

```
.asp
.htm
.jsp
.php
.phtm
.shtm
```

with the following text:

```
This site is defaced!!!

This site is defaced!!!
NeverEverNoSanity WebWorm generation
```

Using MSN to search for sites containing the above strings gives an extensive list of sites; evidence that Santy.a is currently causing an epidemic.

Users should note that this worm is not dangerous; it will not infect computers if users view an infected site.

Net-Worm.Win32.Aler.a

Aliases

Net-Worm.Win32.Aler.a (Kaspersky Lab) is also known as: Worm.Win32.Aler.a (Kaspersky Lab), W32.Scard (Symantec), Win32.HLLW.Golten (Doctor Web), W32/Mofei-E (Sophos), Worm:Win32/Golten.A (RAV), WORM_GOLTEN.A (Trend Micro), Worm/Aler.A.5 (H+BEDV), W32/Aler.A (FRISK), Worm/Aler.D (Grisoft), Win32.Mofei.E (SOFTWIN), W32/Aler.A.worm (Panda), Win32/Golten.A (Eset)

Description added	Nov 25 2004
Behavior	Internet Worm

Technical details

This worm contains a backdoor function. It has been widely spammed via email. However, it does not spread via email, but via network resources with weak password protection.

Infected messages

Message subject

```
Latest News about Arafat!!!
```

Message body

```
Hello guys!
Latest news about Arafat!
Unimaginable!!!!!
```

Attachment name

Infected messages have two files attached. The first is a normal JPEG file:

```
arafat_1.emf
```

The second file is called

```
arafat_2.emf
```

It is specially constructed to exploit an EMF vulnerabilty. More information on this vulnerability can be found in Microsoft Security Bulletin MS04-032

Installation

Once the infected file has been launched, the worm creates the following files in the Windows system folder:

```
Alerter.exe
Comwsock.dll
Dmsock.dll
Mst.tlb
SCardSer.exe
Spc.exe
Spoolsv.exe
Sptres.dll
```

The worm masks its presence in the system by adding itself to Windows processes which are already running, such as explorer.exe, lsass.exe, outlook.exe.

Aler.a creates the following entries in the system registry:

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\netlog]
'Display name': "Net Login Helper"
'ImagePath': %System%\SCardSer.exe
```

Propagation

The worm scans random IP addresses, trying to find victim machines that are running Windows, and have weak password protection. Aler.a uses the following passwords to penetrate systems:

```
0                       !@#$%^
0                       ~!@#
111                     123!@#
123                     1234!@#$
1234                    12345!@#$%
12345                   admin
54321                   fan@ing*
111111                  oracle
123456                  pass
654321                  passwd
888888                  password
1234567                 root
11111111                secret
12345678                security
88888888                stgzs
!@#$                    super
!@#$%
```

The worm then copies itself to the victim computer as Alerter.exe or Alerter16.exe.

Payload

The worm opens a random TCP port and tracks port activity. This open port is used to receive remote commands and files.

Net-Worm.Win32.Allaple.a

Detection added	Dec 07 2006 15:08 GMT
Description added	Aug 08 2007
Behavior	Net-Worm

Technical details

The worm spreads via local networks. It is a Windows PE EXE file. The file is 57,856 bytes in size.

Installation

The worm copies its executable file to the Windows system directory:

```
%System%\urdvxc.exe
```

In order to ensure that the worm is launched automatically when the system is rebooted, the Trojan registers its executable file in the system registry:

```
[HKCR\CLSID\{31D89687-B459-9FEE-EC54-AA92A8105F56}\LocalServer32]

@ = "%System%\urdvxc.exe"

[HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices]

@ = "%System%\urdvxc.exe"
```

The worm also creates a service called "MSWindows" and the alias "Network Windows Service", which will launch the worm's executable file:

```
%System%\urdvxc.exe /service
```

Propagation

The worm gets a list of accessible computers in the surrounding network and conducts buffer overflow attacks on them using the DCOM RPC vulnerability. If the vulnerability is successfully exploited, the worm sends a very small downloader to the victim machine, which in turn downloads and launches the worm's main file.

The worm also attempts to connect to the administrator account on networked computers by using the following passwords:

```
www windows visitor test2 password test1 test temp telnet ruler remote real random qwerty public private poiuytre
passwd pass oracle nopass nobody nick newpass new network monitor money manager mail login internet install hello
guest go X demo default debug database crew computer coffee bin beta backup backdoor anonymous anon alpha adm
access abc123 system sys super sql shit shadow setup security secure secret 123456789 12345678 1234567 123456 12345
1234 123 12 1 00000000 0000000 000000 00000 0000 000 00 server asdfgh root
```

If the worm manages to establish a connection, it will copy its executable file to the Windows system directory (%System%) on the victim machine.

Payload

The worm searches for files with a .htm extension, and harvest email addresses from these files. Harvested addresses are sent to the remote malicious user's site.

The worm is also able to download files from the Internet and launch them for execution on the victim machine.

Removal instructions

If your computer does not have an up-to-date antivirus, or does not have an antivirus solution at all, follow the instructions below to delete the malicious program:

1. Use Task Manager to terminate the backdoor process.

2. Delete the original worm file (the location will depend on how the program originally penetrated the victim machine).
3. Delete the following parameters from the system registry (see What is a system registry and how do I use it for details on how to edit the registry).

```
[HKCR\CLSID\{31D89687-B459-9FEE-EC54-AA92A8105F56}\LocalServer32]

@ = "%System%\urdvxc.exe"

[HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices]

@ = "%System%\urdvxc.exe"
```

4. Delete the following file:

```
%System%\urdvxc.exe
```

5. Delete the following service:

```
Network Windows Service
```

6. Update your antivirus databases and perform a full scan of the computer (download a trial version of Kaspersky Anti-Virus).

Net-Worm.Win32.BlueCode

Aliases

Net-Worm.Win32.BlueCode (Kaspersky Lab) is also known as: IIS-Worm.BlueCode (Kaspersky Lab), W32/CodeBlue.worm (McAfee), W32.BlueCode.Worm (Symantec), W32/CodeBlue (Sophos), VBS/BlueCode* (RAV), VBS_BLUECODE.A (Trend Micro), Worm/BlueCode (H+BEDV), VBS/BlueCode.A (FRISK), VBS:CodeBlue (ALWIL), CodeBlue (Grisoft), VBS.Trojan.CodeBlue (SOFTWIN), W32.Worm.CodeBlue (ClamAV), IIS-Worm/BlueCode (Panda), Win32/BlueCode (Eset)

Description added	Sep 07 2001
Behavior	Net-Worm

Technical details

This is an Internet worm that targets Web sites by infecting Internet Information Servers (ISS). The worm perpetrates this method of spreading from one Web site to another by sending and executing its EXE file.

The name of the worm's files are consistant - SVCHOST.EXE and HTTPEXT.DLL. The EXE file is a Win32 application (PE EXE file) about 29K in length, and it is written in Microsoft C++. There also was a compressed variant discovered, which is about 14K in size. The DLL file is about 47K in size, and it is written in Microsoft C++.

Note that the worm uses standard Win32 EXE file names. SVCHOST.EXE and HTTPEXT.DLL can be found in standard Win2000 installations in the SYSTEM32 subfolder.

The worm infects only machines installed with the IIS package and Web site contents. The worm application, upon being run on a such machine, locates and infects remote Web sites (remote machines with installed IIS package): it enters them and, by using a Web Directory Traversal exploit, sends its copy there, and spawns that copy. As a result, the worm infects all vlunerable Web servers that can be accessed from current a infected machine, and other infected servers spread the worm copy further, and so on.

The worm has a payload routine that, from 10:00 am till 11:00 am global time, performs a DoS attack (Deny of Service) on the http://www.nsfocus.com Web server.

Installing

The worm creates its copies (EXE and DLL) in the root of C: drive - C:\SVCHOST.EXE and C:\HTTPEXT.DLL. This EXE file is then registered in the Registry auto-run key:

> HKLM\Software\Microsoft\Windows\CurrentVersion\Run
> Domain Manager = C:\svchost.exe

The worm then creates and swapns a C:\D.VBS script file, then looks for the INETINFO.EXE application and terminates it if it is active. The VBS script program also searches for Indexing Service, Indexing Query and printer mapping and removes them.

As a result, the worm disables security breaches that can be used (or were used) by other worms to infect the machine and/or hackers to break through the Web-security protections.

Spreading

To spread further, the worm runs 100 threads that scan randomly selected IP addresses and attacks them.

In 50% of the cases, the attacked machines are in the same network, and the attacked IP addresses are "aa.bb.??.??", where "aa.bb" is part of the infected machine IP address, and "??" are random.

In the other 50% of the cases, the attacked addresses are very random.

To attack a victim machine, the worm uses the Web Directory Traversal exploit three times:

1. it tries to determine the IIS directory on a remote machine,
2. then sends a request to the remote machine to download the DLL component of the virus (HTTPEXT.DLL file) from the infected one,
3. the last request is to copy that DLL file to the C: root directory.

To upload a DLL file to a victim machine, the worm uses a "tftp" command, and activates the temporary TFTP server on an infected (current)

machine to process a "get data" command from the victim (remote) machine.

When a DLL file is uploaded to the victim machine, it is activated by a trick. So, the worm copy starts on a remote server, then it drops and executes the EXE component that then spreads the virus futhrer.

Net-Worm.Win32.Bozori.a

Other versions: .b

Aliases

Net-Worm.Win32.Bozori.a (Kaspersky Lab) is also known as: Exploit-DcomRpc.gen (McAfee), Win32.HLLW.Stamin (Doctor Web), Win32.Worm.Zotob.D (SOFTWIN), Worm.Bozari.A (ClamAV), W32/IRCbot.KC.worm (Panda), Win32/Bozori.A (Eset)

Detection added	Aug 16 2005 21:11 GMT
Description added	Aug 17 2005
CME-ID	CME-540
Behavior	Net-Worm

Technical details

This network worm infects computers running Windows. The worm itself is a Windows PE EXE file 10366 bytes in size, written in C++ and packed using UPX. The unpacked file is approximately 20KB in size.

The worm spreads via a vulnerability in Microsoft Windows Plug and Play. Details of the vulnerability can be found in Microsoft Security Bulletin MS05-039.

Bozori functions in a similar way to Lovesan (August 2003) and Sasser (May 2004) in that it exploits a vulnerability analogous to those exploited by these two worms. Lovesan exploited a vulnerability in RPC DCOM, and Sasser exploited a vulnerability in LSASS.

Computers running Windows 2000 are particularly vulnerable. The worm is capable of functioning on machines running other versions of Windows, but is unable to infect them by penetrating via the vulnerability.

The worm contains a backdoor which receives commands via IRC channels.

Installation

Once launched, the worm copies itself to the Windows system directory as “wintbp.exe”:

```
%System%\wintbp.exe
```

It then registers this file in the system registry, ensuring that the worm file will be launched each time Windows is rebooted on the victim machine:

```
[HKLM\Software\Microsoft\Windows\CurrentVersion\Run]
"wintbp.exe" = "wintbp.exe"
```

The file which was originally launched will then be deleted.

The worm flags its presence in the system by creating a unique identifier: "wintbp.exe"

Propagation

The worm opens an TFTP server on the victim machine on UDP port 69. It then selects IP addresses to attack, and sends a request to TCP port 445. If the remote computer responds, the worm exploits the Plug and Play vulnerability, opens TCP port 8594 on the new victim machine and uploads a copy of itself to the new victim machine. It then launches this copy for execution.

Remote administration

Net-Worm.Win32.Bozori.a connects to IRC server 72.20.**.115 to receive commands. This provides the remote malicious user with complete access to the victim machine via IRC channels, making it possible to receive information from the infected computer, upload files, launch them and delete files.

Other

Once infected, the victim machine will display an error notification. The worm may then cause the infected computer to reboot.

Net-Worm.Win32.Bozori.b

Other versions: .a

Aliases

Net-Worm.Win32.Bozori.b (Kaspersky Lab) is also known as: Exploit-DcomRpc.gen (McAfee), Win32.HLLW.Stamin (Doctor Web), Worm.Mytob.Crypt.Gen (ClamAV), W32/IRCbot.KL.worm (Panda)

Detection added	Aug 16 2005 23:42 GMT
Description added	Aug 18 2005
CME-ID	CME-15
Behavior	Net-Worm

Technical details

This network worm infects computers running Windows. The worm itself is a Windows PE EXE file 10878 bytes in size, written in C++ and packed using UPX. The unpacked file is approximately 17KB in size.

The worm spreads via a vulnerability in Microsoft Windows Plug and Play. Details of the vulnerability can be found in Microsoft Security Bulletin MS05-039.

Bozori functions in a similar way to Lovesan (August 2003) and Sasser (May 2004) in that it exploits a vulnerability analogous to those exploited by these two worms. Lovesan exploited a vulnerability in RPC DCOM, and Sasser exploited a vulnerability in LSASS.

Computers running Windows 2000 are particularly vulnerable. The worm is capable of functioning on machines running other versions of Windows, but is unable to infect them by penetrating via the vulnerability.

The worm contains a backdoor which receives commands via IRC channels.

Installation

Once launched, the worm copies itself to the Windows system directory as “wintbp.exe”:

```
%System%\wintbpx.exe
```

It then registers this file in the system registry, ensuring that the worm file will be launched each time Windows is rebooted on the victim machine:

```
[HKLM\Software\Microsoft\Windows\CurrentVersion\Run]
"wintbpx.exe" = "wintbpx.exe"
```

The file which was originally launched will then be deleted.

Propagation

The worm searches for IP addresses to attack, and sends a request to TCP port 445. If the remote computer responds, the worm exploits the Plug and Play vulnerability, and launches itself for execution on the new victim machine.

Remote administration

Net-Worm.Win32.Bozori.b connects to IRC server 72.20.**.139 to receive commands. This provides the remote malicious user with complete access to the victim machine via IRC channels, making it possible to receive information from the infected computer, upload files, launch them and delete files.

Payload

The worm terminates processes with the following names:

```
botzor.exe
csm.exe
llsrv.exe
```

```
mousebm.exe
pnpsrv.exe
service32.exe
svnlitup32.exe
system32.exe
upnp.exe
winpnp.exe
wintbp.exe
```

Other

Once infected, the victim machine will display an error notification. The worm may then cause the infected computer to reboot.

Net-Worm.Win32.CodeGreen.a

Aliases

Net-Worm.Win32.CodeGreen.a (Kaspersky Lab) is also known as: IIS-Worm.CodeGreen.a (Kaspersky Lab), W32/CodeGreen.dr (McAfee), W32.CodeGreen.gen (Symantec), Win2K.CodeGreen.9216 (Doctor Web), Troj/Codegreen (Sophos), Win32/GreenCode.A@IIS (RAV), WORM_CODEGREEN.A (Trend Micro), Worm/CodeGreen.A (H+BEDV), Win32:Trojan-gen. (ALWIL), CodeGreen (Grisoft), Exploit.CodeGreen (SOFTWIN), Worm.CodeGreen.A (ClamAV), IIS-Worm/GreenCode (Panda), CodeGreen (Eset)

Description added	Sep 14 2001
Behavior	Net-Worm

Technical details

This is an Internet worm that targets Web sites by infecting Internet Information Servers (ISS). The worm completes the method of spreading from one Web site to other Web sites by sending and executing its code on remote machines in a similar way to the "CodeRed" IIS worm.

This worm, like the "CodeRed" worm, randomly scans IP addresses and attacks remote IIS servers by using a buffer-overrun exploit.

The main feature of this worm is its "anti-worm" functions. Upon being run on infected machines, it cleans-up and:

- erases traces of the "CodeRed" worm, then displays a message (see below)
- downloads and spawns a Microsoft patch that fixes the problem with IIS worms of this type

The message is as follows:

Des HexXer's CodeGreen V1.0 beta

> CodeGreen has entered your system
> it tried to patch your system and
> to remove CodeRedII's backdoors
>
> You may uninstall the patch via
> SystemPanel/Sofware: Windows 2000 Hotfix [Q300972]
> get details at "www.microsoft.com".
> visit "www.buha-security.de"

Net-Worm.Win32.CodeRed.a

Aliases

Net-Worm.Win32.CodeRed.a (Kaspersky Lab) is also known as: IIS-Worm.CodeRed.a (Kaspersky Lab),

Description added	May 06 2002
Behavior	Net-Worm

Technical details

CodeRed (aka Code Red, Bady) is an Internet worm that replicates between Windows 2000 servers running Microsoft's IIS (Internet Information Services) and the Microsoft Index Server 2.0 or the Windows 2000 Indexing Service. It does this by exploiting a bug known as "Unchecked Buffer in the Index Server ISAPI Extension," described by Microsoft in the Microsoft Security Bulletin MS01-033, released on June 18th, 2001.

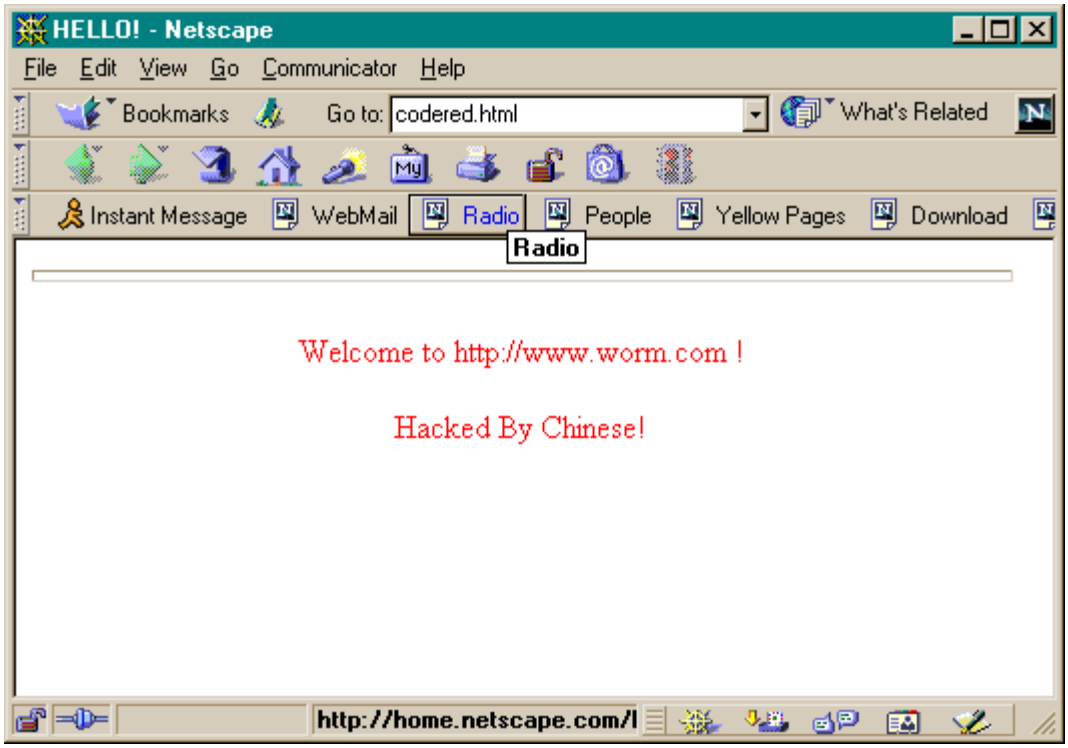
Using a specially crafted string sent to HTTP servers over the Internet, the worm manages to overwrite a variable in the a module named "idq.dll"; thus, forcing the system to jump to an incorrect address, executing the worm code. When run, the worm code will start to create copies of itself in the memory in order to attack even more IIS servers at the same time. The addresses of the servers that the worms attacks are generated random, but because of a bug, each copy of the worm will try to attack the same list of servers, greatly reducing its overall "attack power."

Apparently, the author also noticed this bug, because a few days after the first variant of the worm appeared in the wild, a second, fixed variant was found as well. This second variant known as ".B" or "v2", generates completely random IP addresses streams, with much higher chances to spread than the initial version.

Interestingly, there's a bug in the worm which causes that instead of 100 expected copies of itself running of every infected machine, much, much more are created, wasting large amounts of CPU and memory resources, thus slowing the server, and again, making the worm replication even less efficient. This bug depends on a lot of factors, and will not always show itself - sometimes, the code will operate as expected, and only create 100 threads.

The main worm payload is run if the current date of the month is between the 20th and 27th, inclusively. Then, it will attempt to connect to an IP address associated with the popular site 'www.whitehouse.gov', and tries to flood it with connection attempts.

Also, the worm attempts to deface web sites running on systems which have the language codepage set to US English. In these cases, the worm tries to deface their look by returning instead pages like the following:



If you are running a vulnerable server, we recommend installing the patch released by Microsoft to fix this problem, which can be downloaded at the

following location:

> http://www.microsoft.com/technet/security/bulletin/MS01-033.asp

Technical details:

The worm exploits a buffer overflow in the ISAPI component "idq.dll." When a specific string of characters is sent for processing to one of the functions in "idq.dll," a buffer is overflown, causing the CPU to return control from the function to a bogus address, within the worm "loader."

To do this, the worm sends requests that appear as the following:

> GET /default.ida?{224 'N' characters here}%u9090%u6858%ucbd3%u7801%u9090
> %u6858%ucbd3%u7801%u9090%u6858%ucbd3%u7801%u9090%u9090%u8190%u00c3%u0003
> %u8b00%u531b%u53ff%u0078%u0000%u00{several headers} {worm code appended from here}

The loader encoded in the above request works on the assumption that in the memory at offset 0x7801CBD3h - usually in the memory space allocated to the code segment of the 'msvcrt.dll' library - there is a two-byte long instruction 'call ebx' that is used to jump to the real worm code. However, this is only true if the system is running the default, out-of-the- box version of Windows 2000, with no Service Pack installed. If the system is running NT4, or Win2K SP1/SP2, the worm will most likely crash the Web server, stopping the IIS WWW service.

However, if the system is running the default Windows 2000 installation, the worm receives control through the jump at 0x7801cbd3, and starts to prepare for its next phases.

For that, it will set up a stack space to be later used by the internal operations of the worm, and will look in the memory for the image of the 'kernel32.dll' module. It will perform this checking incrementally various offsets, and whenever a possible candidate is found, the worm verifies that it's indeed a PE file named 'KERNEL32'. If the checks succeed, the worm parses the 'Kernel32.dll' export table in memory, and obtains the address of the very handy API GetProcAddress, which later is used to fetch even more functions: the "socket", "connect", "send", "recv" and "closesocket" subroutine addresses in "WS2_32.dll", and "LoadLibraryA", "GetSystemTime", "CreateThread", "CreateFileA", "Sleep", "GetSystemDefaultLangID" and "VirtualProtect" from 'Kernel32.dll'.

Next, the worm attempts to spawn 100 copies of itself, using the "CreateThread" API, but because of a programming mistake, it will actually create a lot more. Because of this, a server infected with the worm will most likely have a very high CPU load, unless it runs on an extremely fast machine, with lots of memory.

Each thread run by the worm will first look for a file on the disk named "c:\notworm," and if found, it will enter a 'dormant' state, issuing Sleep requests of about 24 days, in an infinite loop. Otherwise, the worm will continue by running one of its two payload subroutines, which check whether the current date of the month is from the 20th to 28th. If so, the worm will attempt to launch connections to the IP address '198.137.240.91', one of the servers hosting the 'www.whitehouse.gov' site. At the time of writing, the respective server seems to have been specifically shut down, and the traffic to the Web site redirected to a different address, probably in an attempt to avoid attacks.

If the current day of the month doesn't match the above rule, the worm attempts to spread itself further. For that, it takes the current second from the system time, and mixes it into a mathematic formula with the thread index in order to produce random numbers suitable for use as IP addresses. However, a bug in the algorithm causes the 'second' field of the time to be ignored; thus, the worm will generate the random numbers only based on the thread index, which is a number between 0 and 99. Therefore, every running copy of the worm will attack the same line of IP addresses, again, a bug which makes the worm less efficient.

To infect servers further, the worm constructs an HTTP request in the memory similar to that used to plant itself initially in the server, and appends its code to it. Then it tries to connect on port 80 to the random IP address provided by the previous subroutine, and if possible, it sends a request to the server. If the respective machine is vulnerable, another copy of the worm will take control, and start doing its job further.

The other worm payload is run only if the codepage of the infected system is 0x409, US English. If so, the worm finds in a specific .DLL module used by the IIS server in the memory, and patches its export table so the 'TcpSockSend' function from it points to a piece of worm code, which instead of the legitimate Web content, it returns a defaced Web site HTML, which looks like the one at the beginning of this description.

After showing the defaced version of the page for 10 hours, the worm reverses the process, and removes itself from the chain of functions used to hijack the Web page, allowing the IIS WWW service to return the proper pages when requested.

"CodeRed.c" (AKA "CodeRedII")

On August 4, 2001, a new variant of the worm was reported in the wild, spreading much faster than the first two variants.

This new variant uses a rather peculiar random IP address generator, which mainly attempts to attack hosts with addresses similar to the one of the host running the worm. For example, if the worm is running on a machine with the address 192.a.b.c, other hosts in the 192.x.x.x family of addresses will have a higher chance of being hit than the others. Apparently, this algorithm had more success than the completely random

approach used in the ".A" and ".B" variants of the worm.

Compared to the ".A" and ".B" versions, the newer one is shorter, but on the flip side, it seems to have been written by someone with better knowledge of the i386 assembler. It will also attempt to backdoor an infected system by copying the standard Windows2K command shell processor "cmd.exe" in two of the IIS server directories, and it will also drop and run a Trojan in the root of the "C:\" and "D:\" drives, named "explorer.exe", 8192 bytes long.

Also, the ".C" variant seems to have been written in response to the "pro-Chinese" ".A" and ".B" versions; if the system language codepage is set either to Traditional or Simplified Chinese, the worm will launch 600 replication threads compared to the default case, where only 300 are run.

Also, on Chinese systems, the worm is allowed to replicate for 48 hours before the system is shutdown. On other machines, the worm runs only for 24 hours, (86,400 seconds) before the system is rebooted.

As mentioned above, the IP random address generator in this variant has been carefully tuned to generate values similar to that of the host on which it is running. With a 1 in 8 probability, the address will be "fully" random, 4 in 8 the address will be in the same Class A family as the one of the system running the worm, and with 3 in 8 chances the randomly generated address will be in the same Class B family as the one of the system running the worm.

Compared to the ".A" and ".B" variants, another improvement in this version is that two main threads of the worm will never run on the same server - a global atom named "CodeRedII" will be set by the first copy of the worm, and any other one will abort execution if the respective atom value is found. Besides that, the worm avoids infecting the machine on which it is running, unlike the first two variants.

This variant of the worm has also a time condition, which is matched after October 2001, when instead of replicating further in an infected machine, the worm will simply reboot the system.

Instructions for deleting the CodeRed II Trojan

1. Click and install the Microsoft patch here:

http://www.microsoft.com/technet/security/bulletin/MS01-033.asp

2. Delete the Trojan from memory in the following way:

2.1 Press CTRL-SHIFT-ESC at the same time to enter "Task Manager";
2.2 Click the "Processes" tab;
2.3 Arrange the process list by names as suits you and click the "Image Name" heading;
2.4 There are two processes in the task list with the names Explorer.exe. In order to recognize the Trojan's process, you must:

2.4.1 In the "View" menu, choose "Select column...";
2.4.2 Then click on "Thread Count" in the window that appears and click "Ok";

2.5 The number of threads involved in each process will be visible in the additional "Thread" column. The Trojan's process with the Explorer.exe name has only one thread. You must delete this process by:
2.6 Selecting this process;
2.7 Clicking "End process";
2.8 Answering "Yes" to the question;
2.9 Closing the "Task Manager" window.

3. Delete the explorer.exe files from the C: and D: disks' root catalogue. To do this, you must complete the following:

3.1 Click on "My computer" twice;
3.2 Click on C: twice;
3.3 If you don't see explorer.exe, you must do the following:

3.3.1 In the "Tools" menu, select "Folder Options...";
3.3.2 Click on "View";
3.3.3 In "Advanced settings," find and switch on "Show hidden files and folders";
3.3.4 Find and switch on "Hide protect operating system files (Recomended)". Answer "Yes" to the question;
3.3.5 Click "OK," and all hidden files will come into view.

3.4 Delete the explorer.exe file by clicking on it with the mouse and clicking "Del," making sure that the file has been deleted;
3.5 Repeat this in order to delete the file from the D: disk, skipping step 3.3 above.

4. If there are four files related to the Trojan, delete them in the same way:

C:\inetpub\Scripts\Root.exe
D:\inetpub\Scripts\Root.exe
C:\Program files\Common Files\System\MSADC\Root.exe
D:\Program files\Common Files\System\MSADC\Root.exe

5. It is now necessary to delete the virtual catalogues created by the Trojan by:

5.1 Clicking the right mouse button on "My computer" and selecting "Manage" from the menu;
5.2 In the "Computer Management" window, choose "Computer Services/Services and Applications/Internet Information Services/")
5.3 Select the "C" virtual catalogue and click "Del" and answer "Yes" to the question.
5.4 Do the same with the "D" catalogue.

6. In order to clean out the register, you must do the following:

6.1 Access the register by hitting "Start" and choosing "Run," enter "regedit" and click "Enter."
6.2 Find the key:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W3SVC\Parameters\Virtual Roots

6.3 Select the "/C" parameters and click "Del," and answer "Yes" to the question.
6.4 Do the same for the "/D" parameters.
6.5 Click on the "/MSDAC" parameters twice and change the end value to 201.
6.6 Do the same with the "/Scripts" parameters.
6.7 Find the key:

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\WinLogon

6.8 Click on the "SFCDisable" parameters twice and change its value to 0.

7. Restart/reboot your computer.

Net-Worm.Win32.Cycle.a

Aliases

Net-Worm.Win32.Cycle.a (Kaspersky Lab) is also known as: Worm.Win32.Cycle.a (Kaspersky Lab), W32/Cycle.worm.a (McAfee), W32.Cycle (Symantec), Win32.HLLW.Cycle (Doctor Web), W32/Cycle-A (Sophos), Win32/Cycle.A.worm (RAV), WORM_CYCLE.A (Trend Micro), Worm/Cycle.A (H+BEDV), Win32:Cycle (ALWIL), I-Worm/Cycle.A (Grisoft), Win32.Worm.Cycle.A (SOFTWIN), W32/Cycle.A.worm (Panda), Win32/Cycle.A (Eset)

Description added	May 11 2004
Behavior	Internet Worm

Technical details

Cycle is an Internet worm that exploits the LSASS vulnerability in MS Windows described in MS Security Bulletin MS04-011

Microsoft released a patch for this vulnerability on April 13, 2004 - available at the above link.

Cycle affects computers running Windows 2000, Windows XP and windows Server 2003

The worm is written in C++ and is about 10 KB (packed by UPX).

Propagation

Upon launching Cycle copies itself into the Windows system folder under the name 'svchost.exe' and registers itself in the following autorun keys:

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run]
[HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run]
 "Generic Host Service" = "%windir%\system\svchost.exe"
```

The worm also create the file cyclone.txt in the Windows folder. This file contains the following letter to the global community from the authour of the worm:

Hi,
My name is Cyclone and I live in Iran,
and I want to speak with you about problems that we have in iran:

A.In Iran we don't have any kind of freedom, because we have islamic republic in iran:
1.we can't speak freely about regime, we can't speak even a little bit against them!!!
2.I have to be a moslem otherwise they don't care about me!
3.we CAN'T even wear the clothes and styles that we wants!
4.women MUST wear a cloth that no one can even see their hair!!!
5.they do not allow our national celebrations to be held, they beat us!!
6.Many more...

B.The human rights is not implemented in Iran and there is no justice,
1.Lynch is very common in Iran. If you are against the regime then you may silently killed, or if there is a tribunal, you can't say anything, everyone works against you there.
2.1985-1990, the Islamic Republic of IRAN has been killed more than 10,000 Iranian youngs. that has been comfirmed by the documentations! This people killed without any tribunal or any proof.
3.there is a punishment that is used so much during this years, in this punishment, the person who must be killed stand in a hole then others attack him with stones, this will continue until he/she dead. there is some pictures and videos that shows this terrible torture!
4.Many more...

C.Misery and poverty grows in Iran, because the islamic republic leaders steal the money, they stolen the money that provided by selling oil, and then the people must die because they don't have enough money to even buy a bread!!!

D.Misery and poverty cause vice to grow, you see many young people in Iran using drugs and I think this is also a trick by the government to not allow us to arise against them!

E.Islamic republic gave Iran a bad name. before islamic republic we can travel anywhere in the world without any problem but now we have so much problems if we want to travel a foreign country, anyone think that we are terrorist. THE PEOPLE OF IRAN ARE NOT TERRORIST, THE ISLAMIC REPUBLIC OF IRAN IS TERRORIST.

The people of Iran trying to arise, but failed to do. About one year ago, Iranian people try to say to the world that we don't need Islamic republic but the government and police beat the people who try to tell the truth and they killed some people.
You see that they don't even care about their own people, think what happen if they gain access to an ATOMIC BOMB!!! it's very dangerous for the world.
With all of this conditions and injustices, european governments still support islamic republic, they say that they just care about their own country!
and I want to show them our WRATH!
All of the european people are my friends and I never want to harm them, just government and the Politicians!
If you protest against iraq war and say why there must be a war against iraq, and if you do this for humanity, please do anything that you can do for helping iranian people.
at least make your country not to support islamic republic anymore, I'm deadly sure that if european countries do not support islamic republic. it will be destroyed after 3-6 months!
so please help!

I don't want to damage, I just want my country to grow, to improve!!! I have no other way to tell this words to world, sorry!!

The worm is built to fight against Internet worms Sasser and Lovesan. It creates unique identifiers in the RAM that match identifiers created by Sasser, thus preventing Sasser infections.

```
Jobaka3
Jobaka3l
JumpallsNlsTillt
SkynetSasserVersionWithPingFast
```

Cycle attempts to detect and stop the processes with names from the following list:

```
avserve.exe
avserve2.exe
msblast.exe
skynetave.exe
```

Cycle deploys an FTP server on TCP port 69, launches 4 IP address scans searching for potential victim machines and sends requests to TCP port 445. If a remote machine allows a connection Cycle sends the LSASS expoit which installs a cmd.exe command shell on the victim machine.

The worm then forwards commands to load and launch itself to the infected machine. The file containing the worm after being forwarded is named cyclone.exe..

Other

After infection, victim machines launch a notice about a LSASS service failiure and may attempt to reboot.

In addition, Cycle attempts to initiate DoS attack on irn.com and www.bbcnews.com everyday in May except Sundays.

Net-Worm.Win32.Dabber.a

Aliases

Net-Worm.Win32.Dabber.a (Kaspersky Lab) is also known as: Worm.Win32.Dabber.a (Kaspersky Lab), W32/Dabber.worm.a (McAfee), W32.Dabber.A (Symantec), Win32.HLLW.Dabber (Doctor Web), W32/Dabber-A (Sophos), Win32/Dabber.worm (RAV), WORM_DABBER.A (Trend Micro), Worm/Dabber.A (H+BEDV), W32/Dabber.A (FRISK), Win32:Dabber (ALWIL), Worm/Dabber.A (Grisoft), Win32.Worm.Dabber.A (SOFTWIN), Worm.Dabber.A (ClamAV), W32/Dabber.A.worm (Panda), Win32/Dabber.A (Eset)

Description added	Jun 09 2004
Behavior	Internet Worm

Technical details

This worm spreads via the Internet using a vulnerability in the FTP component of Worm.Win32.Sasser.

The worm itself is a Windows PE EXE file, 29696 bytes in size, packed using UPX.

Installation

When installing, the worm copies itself to the Windows system directory under the name package.exe

```
c:\Documents and Settings\All Users\Start Menu\Programs\Startup\
%windir%\All Users\Main menu\Programs\StartUp
```

The worm registers this file in the system registry auto-run key:

```
HKLM\Software\Microsoft\Windows\CurrentVersion\Run
  "sassfix"="%System%\package.exe"
```

The worm searches the system registry for keys installed by Sasser and deletes them.

```
avserve2.exe
avvserrve32
avserve
skynetave.exe
```

and deletes them. It also searches for and deletes keys installed by other worms:

```
Video
Microsoft Update
Drvddll.exe
Drvddll_exe
drvsys
drvsys.exe
ssgrate
ssgrate.exe
lsasss
lsasss.exe
Taskmon
Gremlin
Window
Video Process
TempCom
SkynetRevenge
MapiDrv
BagleAV
System Updater Service
soundcontrl
WinMsrv32
drvddll.exe
navapsrc.exe
Generic Host Service
Windows Drive Compatibility
windows
```

The worm scans networks for random IP addresses, searching for victim machines which have the ftp component of Sasser installed on port 5554.

When the worm finds a suitable victim machine, it sends a vulnerability exploit to it to infect the system. It then launches the command shell on port 8967. It also installs a backdoor on port 9898 to receive external commands.

Net-Worm.Win32.DipNet.d

Other versions: .a

Aliases

Net-Worm.Win32.DipNet.d (Kaspersky Lab) is also known as: Exploit-MS04-011.gen (McAfee), Win32.HLLW.Daras (Doctor Web), Worm/DipNet.b (H+BEDV), Win32.Worm.DipNet.D (SOFTWIN), Exploit.DCOM.Gen (ClamAV), Win32/Dipnet.NAC (Eset)

Detection added	Jan 12 2005
Description added	Jan 14 2005
Behavior	Net-Worm

Technical details

DipNet.d infects computers running under Windows. The worm itself is a Windows PE EXE file approximately 91KB in size, packed using UPX. The unpacked file is approximately 264KB in size.

The worm propagates by exploiting a vulnerability in Microsoft Windows LSASS (MS04-011). This vulnerability is described in detail here

The worm contains a backdoor function.

Once launched, the worm copies itself to the Windows system directory under a random name e.g.

```
%System%\wcss.exe
```

and creates a service named 'WebPoster'.

Then the worm registers this file as a key in the system registry:

```
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run]
"WinNetDDE" = "%System%\<random name>.exe"
```

This ensures that the worm will be launched each time the infected machine is rebooted.

It then deletes the original file which contained it.

The worm starts its propagation routine, selecting IP addresses to attack, and sending a request to TCP port 445. If the remote computer responds, then the worm launches its code on the victim machine, by utilizing the LSASS vulnerability.

The worm opens TCP port 11768 in order to receive commands. The backdoor function provides a malicious remote attacker with full access to the victim machine.

The worm causes the victim machine to open one of the following sites to check if it is currently connected to the internet:

```
www.yahoo.com
www.ebay.com
www.google.com
```

P2P-Worm.Win32.Achar.a

Aliases

P2P-Worm.Win32.Achar.a (Kaspersky Lab) is also known as: Worm.P2P.Achar.a (Kaspersky Lab), W32/Achar.worm!p2p (McAfee), W32.Achar.Worm (Symantec), Win32.Cucaracha.8192 (Doctor Web), W32/Achar-A (Sophos), Win32/HLLW.Achar.A (RAV), WORM_ACHAR.A (Trend Micro), Worm/Achar.A (H+BEDV), W32/Achar.A (FRISK), Win32:Achar (ALWIL), Worm/Achar.A (Grisoft), Win32.HLLW.Achar.A (SOFTWIN), Worm Generic (Panda), Win32/Achar.A (Eset)

Description added	May 27 2003
Behavior	P2P Worm

Technical details

This is a family of harmless worms that replicate by making their copies in a Kazaa shared folder.

The worm is a Windows application (PE EXE file) written in Assembler, the worm file size is about 8K.

The worm does not install itself into the system.

To infect Kazaa shared folder the worm reads its name from system registry and copies itself to the folder with following names:

```
'\Crack McAfee 7.exe'
'\Crack Norton 3000.exe'
'\Borland KeyGens.exe'
'\MP3 encoder_decoderV1.8.exe'
'\HackNTTools.zip                    .exe'
'\SophosCrackAllVersion.exe'
'\BitDefender.KeyGen.exe'
'\Nod32Crack.exe'
'\PANDA.lusers.exe'
'\PANDA.AVers.lusers.exe'
```

The worm also tries to copy itself with the "CUCARACHA.exe" name to startup directories on remote computers, but fails because of a bug. So, it is pure P2P worm.

The worm has "copyright" text string:

```
-/Cucaracha\- Programado por ErGrone * SANTIAGO DE CHILE
```

P2P-Worm.Win32.Bare.a

Aliases

P2P-Worm.Win32.Bare.a (Kaspersky Lab) is also known as: Worm.P2P.Bare.a (Kaspersky Lab), W32/Bare.worm.a!p2p (McAfee), W32.HLLW.Bare (Symantec), Win32.HLLW.Bare.24576 (Doctor Web), W32/Bare-A (Sophos), Win32/HLLW.Bare (RAV), WORM_BARE.A (Trend Micro), Worm/Bare.A1 (H+BEDV), W32/Bare.A (FRISK), Win32:Bare-A (ALWIL), Worm/Bare.A (Grisoft), Win32.HLLW.Bare.A (SOFTWIN), Worm.P2P.Bare.A (ClamAV), Worm Generic (Panda), Win32/Bare.B (Eset)

Description added	Aug 28 2002
Behavior	P2P Worm

Technical details

Bare is an Internet worm that spreads in the Kazaa, Morpheus, BearShare and eDonkey2000 peer-to-peer file exchange networks. The worm replicates by placing copies of itself in the shared folders used on the client machines comprising these networks.

The Bare worm is a Windows application (PE EXE file) 7.6KB in size, written in Visual Basic and compressed with the UPX utility (the decompressed size is about 25KB).

Bare does not manifest itself in any way.

The worm copies itself to P2P directories under the following names:

key generator.exe
crack.exe
patch.exe
serial.exe
full downloader.exe
Britney Spears.exe
Christina Aguilera.exe
Jennifer Lopez.exe
Pamela Anderson.exe
Claudia Schiffer.exe
nude.exe
xxx.exe
porno.exe
Windows 2000.exe
Kazaa.exe
MSN.exe
AOL.exe
ICQ.exe
mIRC.exe
hack.exe
backdoor remover.exe
password stealer.exe
Spiderman.exe
Harry Potter.exe
wallpaper.exe
screensaver.exe

P2P-Worm.Win32.Benjamin.a

Aliases

P2P-Worm.Win32.Benjamin.a (Kaspersky Lab) is also known as: Worm.P2P.Benjamin.a (Kaspersky Lab), W32/Benjamin.worm (McAfee), W32.Benjamin.Worm (Symantec), Win32.HLLW.Benjamin (Doctor Web), W32/Benjamin-A (Sophos), Win32/Benjamin.worm (RAV), WORM_BENJAMIN.A (Trend Micro), Worm/Kazaa (H+BEDV), W32/Benjamin.A@mm (FRISK), Win32:Benjamin (ALWIL), Worm/Benjamin.A (Grisoft), Win32.Worm.Benjamin.A (SOFTWIN), Worm.Kazaa (ClamAV), W32/Kazoa (Panda), Win32/Kazaa.Benjamin (Eset)

Description added	Jul 12 2002
Behavior	P2P Worm

Technical details

This worm uses the Kazaa file exchange P2P network to spread itself. The Kazaa network allows its users to exchange files with each other using the Kazaa client software. To learn more about the Kazaa network visit their site at: http://www.kazaa.com.

Benjamin is written in Borland Delphi and is approximately 216 Kb in size - it is compressed by the AsPack utility. The size of a file can vary greatly as the worm ends each file with "dust" for masking.

Installation

Firstly the worm shows a false error report:

Benjamin then copies itself to the %WinDir%\SYSTEM directory as

EXPLORER.SCR

and creates two keys in the system registry:

[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run] "System-Service"="C:\\WINDOWS\\SYSTEM\\EXPLORER.SCR" [HKEY_LOCAL_MACHINE\Software\Microsoft] "syscod"="0065D7DB20008306B6A1"

The worm executes after system restarts.

Spreading

Spreading can most likely only take place if the KaZaa P2P client (software) is installed. Benjamin reads the system registry for information on the Kasaa client and creates the

%WinDir%\Temp\Sys32

directory catalog that registers as the directory accessible to all KaZaa network users. It fills this directory with copies of itself listed under numerous various names from a list contained in the body of the worm.

Spreading occurs as follows. A "victim" searching for a file in the KaZaa network finds it in the list of accessible files on already infected machine. Not suspecting a problem the user downloads this file and opens it, thus infecting his or her own machine.

Effects

The worm opens the benjamin.xww.de Web-site to display an advertisement.

P2P-Worm.Win32.Darby.m

Aliases

P2P-Worm.Win32.Darby.m (Kaspersky Lab) is also known as: Worm.P2P.Darby.m (Kaspersky Lab), W32/Darby.worm.m (McAfee), W32.HLLW.Darby (Symantec), Win32.IRC.Generic.16 (Doctor Web), W32/Darby-G (Sophos), Win32/HLLW.Darby.N (RAV), WORM_DARBY.G (Trend Micro), Worm/Darby.M (H+BEDV), W32/Darby.K (FRISK), Win32:Darby-F (ALWIL), Worm/Darby.R (Grisoft), Win32.P2P.Barby.A (SOFTWIN), Worm.P2P.Darby.Gen (ClamAV), W32/Darby.F.worm (Panda), Win32/Darby.M (Eset)

Description added	Aug 01 2005
Behavior	P2P Worm

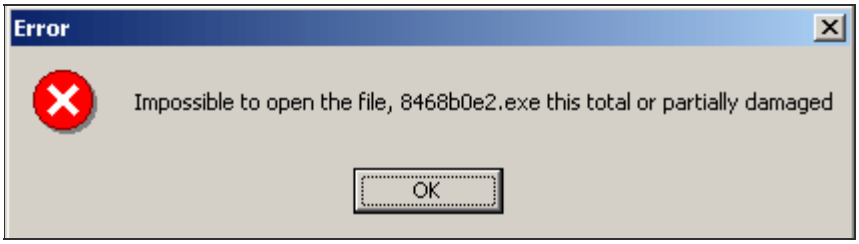
Technical details

This worm spreads via the Internet via file-sharing networks. It also spreads via IRC channels, open network resources, and as an attachment to infected messages. It sends itself to addresses harvested from the victim machine.

The worm itself is a Windows PE EXE file approximately 141KB in size, packed using UPX. The unpacked file is approximately 426KB in size.

Installation

Once launched, the worm causes the following error message to be displayed:



The name of the worm file will be used in order to give the user the impression that the file cannot be executed.

When installing, the worm copies itself to the Windows system directory under the following names:

```
%System%\Image0X.scr
%System%\KillUsa.exe
```

It also creates several copies of itself in the Windows system directory, using random names e.g.

```
%System%\ISZQ.scr
```

The worm creates a PKZIP utility in the system directory under the name bZip.exe. This is approximately 42KB in size. (îêîëî 42 ÊÁ). This is used to create archive copies of the worm in the same directory, under the name GZIP.ZIP. This file is approximately 127KB in size.

The worm also creates the following HTML files:

```
%Windir%\microsoftweb.htm
C:\Bardiel.hta
```

The worm then registers its files in the system registry:

```
[HKLM\Software\Microsoft\Windows\CurrentVersion\Run]
 "NETCOMMAND503"="<path to copy of worm>"

[HKLM\Software\Microsoft\WindowsNT\CurrentVersion\Run]
 "NETCOMMAND503"="<path to copy of worm>"

[HKCU\Software\Microsoft\Windows NT\CurrentVersion\Windows]
 "run"="<path to copy of worm>"
```

This ensures that the worm file will be launched each time Windows is rebooted on the victim machine.

The worm modifies the registry keys listed below. This means that when files with .bat, .com, .exe, .pif or .scr extensions are launched, a copy of the worm will be launched instead of these files.

```
[HKCR\batfile\shell\open\command]
```

```
[HKLM\Software\Classes\batfile\shell\open\command]
"default"="<path to copy of worm> %1"

[HKCR\comfile\shell\open\command]
[HKLM\Software\Classes\comfile\shell\open\command]
"default"="<path to copy of worm> %1"

[HKCR\exefile\shell\open\command]
[HKLM\Software\Classes\exefile\shell\open\command]
"default"="<path to copy of worm> %1"

[HKCR\piffile\shell\open\command]
[HKLM\Software\Classes\piffile\shell\open\command]
"default"="<path to copy of worm> %1"

[HKCR\scrfile\shell\open\command]
[HKLM\Software\Classes\scrfile\shell\open\command]
"default"="<path to copy of worm> %1"
```

The worm also modifies the following system registry values to block Task Manager and Registry Tools:

```
[HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\System]
[HKCU\Software\Microsoft\WindowsNT\CurrentVersion\Policies\System]
"DisableRegistryTools"="dword:00000001"
"DisableTaskMgr"="dword:00000001"
```

Propagation via P2P

The worm checks the victim machine for an installed P2P client (edonkey2000, emule, kazaa, morpheus and others). It then copies itself into the client's shared directories and open network resource directories under the following names:

```
ACDSee 5.5.exe
Age of Empires 2 crack.exe
Ana Kournikova Sex Video.exe
Animated Screen 7.0b.exe
aol cracker.exe
AOL Instant Messenger.exe
aol password cracker.exe
AquaNox2 Crack.exe
Audiograbber 2.05.exe
AVP Antivirus Pro Key Crack.exe
BabeFest 2004 ScreenSaver 1.5.exe
Babylon 3.50b reg_crack.exe
Battlefield1942_bloodpatch.exe
Battlefield1942_keygen.exe
Britney Spears Sex Video.exe
Buffy Vampire Slayer Movie.exe
Business Card Designer Plus 7.9.exe
cable modem ultility pack.exe
cable modem ultility pack.exe
Clone CD 5.0.0.3 (crack).exe
Clone CD 5.0.0.3.exe
Coffee Cup Free zip 7.0b.exe
Cool Edit Pro v2.55.exe
counter-strike.exe
Crack Passwords Mail.exe
Credit Card Numbers generator(incl Visa,MasterCard,...).exe
Cristina Aguilera Sex Video.exe
delphi.exe
Diablo 2 Crack.exe
DirectDVD 5.0.exe
DirectX Buster (all versions).exe
DirectX InfoTool.exe
divx pro.exe
DivX Video Bundle 6.5.exe
divx_pro.exe
Download Accelerator Plus 6.1.exe
DVD Copy Plus v5.0.exe
DVD Region-Free 2.3.exe
Edonkey2000-Speed me up scotty.exe
FIFA2004 crack.exe
Final Fantasy VII XP Patch 1.5.exe
Flash MX crack (trial).exe
FlashGet 1.5.exe
FreeRAM XP Pro 1.9.exe
Game Cube Real Emulator.exe
GetRight 5.0a.exe
Global DiVX Player 3.0.exe
Gothic2 licence.exe
GTA 3 Crack.exe
GTA 3 Serial.exe
Guitar Chords Library 5.5.exe
Hentai Anime Girls Movie.exe
Hitman_2_no_cd_crack.exe
Hot Babes XXX Screen Saver.exe
HotGirls.exe
Hotmail Hacker 2004 - Xss Exploit.exe
Hotmail Hacker 2004-Xss Exploit.exe
hotmail_hack.exe
ICQ Pro 2004a.exe
ICQ Pro 2004b (new beta).exe
iMesh 3.6.exe
iMesh 3.7b (beta).exe
IrfanView 4.5.exe
Jenifer Lopez Sex Video.exe
KaZaA Hack 2.5.0.exe
Kazaa SDK + Xbit speedUp for 2.xx.exe
KaZaA Speedup 3.6.exe
Links 2004 Golf game (crack).exe
Living Waterfalls 1.3.exe
macromedia dreamweaver key generator.exe
```

```
Mafia_crack.exe
Matrix Movie.exe
Matrix Screensaver 1.5.exe
Mcafee Antivirus Scan Crack.exe
MediaPlayer Update.exe
Microsoft KeyGenerator-Allmost all microsoft stuff.exe
mIRC 6.40.exe
mp3Trim PRO 2.5.exe
MSN Messenger 5.2.exe
NBA2004_crack.exe
Need 4 Speed crack.exe
Nero Burning ROM crack.exe
Netbios Nuker 2004.exe
Netfast 1.8.exe
Network Cable e ADSL Speed 2.0.5.exe
NHL 2004 crack.exe
Nimo CodecPack (new) 8.0.exe
Norton Anvirus Key Crack.exe
PalTalk 5.01b.exe
pamela_anderson.exe
Panda Antivirus Titanium Crack.exe
PerAntivirus 8.9.exe
play station emulator.exe
Popup Defender 6.5.exe
Pop-Up Stopper 3.5.exe
PS2 PlayStation Simulator.exe
Quick Time Key Crack.exe
QuickTime_Pro_Crack.exe
Sakura Card Captor Movie.exe
Screen saver christina aguilera naked.exe
Security-2004-Update.exe
Serials 2004 v.8.0 Full.exe
serials2000.exe
Sex Live Simulator.exe
Sex Passwords.exe
SmartFTP 2.0.0.exe
SmartRipper v2.7.exe
Space Invaders 1978.exe
Spiderman Movie.exe
Splinter_Cell_Crack.exe
Starcraft serial.exe
Start Wars Trilogy Movies.exe
Steinberg_WaveLab_5_crack.exe
Stripping MP3 dancer+crack.exe
subseven.exe
Thalia Sex Video.exe
The Hacker Antivirus 5.7.exe
Trillian 0.85 (free).exe
TweakAll 3.8.exe
Unreal2_bloodpatch.exe
Unreal2_crack.exe
UT2004_bloodpatch.exe
UT2004_keygen.exe
UT2004_no cd (crack).exe
UT2004_patch.exe
VB6.exe
virtua girl - adriana.exe
virtua girl - bailey short skirt.exe
Virtua Girl (Full).exe
VirtualSex.exe
Visual Basic 6.0 Msdn Plugin.exe
Visual basic 6.exe
warcraft 3 crack.exe
warcraft 3 serials.exe
WarCraft_3_crack.exe
Winamp 3.8.exe
winamp plugin pack.exe
WindowBlinds 4.0.exe
Windows XP complete + serial.exe
Windows Xp Exploit.exe
WinOnCD 4 PE_crack.exe
WinRar 3.xx Password Cracker.exe
WinZip 9.0b.exe
winzip full version key generator.exe
Winzip KeyGenerator Crack.exe
WinZipped Visual C++ Tutorial.exe
XNuker 2004 2.93b.exe
Yahoo Messenger 6.0.exe
Zelda Classic 2.00.exe
```

This means that other users of the P2P client will be able to access the infected files.

Propagation via email

The worm harvests email addresses from the victim machine. Harvested addresses are saved in the following files:

```
%Temp%\bh.dat
%Temp%\bl.dat
%Temp%\bm.dat
```

The worm uses its own SMTP library to send infected messages.

Infected messages

Message subject (chosen from the list below):

- 100% Ideal

- Amor y Sexo
- do you Know if they lie you?
- Fotos en tu email
- HackHotmail
- Looks at the picture
- Mail Delivery Return System
- Manual de Seduccion
- Message
- Mi Album
- Mira la foto
- MORE Drawings
- New Registry
- No Adware
- NoMentir
- Nuevo Registro
- Pictures in your email
- Planet PlayBoy
- Planeta PlayBoy
- PornStars Show
- ReturnMsg
- Sex Tantrico Images
- Sexo Tantrico Images
- Ten commandments give the Love and Sex
- Test Here
- Virtual Card
- you Have a Mensage
- you have a Virtual Gift
- Your Name

Message body (chosen from the list below):

- Debido a las reformas del servidor, se pide a los usuarios completar el nuevo registro a fin de validar sus cuentas y no sean suspendidas. Atentamente AdminSystem
- due to the reformations he/she gives the servant, it is asked the users to complete the new registration in order to validate their you count and don't be suspended. Sincerely AdminSystem"
- Este es un test usado por el ejercito de estados unidos al reclutar soldados, para en palabras simples medir cuan propensos a la locura son, hacelo y ve cuan zafado estas.
- he/she looks at the image 30 second and then he/she looks to another part and truth at something surprising (good optic illusion, almost hallucination)
- Hello, you don't know me, but I ship you something that interested you, God willing it is you gives utility, bye
- I ship You the info that you requested me, responds that such this, bye
- Looks at this scrensaver gives the actresses he/she gives the cinema porn
- mira la imagen 30 segundos y luego mira a otra parte y veras algo sorprendente ......(buena ilusion optica, casialucinacion)
- Osama Ben Laden the man that I declare the War to United States
- Se te cambia la pagina de inicio?, te salen ventanas de publicidad, problemas con dialers, troyanos u otros adwares, prueba este programa gratis y acabemos con la lacra que es el Adware.
- The best pictures give PlayBoy gives this year, it passes them ;)
- The corporal language accuses the lie subtly, 5 tips to know if they are telling you e truth.
- The names and the last names like all word have a meaning, the one which already in most he/she gives times or we don't remember, perhaps find the meaning he/she gives yours in our database:)
- there is an available card for you on behalf of a friend. discharge it or enters to the link:)
- they have sent You a virtual Gift, this available one during 7 days, discharge it or enters to the link:)
- to Maintain a healthy loving relationship and upper demands a lot of effort and many desires, we give you these 10 keys
- you Know that it means the form gives to kiss or that types and techniques exist, know them
- you Want to improve your success with the opposite sex, search keeps an eye on this text. that has useful advice.

Attachment name (chosen from the list below):

- 10Claves.zip
- 16Playboy.zip
- CrazyTest.zip
- CwshredderPlus.zip
- Drawings.zip
- E-Card.zip
- EL-Card.zip
- FuckSanta.zip
- Gusanito.com
- HackHotmail.zip
- Ideal.zip
- Kiss.zip
- Lie.zip
- NoMentir.zip
- Ph0t0.zip
- Photo.zip
- PornStars.zip
- Registro.zip
- Registry.zip
- ReturnMsg.zip
- Seduc.zip

- Sex_Tantra.zip
- SigName.zip
- TestRayado.zip
- TuFuturo.zip
- videoClip.zip
- Virtual0034.zip
- xImages.zip

Propagation via IRC channels

The worm will rewrite the files listed below in order to send copies of itself to users in the same IRC channel as the victim machine:

```
%ProgramFiles%\mIRC\script.ini
%ProgramFiles%\mIRC32\script.ini
```

Payload

The worm terminates active processes where the names of the processes contain the following text strings:

```
ate32class
adaware
advxdwin
auto-protect
alogserv
anti-trojan
avsched32
avconsol
ackwin32
autodown
antivir
avsynmgr
avrep32
atupdater
atwatch
autotrace
aplica32
atro55en
aupdate
autoupdate
avrescue
avltmain
backweb
blackice
bd_professional
bidserver
bootwarn
buscareg
claw95ct
cfiaudit
cfiadmin
cmgrdian
cleanpc
cmon016
cpf9x206
cpfnt206
csinject
csinsm32
css1631
cwnb181
cwntdwmo
ccevtmgr
ccpxysvc
defwatch
defalert
drwatson
drweb32
drwebupw
efinet32
espwatch
efpeadm
etrustcipe
ecengine
findviru
f-agnt95
f-stopw
filemon
fameh32
flowprotector
fp-win_trial
generics
hacktracer
icssuppnt
icsupp95
iomon98
ifw2000
iparmor
kavlite
lookout
lockdown
lucomserver
ldpromenu
ldnetmon
localnet
mpftray
moolive
msconfig
monitor
mcmnhdlr
```

mcupdate
mcvsrte
minilog
mcvsshld
mpfservice
mcshield
mfweng3
msinfo32
mssmmc32
mu0311ad
nspclean
nupgrade
nwtool16
normist
nisserv
nsched32
neowatchlog
nvsvc32
nwservice
ntxconfig
npscheck
netutils
notstart
ncinst4
netarmor
netinfo
netspyhunter
netstat
nvarch16
nvlaunch
nwinst4
nvapsvc
outpost
offguard
ostronet
procexp
pcfwallicon
programauditor
pop3trap
poproxy
pcntmon
pview95
pgremove
pfwagent
prebind
pcdsetup
pcip10117_0
pfwadmin
portdetective
ppinupdt
ppvstop
procexplorerv1
proport
protect
pccntmon
qconsole
qserver
rtvscn95
rulaunch
regedit
regedt32
realmon
stinger
safeweb
symproxysvc
symtray
ss3edit
swnetsup
schedapp
setupvameeval
setup_flowprotector_us
sgssfw32
shellspyinstall
srwatch
supftrl
supporter5
sysdoc32
sysedit
sharedaccess
taskmon
tauscan
titanin
tmntsrv
undoboot
vshwin32
vsecomr
vbcmserv
vir -help
vettray
vcontrol
vccmserv
vcsetup
vfsetup
vnlan300
vnpc3000
vpfw30s
vscenu6
vsisetup
wfindv32
wimmun32
webtrap
watchdog
wradmin
w32dsm89
whoswatchingme
winrecon
winroute
winsfcm

```
wsbgate
zonealarm
zatutor
zonestub
zlclient
zauinst
zonalm2601
taskmgr
```

The worm may also download files from the servers listed below without the user's knowledge or consent.

```
http://hosting.m***at.com/interserv7
http://interserv1.thefr***izhost.com
http://interserv10.i***tworx.de
http://interserv6.m***tespace.com
http://interserv9.t**.com
```

P2P-Worm.Win32.Duload.a

Other versions: .b

Aliases

P2P-Worm.Win32.Duload.a (Kaspersky Lab) is also known as: Worm.P2P.Duload.a (Kaspersky Lab), W32/Duload.worm.gen!p2p (McAfee), W32.HLLW.Yoof (Symantec), Win32.HLLW.Duload.18432 (Doctor Web), W32/Duload-A (Sophos), Win32/Duload.A.worm (RAV), WORM_DULOAD.A (Trend Micro), Worm/Duload.A (H+BEDV), Win32:Duload (ALWIL), Worm/Duload.A (Grisoft), Win32.P2P.Duload.A@mm (SOFTWIN), Worm.Duload.A (ClamAV), W32/Duload.A (Panda), Win32/Duload.A (Eset)

Description added	Oct 31 2002
Behavior	P2P Worm

Technical details

Worm.P2P.Duload represents a family of worms that replicate by copying themselves into a Kazaa network shared folder located on victim machines.

The worm itself is a Windows application (PE EXE file) written in Visual Basic, 18432 bytes in size.

Installation

The worm copies itself to the Windows System directory under the name SystemConfig.exe and modifies the system registry so that this file automatically loads upon start-up.

This is done by writing the following registry values:

```
[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run]
 "Windows System Configure"="[System Directory path]\SystemConfig.exe"
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run]
 "Windows System Configure"="[System Directory path]\SystemConfig.exe"
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices]
 "Windows System Configure"="[System Directory path]\SystemConfig.exe"
```

Replication

The Duload worm creates a directory in the Windows System directory named "Media" and then copies itself to this directory under the following names:

```
Alicia Silverstone Payboy Nude.exe
Bingo.exe
Britney Spears Dance Beat.exe
DDos Client.exe
Email Bomber.exe
FileServer.exe
Flash Golf.exe
Free Mpegs.exe
Free Pics.exe
Free Porn.exe
Hoes For You Solitare.exe
Hotmail Hacker.exe
Irc Client.exe
J.Lo Bikini Screensaver.exe
Jenna Jamison Dildo Humping.exe
Kama Sutra Tetris.exe
Kazaa Clone.exe
Mirc 7.0.exe
Napster Clone.exe
Pamela Anderson And Tommy Lee Home Video.exe
Play Games Online For FREE.exe
Ps2 Emulator.exe
Ps2 Iso 2 Rom Converter.exe
Shakira Dancing.exe
Soldier Of Fortune 2 Mutiplayer Serial Hack.exe
System Monitor.exe
The Sims Game Crack.exe
Universal Game Crack.exe
Warcraft 3 Battle.net Crack.exe
Website Hacker.exe
Win A Ps2.exe
Win An Xbox.exe
Winace.exe
Windows Hacker.exe
Winmx.exe
Winrar.exe
Winzip.exe
Working Iso Burner.exe
```

```
Xbox Emulator.exe
Xbox Iso 2 Rom Converter.exe
```

Then the worm writes several registry values in the [HKEY_CURRENT_USER\Software\Kazaa] registry key, so that the Media directory becomes available as a Kazaa shared directory.

Other

The Worm.P2P.Duload.a variant also acts as a TrojanDownloader: it downloads a malware program from the "http://thisistrash.0catch.com/" site, saves it to "c:\Uninstall.exe" and executes it.

P2P-Worm.Win32.Duload.b

Other versions: .a

Aliases

P2P-Worm.Win32.Duload.b (Kaspersky Lab) is also known as: Worm.P2P.Duload.b (Kaspersky Lab), W32/Duload.worm.gen!p2p (McAfee), Trojan Horse (Symantec), Win32.HLLW.Duload.18432 (Doctor Web), W32/Duload-B (Sophos), Win32/Duload.B.worm (RAV), WORM_DULOAD.B (Trend Micro), Worm/Duload.P2P.B (H+BEDV), W32/Duload.B (FRISK), Win32:Duload-B (ALWIL), Worm/Duload.B (Grisoft), Win32.Worm.Duload.B (SOFTWIN), Worm.P2P.Duload.B (ClamAV), W32/Duload (Panda), Win32/Duload.B (Eset)

Description added	Jun 22 2002
Behavior	P2P Worm

Technical details

Worm.P2P.Duload represents a family of worms that replicate by copying themselves into a Kazaa network shared folder located on victim machines.

The worm itself is a Windows application (PE EXE file) written in Visual Basic, 7680 bytes in size (packed with UPX).

Installation

The worm copies itself to the Windows System directory under the name SystemConfig.exe and modifies the system registry so that this file automatically loads upon start-up.

This is done by writing the following registry values:

```
[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run]
 "Windows System Configure"="[System Directory path]\SystemConfig.exe"
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run]
 "Windows System Configure"="[System Directory path]\SystemConfig.exe"
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices]
 "Windows System Configure"="[System Directory path]\SystemConfig.exe"
```

Replication

The Duload worm creates a directory in the Windows System directory named "Media" and then copies itself to this directory under the following names:

```
Alicia Silverstone Payboy Nude.exe
Bingo.exe
Britney Spears Dance Beat.exe
DDos Client.exe
Email Bomber.exe
FileServer.exe
Flash Golf.exe
Free Mpegs.exe
Free Pics.exe
Free Porn.exe
Hoes For You Solitare.exe
Hotmail Hacker.exe
Irc Client.exe
J.Lo Bikini Screensaver.exe
Jenna Jamison Dildo Humping.exe
Kama Sutra Tetris.exe
Kazaa Clone.exe
Mirc 7.0.exe
Napster Clone.exe
Pamela Anderson And Tommy Lee Home Video.exe
Play Games Online For FREE.exe
Ps2 Emulator.exe
Ps2 Iso 2 Rom Converter.exe
Shakira Dancing.exe
Soldier Of Fortune 2 Mutiplayer Serial Hack.exe
System Monitor.exe
The Sims Game Crack.exe
Universal Game Crack.exe
Warcraft 3 Battle.net Crack.exe
Website Hacker.exe
Win A Ps2.exe
Win An Xbox.exe
Winace.exe
Windows Hacker.exe
Winmx.exe
Winrar.exe
Winzip.exe
Working Iso Burner.exe
```

```
Xbox Emulator.exe
Xbox Iso 2 Rom Converter.exe
```

Then the worm writes several registry values in the [HKEY_CURRENT_USER\Software\Kazaa] registry key, so that the Media directory becomes available as a Kazaa shared directory.

P2P-Worm.Win32.Franvir

Aliases

P2P-Worm.Win32.Franvir (Kaspersky Lab) is also known as: Worm.P2P.Franvir (Kaspersky Lab), W32/Franriv.worm (McAfee), Franvir.Worm (Symantec), W32/Franriv-A (Sophos), WORM_FRANRIV.A (Trend Micro), Win32:Trojan-gen. (ALWIL), Win32.P2P.Franvir.A@mm (SOFTWIN), Worm Generic (Panda), Win32/Franvir.A (Eset)

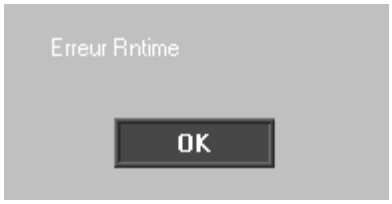
Detection added	Jun 20 2005 08:19 GMT
Update released	Jun 20 2005 09:04 GMT
Description added	Sep 20 2005
Behavior	P2P Worm

Technical details

This worm spreads via file-sharing networks. The worm itself is a Windows PE EXE file approximately 1274KB in size.

Installation

Once launched, the worm causes the following error message to be displayed:



On repeated launched, the worm will cause the error message below to be displayed:

When installing, the worm copies itself to the Windows root directory as "microsoftscanreg.exe":

```
%Windir%\microsoftscanreg.exe
```

It then registers this file in the system directory, ensuring that the worm will be launched each time Windows is rebooted on the victim machine:

```
[HKLM\Software\Microsoft\Windows\CurrentVersion\Run]
"Microsoft Scanreg" = "%Windir%\microsoftscanreg.exe"
```

Propagation via P2P

The worm checks to see if Kazaa is installed on the victim machine, and creates the following folder:

```
%Windir%\scanregfile\kazaa\My Shared Folder
```

The worm then copies itself to this folder under the following names:

```
Age Of Mythology FR CRACK.exe
Alcatraz Fr Crack.exe
Allopass + audiotel Keygen 2003.exe
Arx Fatalis FR CRACK.exe
Battlefield 1942 FR Crack.exe
Clone CD 5 keygen.exe
Delphi 5 fr crack keygen.exe
Delphi 6 fr crack keygen.exe
```

```
Delphi 7 fr crack keygen.exe
Dreamweaver MX keygen + crack by orran.exe
Fire-Works MX keygen + crack by orran.exe
Flash MX keygen + crack by orran.exe
Madden NFL 2003 FR CRACK.exe
Mafia Fr Nocd.exe
Medieval Total War Fr Crack.exe
Mega-Serial Microsoft Macromedia Borland Photoshop.exe
Nero FR 6 keygen + crack.exe
No One Lives Forever 2 FR CRACK.exe
Office XP fr Activation crack keygen.exe
Photoshop FR 7 keygen + crack by orran.exe
Sim City 4 FR Crack by zorio.exe
Unreal 2003 Fr Nocd.exe
Visual Basic fr 6.00 crack keygen.exe
Visual fr c++ crack keygen.exe
Visual.net fr Activation keygen crack.exe
Winace fr 4 keygen crack.exe
Windows XP Activation fr home Pro keygen 2003.exe
Windows XP fr home et pro SP1 crack.exe
Winrar fr 3.X keygen.exe
Winzip fr 8.X keygen crack.exe
```

The worm modifies the configuration of Kazaa in the system registry so the resources which are shared by default will include the folder created by the worm:

```
[HKCU\Software\Kazaa\LocalContent]
"DownloadDir" = "%Windir%\scanregfile\kazaa\My Shared Folder"
```

This means that other Kazaa users will be able to access these files.

P2P-Worm.Win32.Gotorm

Aliases

P2P-Worm.Win32.Gotorm (Kaspersky Lab) is also known as: Worm.P2P.Gotorm (Kaspersky Lab), W32/Gotorm.worm (McAfee), W32.HLLW.Gotorm (Symantec), Win32.HLLW.Gotorm (Doctor Web), W32/Gotorm-A (Sophos), Win32/HLLW.Gotorm.A (RAV), WORM_GOTORM.A (Trend Micro), Worm/Gotorm (H+BEDV), W32/Gotorm.A (FRISK), Win32:Gotorm (ALWIL), Worm/Gotorm.A (Grisoft), Win32.P2P.Gotorm.A@mm (SOFTWIN), Worm.P2P.Gotorm (ClamAV), Worm Generic (Panda), Win32/Gotorm.A (Eset)

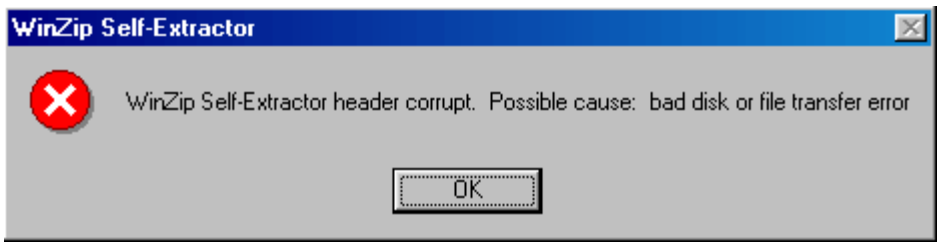
Description added	Aug 01 2003
Behavior	P2P Worm

Technical details

This is a Worm virus. It spreads through the peer-to-peer network Kazaa. Additionally, it performs some spying functions, gathering data on certain games installed on the affected PC. This worm is a Windows application (PE EXE-file). It is written in Visual C, and its size is 196 608 bytes.

Installation

During installation the worm produces the following false error message concerning the archive extraction:



Subsequently it writes itself into the Windows directory under the following name:

mrowyekdc.exe

This installation of the worm is then registered in the auto run key within the system registry:

```
HKLM\Software\Microsoft\Windows\CurrentVersion\Run
 SVCHOST = %WindowsDir%\mrowyekdc.exe
```

Spreading

The worm creates a folder named "User Files" in the Windows directory and writes itself into it under the following names:

Starcraft + Broodwar 1.10 map hack.exe
Starcraft + Broodwar 1.10 no-cd hack.exe
Diablo 2 map hack.exe
Diablo 2 no-cd hack.exe
Jamella's Diablo 2 hero editor.exe
Warcraft 3 map hack.exe
Warcraft 3 stat hack.exe
Warcraft 3 no-cd hack.exe
Warcraft 3 Frozen Throne map hack.exe
Warcraft 3 Frozen Throne cd-cd hack.exe
The Frozen Throne map hack.exe
Counterstrike hacks.exe
Counterstrike aim hack.exe

This folder is then noted in the Windows system registry as Local Content for the file exchange network Kazaa:

```
HKCU\Software\Kazaa\LocalContent
 dir0 = 012345:%Windir%\User Files
 DisableSharing = "0
```

As a result, the files contained in this folder become available for download to other users of P2P networks.

Spy function

The worm checks the system registry for keys relating to popular computer games (Counter Strike, Diablo, Warcraft, Starcraft) and sends gathered data to the worm's "owner" using an SMTP-server connection.

Miscellaneous

The worm checks the system's date and time. If the month of the worm's activation is earlier than August it ceases performing its functions and deletes all its entries in the system registry.

P2P-Worm.Win32.Harex.b

Other versions: .a, .c

Aliases

P2P-Worm.Win32.Harex.b (Kaspersky Lab) is also known as: Worm.P2P.Harex.b (Kaspersky Lab), Downloader-CG (McAfee), W32.HLLW.Genky (Symantec), Win32.HLLW.Genky (Doctor Web), W32/Genky-A (Sophos), Win32/HLLW.Genky (RAV), BKDR_NIVRAM.A (Trend Micro), Worm/Genky.P2P.2 (H+BEDV), Win32:Genky (ALWIL), Worm/Genky (Grisoft), Win32.Worm.P2P.Genky.A@mm (SOFTWIN), Worm Generic (Panda), Win32/Genky.A (Eset)

Description added	Sep 01 2003
Behavior	P2P Worm

Technical details

Harex.b (aka Genky) is about 4KB when compressed by FSG. The virus file is 33KB when uncompressed.

Installing

When installing, the worm creates a sub directory called 'windows' within the Windows directory and writes itself to this sub directory under the following names:

```
Ipswich Town Official Management Game - Update.exe
Ipswich Town Official Management Game - CD Crack.exe
Ipswich Town Official Management Game - Update Crack.exe
Ipswich Town Official Management Game - Cd Key Changer.exe
Ipswich Town Official Management Game - CD Key Generator.exe
Ipswich Town Official Management Game - CD Keygen.exe
Ipswich Town Official Management Game - Keygen.exe
Ipswich Town Official Management Game - NoCd.exe
Bridge Baron 13 - Update.exe
Bridge Baron 13 - CD Crack.exe
Bridge Baron 13 - Update Crack.exe
Bridge Baron 13 - Cd Key Changer.exe
Bridge Baron 13 - CD Key Generator.exe
Bridge Baron 13 - CD Keygen.exe
Bridge Baron 13 - Keygen.exe
Bridge Baron 13 - NoCd.exe
American Conquest - Update.exe
American Conquest - CD Crack.exe
American Conquest - Update Crack.exe
American Conquest - Cd Key Changer.exe
American Conquest - CD Key Generator.exe
American Conquest - CD Keygen.exe
American Conquest - Keygen.exe
American Conquest - NoCd.exe
Grom - Update.exe
Grom - CD Crack.exe
Grom - Update Crack.exe
Grom - Cd Key Changer.exe
Grom - CD Key Generator.exe
Grom - CD Keygen.exe
Grom - Keygen.exe
Grom - NoCd.exe
Alex Ferguson's Player Manager 2003 - Update.exe
Alex Ferguson's Player Manager 2003 - CD Crack.exe
Alex Ferguson's Player Manager 2003 - Update Crack.exe
Alex Ferguson's Player Manager 2003 - Cd Key Changer.exe
Alex Ferguson's Player Manager 2003 - CD Key Generator.exe
Alex Ferguson's Player Manager 2003 - CD Keygen.exe
Alex Ferguson's Player Manager 2003 - Keygen.exe
Alex Ferguson's Player Manager 2003 - NoCd.exe
Command and Conquer Generals - Update.exe
Command and Conquer Generals - CD Crack.exe
Command and Conquer Generals - Update Crack.exe
Command and Conquer Generals - Cd Key Changer.exe
Command and Conquer Generals - CD Key Generator.exe
Command and Conquer Generals - CD Keygen.exe
Command and Conquer Generals - Keygen.exe
Command and Conquer Generals - NoCd.exe
Nascar Racing 2003 Season - Update.exe
Nascar Racing 2003 Season - CD Crack.exe
Nascar Racing 2003 Season - Update Crack.exe
Nascar Racing 2003 Season - Cd Key Changer.exe
Nascar Racing 2003 Season - CD Key Generator.exe
Nascar Racing 2003 Season - CD Keygen.exe
Nascar Racing 2003 Season - Keygen.exe
Nascar Racing 2003 Season - NoCd.exe
Eonix Realm Of Hepmia - Update.exe
Eonix Realm Of Hepmia - CD Crack.exe
Eonix Realm Of Hepmia - Update Crack.exe
Eonix Realm Of Hepmia - Cd Key Changer.exe
Eonix Realm Of Hepmia - CD Key Generator.exe
Eonix Realm Of Hepmia - CD Keygen.exe
Eonix Realm Of Hepmia - Keygen.exe
Eonix Realm Of Hepmia - NoCd.exe
I Was An Atomic Mutant - Update.exe
```

I Was An Atomic Mutant - CD Crack.exe
I Was An Atomic Mutant - Update Crack.exe
I Was An Atomic Mutant - Cd Key Changer.exe
I Was An Atomic Mutant - CD Key Generator.exe
I Was An Atomic Mutant - CD Keygen.exe
I Was An Atomic Mutant - Keygen.exe
I Was An Atomic Mutant - NoCd.exe
Fetish Fighters - Update.exe
Fetish Fighters - CD Crack.exe
Fetish Fighters - Update Crack.exe
Fetish Fighters - Cd Key Changer.exe
Fetish Fighters - CD Key Generator.exe
Fetish Fighters - CD Keygen.exe
Fetish Fighters - Keygen.exe
Fetish Fighters - NoCd.exe
Battlefield 1942 The Road to Rome - Update.exe
Battlefield 1942 The Road to Rome - CD Crack.exe
Battlefield 1942 The Road to Rome - Update Crack.exe
Battlefield 1942 The Road to Rome - Cd Key Changer.exe
Battlefield 1942 The Road to Rome - CD Key Generator.exe
Battlefield 1942 The Road to Rome - CD Keygen.exe
Battlefield 1942 The Road to Rome - Keygen.exe
Battlefield 1942 The Road to Rome - NoCd.exe
The Campaigns of La Grande Armee - Update.exe
The Campaigns of La Grande Armee - CD Crack.exe
The Campaigns of La Grande Armee - Update Crack.exe
The Campaigns of La Grande Armee - Cd Key Changer.exe
The Campaigns of La Grande Armee - CD Key Generator.exe
The Campaigns of La Grande Armee - CD Keygen.exe
The Campaigns of La Grande Armee - Keygen.exe
The Campaigns of La Grande Armee - NoCd.exe
Unreal II The Awakening - Update.exe
Unreal II The Awakening - CD Crack.exe
Unreal II The Awakening - Update Crack.exe
Unreal II The Awakening - Cd Key Changer.exe
Unreal II The Awakening - CD Key Generator.exe
Unreal II The Awakening - CD Keygen.exe
Unreal II The Awakening - Keygen.exe
Unreal II The Awakening - NoCd.exe
The Emperors Mahjong - Update.exe
The Emperors Mahjong - CD Crack.exe
The Emperors Mahjong - Update Crack.exe
The Emperors Mahjong - Cd Key Changer.exe
The Emperors Mahjong - CD Key Generator.exe
The Emperors Mahjong - CD Keygen.exe
The Emperors Mahjong - Keygen.exe
The Emperors Mahjong - NoCd.exe
Sim City 4 - Update.exe
Sim City 4 - CD Crack.exe
Sim City 4 - Update Crack.exe
Sim City 4 - Cd Key Changer.exe
Sim City 4 - CD Key Generator.exe
Sim City 4 - CD Keygen.exe
Sim City 4 - Keygen.exe
Sim City 4 - NoCd.exe
Private Nurse - Update.exe
Private Nurse - CD Crack.exe
Private Nurse - Update Crack.exe
Private Nurse - Cd Key Changer.exe
Private Nurse - CD Key Generator.exe
Private Nurse - CD Keygen.exe
Private Nurse - Keygen.exe
Private Nurse - NoCd.exe
Impossible Creatures - Update.exe
Impossible Creatures - CD Crack.exe
Impossible Creatures - Update Crack.exe
Impossible Creatures - Cd Key Changer.exe
Impossible Creatures - CD Key Generator.exe
Impossible Creatures - CD Keygen.exe
Impossible Creatures - Keygen.exe
Impossible Creatures - NoCd.exe
Slot City 3 - Update.exe
Slot City 3 - CD Crack.exe
Slot City 3 - Update Crack.exe
Slot City 3 - Cd Key Changer.exe
Slot City 3 - CD Key Generator.exe
Slot City 3 - CD Keygen.exe
Slot City 3 - Keygen.exe
Slot City 3 - NoCd.exe
Test Drive - Update.exe
Test Drive - CD Crack.exe
Test Drive - Update Crack.exe
Test Drive - Cd Key Changer.exe
Test Drive - CD Key Generator.exe
Test Drive - CD Keygen.exe
Test Drive - Keygen.exe
Test Drive - NoCd.exe
Shadow of Memories - Update.exe
Shadow of Memories - CD Crack.exe
Shadow of Memories - Update Crack.exe
Shadow of Memories - Cd Key Changer.exe
Shadow of Memories - CD Key Generator.exe
Shadow of Memories - CD Keygen.exe
Shadow of Memories - Keygen.exe
Shadow of Memories - NoCd.exe
World Of Outlaws Sprint Car Racing 2002 - Update.exe
World Of Outlaws Sprint Car Racing 2002 - CD Crack.exe
World Of Outlaws Sprint Car Racing 2002 - Update Crack.exe
World Of Outlaws Sprint Car Racing 2002 - Cd Key Changer.exe
World Of Outlaws Sprint Car Racing 2002 - CD Key Generator.exe
World Of Outlaws Sprint Car Racing 2002 - CD Keygen.exe
World Of Outlaws Sprint Car Racing 2002 - Keygen.exe
World Of Outlaws Sprint Car Racing 2002 - NoCd.exe
Tombstone 1882 - Update.exe
Tombstone 1882 - CD Crack.exe
Tombstone 1882 - Update Crack.exe
Tombstone 1882 - Cd Key Changer.exe
Tombstone 1882 - CD Key Generator.exe

```
Tombstone 1882 - CD Keygen.exe
Tombstone 1882 - Keygen.exe
Tombstone 1882 - NoCd.exe
Las Vegas Casino Player's Collection - Update.exe
Las Vegas Casino Player's Collection - CD Crack.exe
Las Vegas Casino Player's Collection - Update Crack.exe
Las Vegas Casino Player's Collection - Cd Key Changer.exe
Las Vegas Casino Player's Collection - CD Key Generator.exe
Las Vegas Casino Player's Collection - CD Keygen.exe
Las Vegas Casino Player's Collection - Keygen.exe
Las Vegas Casino Player's Collection - NoCd.exe
Airport Tycoon II - Update.exe
Airport Tycoon II - CD Crack.exe
Airport Tycoon II - Update Crack.exe
Airport Tycoon II - Cd Key Changer.exe
Airport Tycoon II - CD Key Generator.exe
Airport Tycoon II - CD Keygen.exe
Airport Tycoon II - Keygen.exe
Airport Tycoon II - NoCd.exe
Filbert Fledgling - Update.exe
Filbert Fledgling - CD Crack.exe
Filbert Fledgling - Update Crack.exe
Filbert Fledgling - Cd Key Changer.exe
Filbert Fledgling - CD Key Generator.exe
Filbert Fledgling - CD Keygen.exe
Filbert Fledgling - Keygen.exe
Filbert Fledgling - NoCd.exe
Apache AH-64 Air Assault - Update.exe
Apache AH-64 Air Assault - CD Crack.exe
Apache AH-64 Air Assault - Update Crack.exe
Apache AH-64 Air Assault - Cd Key Changer.exe
Apache AH-64 Air Assault - CD Key Generator.exe
Apache AH-64 Air Assault - CD Keygen.exe
Apache AH-64 Air Assault - Keygen.exe
Apache AH-64 Air Assault - NoCd.exe
A+ Certification Test.exe
Cisco Certification Test.exe
MSCE Certification Test.exe
Unix Certification Test.exe
Windows Nt Certification Test.exe
Serious Sam - Gold Edition - Update.exe
Serious Sam - Gold Edition - CD Crack.exe
Serious Sam - Gold Edition - Update Crack.exe
Serious Sam - Gold Edition - Cd Key Changer.exe
Serious Sam - Gold Edition - CD Key Generator.exe
Serious Sam - Gold Edition - CD Keygen.exe
Serious Sam - Gold Edition - Keygen.exe
Serious Sam - Gold Edition - NoCd.exe
Global Power - Update.exe
Global Power - CD Crack.exe
Global Power - Update Crack.exe
Global Power - Cd Key Changer.exe
Global Power - CD Key Generator.exe
Global Power - CD Keygen.exe
Global Power - Keygen.exe
Global Power - NoCd.exe
IGI-2 Covert Strike - Update.exe
IGI-2 Covert Strike - CD Crack.exe
IGI-2 Covert Strike - Update Crack.exe
IGI-2 Covert Strike - Cd Key Changer.exe
IGI-2 Covert Strike - CD Key Generator.exe
IGI-2 Covert Strike - CD Keygen.exe
IGI-2 Covert Strike - Keygen.exe
IGI-2 Covert Strike - NoCd.exe
Tom Clancy's Splinter Cell - Update.exe
Tom Clancy's Splinter Cell - CD Crack.exe
Tom Clancy's Splinter Cell - Update Crack.exe
Tom Clancy's Splinter Cell - Cd Key Changer.exe
Tom Clancy's Splinter Cell - CD Key Generator.exe
Tom Clancy's Splinter Cell - CD Keygen.exe
Tom Clancy's Splinter Cell - Keygen.exe
Tom Clancy's Splinter Cell - NoCd.exe
Robot Arena Design And Destroy - Update.exe
Robot Arena Design And Destroy - CD Crack.exe
Robot Arena Design And Destroy - Update Crack.exe
Robot Arena Design And Destroy - Cd Key Changer.exe
Robot Arena Design And Destroy - CD Key Generator.exe
Robot Arena Design And Destroy - CD Keygen.exe
Robot Arena Design And Destroy - Keygen.exe
Robot Arena Design And Destroy - NoCd.exe
Freelancer - Update.exe
Freelancer - CD Crack.exe
Freelancer - Update Crack.exe
Freelancer - Cd Key Changer.exe
Freelancer - CD Key Generator.exe
Freelancer - CD Keygen.exe
Freelancer - Keygen.exe
Freelancer - NoCd.exe
```

The sub directory created by the worm is recorded in the Windows Registry as local content system files for Kazaa and iMesh:

```
HKCU\Software\Kazaa\LocalContent
HKCU\Software\Kazaa\Transfer
 dir0 = 012345:%Windir%\system\windows


HKCU\Software\iMesh\Client\LocalContent
 dir0 = 012345:%Windir%\system\windows
```

As a result of these entries, the files become available for download by other P2P network users.

Other

Version 'A' of the virus is downloaded and launched from the server 'cnets.0catch.com'. The virus is contained in a file called 'Kernell16.dll.exe',

which resides in a root level directory on the C: drive.

P2P-Worm.Win32.Harex.c

Other versions: .a, .b

Aliases

P2P-Worm.Win32.Harex.c (Kaspersky Lab) is also known as: Worm.P2P.Harex.c (Kaspersky Lab), Downloader-DO (McAfee), W32.Mexer.D.Worm (Symantec), Trojan.DownLoader (Doctor Web), W32/Dividend-A (Sophos), Win32/HLLW.Dividend (RAV), WORM_MEXER.D (Trend Micro), TR/SDBot.Drp.Gen (H+BEDV), W32/Harex.C (FRISK), Win32:Harex (ALWIL), Worm/Exebat.A (Grisoft), Win32.P2P.Harex.C@mm (SOFTWIN), Worm.P2P.Harex.C (ClamAV), W32/P2P.Harex.C (Panda), Win32/Harex.C (Eset)

Description added	Jun 11 2004
Behavior	P2P Worm

Technical details

This is a peer-to-peer worm, also known as Exebat. The worm file is about 2 KB in size, packed with FSG. The unpacked file is 17 KB in size.

Installation

During installation the worm creates a folder named "sys32" in the Windows system folder and copies itself to this folder under one of the following filenames:

```
All Adobe Products Keygen.exe
All Macromedia Products Keygen.exe
All Microsoft Products Keygen.exe
BurnDvds.exe
Divx Pro 5.1 Serial.exe
Dvd Plus Crack.exe
Dvd Ripper.exe
Dvd To Vcd.exe
Dvd Wizard Pro Crack.exe
Dvd Xcopy Crack.exe
DvdCopyOne Crack.exe
DvdToVcd Crack.exe
Easy Dvd creator Crack.exe
Easy Dvd Ripper.exe
EZ Dvd Ripper.exe
Nero Burning Rom Crack.exe
Nimo Codec Pack Updater.exe
Xvid Codec Installer.exe
```

This folder is then registered in the Windows system registry as Local Content for Kazaa and iMesh file sharing systems:

```
[HKCU\Software\Kazaa\LocalContent]
[HKCU\Software\Kazaa\Transfer]
"dir0"="012345:%Windir%\system\sys32"

[HKCU\Software\iMesh\Client\LocalContent]
"dir0"="012345:%Windir%\system\sys32"
```

Other details

As two previous Harex variants did, this worm downloads a file from the server cnet.0catch.com, saves it in the root folder of drive C: as autoexec.bat.Exe and executes it.

P2P-Worm.Win32.Hofox

Aliases

P2P-Worm.Win32.Hofox (Kaspersky Lab) is also known as: Worm.P2P.Hofox (Kaspersky Lab), W32/Generic.worm!p2p (McAfee), W32.HLLW.Hofox@mm (Symantec), Win32/HLLW.Hofox.A (RAV), WORM_HOFOX.A (Trend Micro), I-Worm/Hofox.E (Grisoft), Worm Generic (Panda), Win32/Hofox.A (Eset)

Description added	Jan 14 2004
Behavior	P2P Worm

Technical details

Hofox is a worm that spreads via P2P networks. Hofax is a Windows PE exe file; written in Visual Basic; about 49K in size.

During launch, the worm blocks the Norton Antivirus Auto Protect Service

Installation

Hofax registers itself as a launched application in the system registry key:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\worm

It then copies itself into:

C:\My shared folder\ under the following names:

Norton Anti-Virus 2004.exe
How To Hack.doc.exe
Win XP Pro .exe
Windows Longhorn full beta version.exe
Norton Anti-Virus keygen.exe
Hotmail H4x0r.exe
Halo - Combat Evolced.exe
DivX Pro .exe
Super Encrypt.exe
PornViewer.exe
Panda internet security.exe
Paint Shop Pro 8.exe
Paint Shop Pro 9 beta.exe
McAfee Anti-Virus.exe

C:\Windows\System32\ under the following names:

Norton Anti-Virus.exe
Halo.exe
Dunno.exe
Your Ad Here.exe
Girls Peeing.exe
Hacking is fun.exe

\Program Files\Accessories/Your Gay.exe

Manifestations

Launches:

- charmap.exe and notepad.exe
- Internet Explorer and connects to: http://www.ratemypoo.com

Destructive behaviour

Deletes files with the following extensions:

- *.jpg
- *.gif
- *.mov
- *.mpg
- *.mpeg
- *.avi
- *.doc
- *.pdf
- *.txt,/ul>

P2P-Worm.Win32.Irkaz

Aliases

P2P-Worm.Win32.Irkaz (Kaspersky Lab) is also known as: Worm.P2P.Irkaz (Kaspersky Lab), W32/Irkaz.worm!p2p (McAfee), W32.HLLW.Irkaz (Symantec), W32/Irkaz-A (Sophos), Win32/HLLW.Irkaz (RAV), WORM_IRKAZ.A (Trend Micro), W32/Irkaz.A (FRISK), Win32:PWNed (ALWIL), Worm/Irkaz.A (Grisoft), Win32.P2P.Irkaz.A@mm (SOFTWIN), Worm Generic (Panda), Win32/Irkaz.A (Eset)

Description added	Jul 08 2004
Behavior	P2P Worm

Technical details

This primitive, harmless virus is a Windows PE EXE file, written in C. It is 6176 bytes in size.

When lanching it copies itself to the Windows system directory and registers a file named netdll32 to the following registry keys:

```
[HKLM\Software\Microsoft\Windows\CurrentVersion\Run]
     [HKLM\Software\Microsoft\Windows\CurrentVersion\RunServices]
```

If the Kazaa P2P network is accessible, the worm will copy itself to the network under the name:

```
sex_xxx_teen_porn_teen_sex.jpg.exe
```

It will change the Internet Explorer home page.

P2P-Worm.Win32.Kazmor.a

Aliases

P2P-Worm.Win32.Kazmor.a (Kaspersky Lab) is also known as: Worm.P2P.Kazmor.a (Kaspersky Lab), W32/Kazmor.worm.gen!p2p (McAfee), W32.HLLW.Kazmor (Symantec), Win32.HLLW.Kazmor (Doctor Web), W32/Kazmor-A (Sophos), Win32/HLLW.Kazmor.A (RAV), WORM_KAZMOR.A (Trend Micro), Worm/Kazmor (H+BEDV), W32/Kazmor.A (FRISK), Worm/Kazmor.A (Grisoft), Win32.Worm.Kazmor.A (SOFTWIN), Worm Generic (Panda)

Description added	Aug 29 2002
Behavior	P2P Worm

Technical details

Kazmor is a P2P (peer to peer) and network worm with backdoor abilities. The worm itself is a Windows PE EXE file written in Delphi. Depending on the specific version the worm's size varies, however it is typically about 52KB or 56KB when it is compressed by the TeLock utility (the decompressed size is about 80-90KB).

This worm is very closely related to another worm - **Worm.Win32.Apart**.

Installing
While installing the Kazmor worm copies itself to the Windows system directory under either of these names:

"Kazmor.a": Windows.exe
"Kazmor.b": KERNEL32.VMM

It then sets "hidden" attributes for this file and registers it in the system registry auto-run key:

"Kazmor.a":

HKLM\Software\Microsoft\Windows\CurrentVersion\Run
Windows = %WindowsDir%\Windows.exe

"Kazmor.b":

HKLM\Software\Microsoft\Windows\CurrentVersion\Run
Windows Kernel = %WindowsDir%\KERNEL32.VMM

The **Kazmor.a** worm also hides itself in the system. It installs its own 'hooks' on Win32 API FindProcess/Modules functions and "skips" its process on these calls. Thus the worm's process is not visible in the active tasks list.

The **Kazmor.b** worm also creates the HKCR\.vmm key that is associated with the "exefile" file type. Thus '.VMM' files will be executed as original '.EXE' files.

Spreading
At the request of the worm's master's (see "Backdoor" below) the worm spreads over a local network or infects P2P shared folders.

Local network infection: the Kazmor worm opens network drives that are available for full access and copies itself to the \WINDOWS\Start Menu\Programs\StartUp\ directory under the name "REAL PLAYER.EXE".

P2P folders infection: Kazmor copies itself to the Kazaa and Morpheus folders with following names:

'preteen snuff sex rape with a stick hardcore.exe'
'violent preteen gang bang illegal.exe'
'teen tied up and raped.exe'
'teen raped in basement with dildo by 2 men.exe'
'14 year old on beach.exe'
'15 year old on beach.exe'
'16 year old on beach.exe'
'preteen sucking huge cock illegal.exe'
'illegal preteen porn anal fisting.exe'

'fetish bondage preteen porno.exe'
'jenna jameson sex scene huge dick blowjob.exe'
'nikki nova sex scene huge dick blowjob.exe'
'jenna jameson - built for speed.exe'
'cute girl giving head.exe'
'jenna jameson - shower scene.exe'
'jenna jameson - xxx nurse scene.exe'
'chubby girl fucked from all angles xxx.exe'
'[tmd]star wars episode 2 - attack of the clones [1of1].exe'
'[tmd]sum of all fears [1of1].exe'
'kill osama bin laden game.exe'
'caught on camera - man hit by car - faces of death.exe'
'CKY2K - Bam Margera.exe'
'CKY3 - Bam Margera.exe'
'chubby girl bukkake gang banged sucking cock.exe'
'brutal preteen porn xxx.exe'
'illegal porno - 15 year old raped by two men on boat.exe'
'windows xp key generator and cracker.exe'
'daniel pearl execution video gruesome and hardcore.exe'
'winzip key generator.exe'
'cat attacks child.exe'
'evil pranksters - light church on fire.exe'
'jesus game - really fun.exe'
'divx codec installer.exe'
'hot girl on the beach sucking cock and fucking guy.exe'
'devin in elevator sex.exe'
'microsoft office xp cracked.exe'
'microsoft visual studio 6.0.exe'
'microsoft .NET.exe'
'[DiVX] Lord of the rings.exe'
'[DiVX] Harry Potter and the sorcerors stone.exe'
'macromedia flash 5.0.exe'
'macromedia dreamweaver 4.0.exe'
'nuke afghanistan game.exe'
'Britney Spears Nude Cum.exe'
'Christina Agulera Nude Cum.exe'
'Christina Ricci Nude Cum.exe'
'AIM Password Stealer.exe'
'AIM Account Stealer.exe'
'AIM Account Hacker.exe'
'AIM Flooder.exe'
'MSN Password Hacker and Stealer.exe'
'MSN Flooder.exe'
'Hacking Tool Collection.exe'
'WinZip.exe'
'Windows XP.exe'
'Halflife Crack.exe.exe'
'Halflife Key Generator.exe.exe'
'Counterstrike Key Generator.exe.exe'
'Halflife and Counterstrike serial database.exe'
'DSL Modem Uncapper.exe'
'Cable Modem Uncapper.exe'
'T1 Modem Uncapper.exe'
'T3 Modem Uncapper.exe'
'DivX Install.exe'
'Two girls - Blonde and Brunette - Giving head.exe'
'How to hack.exe'
'How to hack websites.exe'
'Preteen Rape Sex Illegal - Jenny - 13 Years old.exe'
'Lolita preteen sex.exe'

'Bondage Fetish Foot Cum.exe'
'Blonde and Japanese girl bukkake.exe'
'Kill Osama Bin Ladin game.exe'
'Preteen lesbians.exe'
'Choke on cum (sodomy, rape).exe'
'Halflife and Counterstrike Cheating Death Hack!!!.exe'
'WebCam Voyeur Spy.exe.exe'
'FBI Spy Program.exe'
'XXX Porn Passwords.exe'
'Jenna Jameson Nude Gang Bang Forced Cum Blowjob.exe'
'CKY2K - Bam Margera Toy Machine.exe'
'CKY3 - Bam Margera World Industries Alien Workshop.exe'
'Chip and dale.exe'
'14 Year old webcam.exe
' '15 year old webcam.exe'
'16 year old webcam.exe'
'12 year old forced rape cum.exe'
'illgal incest preteen porn cum.exe'
'girls gone wild.exe'
'debby does dallas.exe'
'Devon - Elevator Scene.exe
' 'I Deep Throat - Kelly.exe'
'Another bang bus victim forced rape sex cum.exe'
'ZoneAlarm Firewall.exe'
'WinZip Key Generator and Crack.exe'
'How to be a terrorist - anarchist cookbook.exe'
'Government Secrets.exe'
'Nero Burning ROM [Cracked].exe'
'Internet and Computer Speed Booster.exe'
'Teen Violent Forced Gangbang.exe'
'PS1 Boot Disc.exe'
'Sony Play station boot disc.exe'
'PS2 Boot Disc.exe'
'Borland Delphi 5 Key Generator.exe'
'Borland Delphi 6 Key Generator.exe'

Backdoor
The backdoor routine allows a remote master to perform the following actions on victim computers:

- send out detailed computer information: drivers description, local date and time, default language, computer name, CPU speed and number of processors, RAM size, Windows version e.t.c.
- steal cached passwords, MSN account login and password, as well as .NET Messenger information.

Kazmor also performs the following routines, it:

- spreads over local networks and to P2P networks
- receives files or download files from a Web site
- executes a file
- performs DoS attacks on remote computers
- pings a remote computer
- scans ports and IP addresses
- redirects PC ports
- sends spam messages through AOL Instant Messenger and to a mIRC channel

Other
The Kazmor worm contains the *copyright* text string:

> Apartheid v.1.7 alpha copy. "50 Years later, you've still got an agenda, for world domination, but you better think again" - Vaginal Jesus.

P2P-Worm.Win32.Krepper.c

Aliases

P2P-Worm.Win32.Krepper.c (Kaspersky Lab) is also known as: Worm.P2P.Krepper.c (Kaspersky Lab), W32/Sndc.worm!p2p (McAfee), W32.IRCBot (Symantec), Win32.HLLW.Krepper (Doctor Web), W32/Ircbot-X (Sophos), Win32/HLLW.Krepper.B (RAV), WORM_SHAREBOT.A (Trend Micro), Worm/Krepper.C (H+BEDV), W32/Pcbot.A@p2p (FRISK), Win32:Mopy (ALWIL), Worm/Krepper.C (Grisoft), Win32.P2P.Poom.A (SOFTWIN), Worm.P2P.Poom.A (ClamAV), W32/Sndc.A.worm (Panda), Win32/Krepper.C (Eset)

Description added	Jul 15 2004
Behavior	P2P Worm

Technical details

This virus is written in C, and is a Windows PE EXE file, approximately 17KB in size, packed using UPX. The unpacked file is approximately 45KB in size.

On launch, the worm checks the victim machine for VMWare. If it is launched under VMWare, some of the malicious functions will not be executed.

Installation

When installing, the worm copies itself to the Windows system directory as sndcfg16.exe. It registers this file in the system registry to ensure this file is run each time the system is started:

```
[Software\Microsoft\Windows\CurrentVersion\Run]
     Services = <name of worm>
```

Propagation

This worm propagates via P2P networks. On launch, the worm scans the system registry, searching for any of the following clients which may be installed on the machine:

```
Altnet
Morpheus
iMesh
eDonkey2000
LimeWire
Kazaa
```

If the worm detects a P2P client, it will copy itself under a name chosen at random from the list below:

```
Ad-aware Pro Crack.exe
Adobe Acrobat Reader crack.exe
Adobe Golive v6.0 Keygen.exe
Adobe Illustrator v10.0 Time Limit Crack.exe
Adobe ImageReady v1.0 crack.exe
Adobe PageMaker v7.0 Keygen.exe
Adobe Photoshop 7 keygen.exe
Adobe Photoshop all.exe
Adobe Serial Generator v2.0.exe
Age of Empires II The Age of Kings NO CD crack.exe
Age Of Mythology -  The Titans no cd crack.exe
Age Of Mythology no cd crack.exe
Alias Acclaim crack.exe
All Macromedia Products Keygen.exe
Anti-Trojan 4.0.exe
Avant Browser.exe
Backyard Baseball 2003  no cd crack.exe
Backyard Wrestling 2 - There Goes the Neighborhood Eidos Interactive crack.exe
Battlefield 1942  no cd crack.exe
Battlefield Vietnam EA Games crack.exe
Battlefield Vietnam Multiplayer Online Crack.exe
Besieger Strategy DreamCatcher Interactive crack.exe
Blinx 2 - Masters of Time & Space Microsoft crack.exe
Blitzkrieg - Burning Horizon Strategy CDV Software GmbH crack.exe
Call of Duty Activision crack.exe
Call Of Duty no cd crack.exe
City of Heroes Role-Playing NCsoft crack.exe
Civilization III crack.exe
Classic NES Series - The Legend of Zelda GBA Role-Playing Nintendo crack.exe
CloneDVD v1.x crack.exe
Command & Conquer -  Generals no cd crack.exe
Command & Conquer -  Generals Zero Hour no cd crack.exe
Command & Conquer - Generals Zero Hour Strategy EA Games crack.exe
Counter-Strike Condition Zero Keygen.exe
Credit card generator.exe
Crusader Kings Strategy Paradox Entertainment crack.exe
```

Cubase Audio XT 3.X crack.exe
Dark Age Of Camelot - Trials Of Atlantis no cd crack.exe
Dark Matter - The Baryon Proj crack.exe
Deus Ex Invisible War NO CD Crack.exe
Diablo 2 NO CD crack.exe
Diablo 2 no cd crack.exe
DivX Player and Codec.exe
Doom 3 Activision crack.exe
Doom 3 NO CD Crack.exe
Download Accelerator Plus (spyware free).exe
Dragon Ball Z - Budokai 3 Atari crack.exe
Dragon Ball Z - Supersonic Warriors GBA Atari crack.exe
Dragon Warrior VIII Role-Playing Square Enix crack.exe
DRIV3R Atari crack.exe
Dungeon Lords Role-Playing DreamCatcher Interactive crack.exe
Dungeon Siege no cd crack.exe
Enter the Matrix Atari crack.exe
ESPN NFL 2K5 Sega crack.exe
F.E.A.R. VU Games crack.exe
Fable Role-Playing Microsoft crack.exe
Far Cry Ubisoft crack.exe
Final Fantasy VII - Advent Children PSP Role-Playing Square Enix crack.exe
Final Fantasy XI - Square Enix USA no cd crack.exe
Final Fantasy XII Role-Playing Square Enix crack.exe
Fire Emblem - Seima no Kouseki GBA Role-Playing Nintendo crack.exe
FlashFXP 2 RC2 Crack.exe
FlashFXP v1.4.1 Crack.exe
FlashFXP v1.4.3 Crack.exe
FlashFXP v2.0 Crack.exe
FlashFXP v2.1 crack.exe
FlashFXP v2.2 crack.exe
FlashGet.exe
Forgotten Realms - Demon Stone Atari crack.exe
Forgotten Realms - Demon Stone crack.exe ; 00405370 o
Freedom Force no cd crack.exe
Front Mission 4 Strategy Square Enix crack.exe
Full Spectrum Warrior Strategy THQ crack.exe
Geist GC Nintendo crack.exe
Goblin Commander - Unleash the Horde Strategy Jaleco Entertainment crack.exe
Gran Turismo 4 SCEA crack.exe
Grand Theft Auto - San Andreas Rockstar Games crack.exe
Grand Theft Auto 3 no cd crack.exe
Grand Theft Auto III no cd crack.exe
Grand Theft Auto San Andreas NO CD crack.exe
Grand Theft Auto Vice City NO CD crack.exe
GTA crack.exe
Half-Life 2 Keygen.exe
Half-Life 2 NO CD Crack.exe
Half-Life 2 VU Games crack.exe
Halo - Combat Evolved - Microsoft no cd crack.exe
Halo 2 crack.exe
Harry Potter & The Sorcerers Stone no cd crack.exe
Harry Potter and the Prisoner of Azkaban Adventure EA Games crack.exe
Harry Potter and the Sorcerers Stone no cd crack.exe
Heroes of Might & Magic IV no cd crack.exe
Hidden & Dangerous 2 NO CD Crack.exe
Icewind Dale 2 no cd crack.exe
ICQ 4.exe
ICQ Pro 2003b.exe
iMesh patch.exe
Jedi Academy NO CD Crack.exe
Joint Operations - Typhoon Rising NovaLogic crack.exe
Juiced Acclaim crack.exe
Kingdom Hearts II Role-Playing Square Enix crack.exe
Knights Apprentice Memoricks Adventures Games crack.exe
LimeWire server scanner.exe
Macromedia ColdFusion MX crack.exe
Macromedia Contribute v2.0 crack.exe
Macromedia Director 8 Crack.exe
Macromedia Dreamweaver 4.0 Patch.exe
Macromedia Dreamweaver MX v6.0 crack.exe
Macromedia Dreamweaver UltraDev 4.0 Patch.exe
Macromedia Fireworks 4.0 Patch.exe
Macromedia Flash All Versions keygen.exe
Macromedia Flash MX v6.0 crack.exe
Macromedia Flash SWF-Unprotect v2.0.exe
Macromedia FreeHand v10 Loader.exe
Madden NFL 2003 no cd crack.exe
Madden NFL 2005 EA crack.exe
Mafia no cd crack.exe
Malice Mud Duck Productions crack.exe
Mario Pinball Land GBA Puzzle Nintendo crack.exe
Mario Tennis GC Nintendo crack.exe
Matrix Screensaver.exe
Max Payne 2 Fall Of Max Payne no cd crack.exe
Max Payne 2 NO CD Crack.exe
Max Payne 2 The Fall of Max Payne NO CD crack.exe
MaxPayne 2 The Fall Of Max Payne Crack.exe
McFarlanes Evil Prophecy Konami crack.exe
Medal Of Honor - Allied Assault no cd crack.exe
Medal Of Honor - Allied Assault BreakThrough no cd crack.exe
Medal Of Honor - Allied Assault no cd crack.exe
Medal of Honor- Allied Assault no cd crack.exe
Medal of Honor Pacific Assault EA Games crack.exe
Medieval - Total War no cd crack.exe
Mega Man Anniversary Collection GC Capcom crack.exe
Metal Gear Acid PSP Strategy Konami crack.exe
Metal Gear Solid 3 - Snake Eater Konami crack.exe
Microsoft Flight Simulator 2004 - A Century Of Flight no cd crack.exe
Microsoft Office 2000 Regmaker.exe
Microsoft Office XP Activation Crack.exe
Microsoft Office XP Activation Killer.exe
Microsoft Office XP Professional Crack.exe
Microsoft Office XP Professional Serial.exe
Microsoft Office XP Universal Activator v1.0.exe
Midnight Club 3 - DUB Edition Rockstar Games crack.exe
mirc 6.1x reg entries.exe
mIRC 6.X crack.exe

Morpheus patch.exe
MS Office XP Activation Crack.exe
MS Zoo Tycoon no cd crack.exe
MSN advert remover.exe
MSN Toolbar advert remover.exe
MVP Baseball 2004 EA crack.exe
NBA Live 2003 crack.exe
NBA Live 2004 crack.exe
NCAA Football 2005 EA crack.exe
Need For Speed 5 - no cd.exe
Need for Speed Hot Pursuit 2 CD KeyGenerator.exe
Need for speed underground - nocd.exe
Need for Speed Underground 2 crack.exe
Need for Speed Underground 2 Electronic Arts crack.exe
Need for Speed Underground 2 NO CD crack.exe
Need for Speed Underground NO CD crack.exe
Need for Speed4 - NOCD.exe
NeedforspeedUnderground-nocd.exe
Nero Burning ROM v6.x crack.exe
Ninja Gaiden Tecmo crack.exe
Norton AntiVirus 2004 crack.exe
Onimusha 3 - Demon Siege Adventure Capcom crack.exe
Psi-Ops - The Mindgate Conspiracy Midway crack.exe
Purge Jihad Freeform Interactive LLC crack.exe
RealPlayer crack (keygen).exe
Red Dead Revolver Rockstar Games crack.exe
Resident Evil 4 GC Adventure Capcom crack.exe
Rise of Nations - Thrones & Patriots Strategy Microsoft crack.exe
RoboForm crack.exe
Roller Coaster Tycoon no cd crack.exe
RYL crack.exe
Second Life Role-Playing Linden Lab crack.exe
Shadow Ops - Red Mercury Atari crack.exe
ShellShock - Nam 67 Eidos Interactive crack.exe
Silent Storm - Sentinels Strategy _No Company crack.exe
Sim City 4 - Rush Hour no cd crack.exe
Sim City 4 Deluxe no cd crack.exe
Sim Theme Park World no cd crack.exe
Singles - Flirt Up Your Life Strategy Eidos Interactive crack.exe
Snood crack.exe
Snowblind Eidos Interactive crack.exe
Soldier of Fortune II- Double Helix no cd crack.exe
SolSuite 2004 - Solitaire Card Games Suite crack.exe
Sonic the Hedgehog 3 crack.exe
Spider-Man 2 Activision crack.exe
Spider-Man 2 GC Activision crack.exe
Sponge Bob Square Pants - Operation Krabby Patty no cd crack.exe
Spybot Search and Destroy.exe
Star Wars - Jedi Knight - Jedi Academy no cd crack.exe
Star Wars - Knights of the Old Republic Role-Playing LucasArts crack.exe
Star Wars Galactic Battlegrounds- Clone Campaigns no cd crack.exe
Star Wars Jedi Knight II - Jedi Outcast no cd crack.exe
Star Wars Jedi Knight II- Jedi Outcast no cd crack.exe
Star Wars Knights of the Old Republic II - The Sith Lords Role-Playing LucasArts
crack.exe
Starcraft - Battlechest no cd crack.exe
The Chronicles of Riddick - Escape From Butcher Bay VU Games crack.exe
The Elder Scrolls III - Morrowind Game of the Year Edition Role-Playing Bethesda
Softworks crack.exe'
The Legend of Zelda - Four Swords Adventures GC Nintendo crack.exe
The Legend of Zelda - The Minish Cap GBA Nintendo crack.exe
The Legend of Zelda (working title) GC Nintendo crack.exe
The Lord of the Rings The Battle for Middle-earth Strategy EA Games crack.exe
The Lord of the Rings The Return of The King crack.exe
The Sims - Hot Date Expansion Pack no cd crack.exe
The Sims - Makin Magic Expansion Pack no cd crack.exe
The Sims - Superstar Expansion Pack no cd crack.exe
The Sims - Unleashed Expansion Pack no cd crack.exe
The Sims - Vacation Expansion Pack no cd crack.exe
The Sims - Hot Date Expansion Pack no cd crack.exe
The Sims no cd crack.exe
The Sims - Vacation Expansion Pack no cd crack.exe
The Sims 2 crack.exe
The Sims Deluxe no cd crack.exe
The Sims Deluxe no cd crack.exe
The Sims Double Deluxe no cd crack.exe
The Sims no cd crack.exe
The Sims- Vacation no cd crack.exe
The Suffering Encore Software Inc. crack.exe
The Suffering Midway crack.exe
Thief - Deadly Shadows Eidos Interactive crack.exe
Tiger Woods PGA Tour 2004 crack.exe
Tom Clancys Ghost Recon - Desert Siege no cd crack.exe
Tom Clancy's Splinter Cell Pandora Tomorrow crack.exe
Tom Clancys Splinter Cell Pandora Tomorrow Ubisoft crack.exe
Tom Clancys Splinter Cell Ubisoft crack.exe
Tony Hawks Underground crack.exe
Trillian crasher.exe
Unreal Tournament 2003 no cd crack.exe
Unreal Tournament 2004 Atari crack.exe
Unreal Tournament 2004 crack (keygen).exe
Unreal Tournament 2004 NO CD crack.exe
Vampire - The Masquerade - Bloodlines Role-Playing Activision crack.exe
VirtualLab Data Recovery crack.exe
Warcraft III - Reign Of Chaos no cd crack.exe
Warez P2P.exe
Webroot Spy Sweeper.exe
windows server 2003 crack.exe
Windows XP Activation Crack.exe
Windows XP home edition Activation.exe
Windows XP Professional crack.exe
WinRAR crack (keygen).exe
WinZip All Versions keygen.exe
Winzip keygen.exe
WinZip Self-Extractor v2.2 keygen.exe
WinZip Self-Extractor v2.2 Patch.exe
WinZip v8.0 Keygen.exe
WinZip v8.x - v9.x patch.exe

```
WinZIP v9.0 Keygen.exe
WinZip v9.0 Registration.exe
World of Warcraft Role-Playing Blizzard Entertainment crack.exe
Worms Armageddon NO CD crack.exe
WWE Day of Reckoning GC THQ crack.exe
WWE SmackDown! vs. Raw THQ crack.exe
XBOX X-Fer Ripper and Transfer.exe
Yoshinoya Success crack.exe
ZoneAlarm crack (keygen).exe
Zoo Tycoon -  Complete Collection no cd crack.exe
Zoo Tycoon- Dinosaur Digs no cd crack.exe
Zoo Tycoon no cd crack.exe
```

In order to mask the fact that it is propagating, it pauses before starting to infect the next P2P network.

Once a P2P network is infected, the worm will search for folders with the following names:

```
share*
download*
music*
mp3*
```

Every ten minutes, the worm launches an infection routine affecting P2P networks.

It creates a BAT file on disk under a random name. This file, when launched, is designed to track when a user ends a process. When this happens, the BAT file will delete the worm's executable file from the disk.

The worm checks the system registry value every second.

It downloads and launches files from the Internet.

How it manifests itself in the system

In order to baffle users, depending on the name of the file the following error messages may be displayed during work with the computer:

```
Key Generator
    --------------
    Unable to load genereration tables.
    Check tables.gen is in current directory.

    Crack Engine
    ------------
    Unable to patch file.',0Ah,'Must be in same folder
```

The worm also connects to a number of IRC channels to inform the author of the worm about infected machines.

P2P-Worm.Win32.Lolol.a

Aliases

P2P-Worm.Win32.Lolol.a (Kaspersky Lab) is also known as: Worm.P2P.Lolol.a (Kaspersky Lab), W32/Lolol.worm.gen (McAfee), Win32.HLLW.Lolol.58400 (Doctor Web), W32/Lolol-A (Sophos), Win32/HLLW.Lolol.A (RAV), WORM_LOLOL.A (Trend Micro), Worm/Lolol.gen (H+BEDV), Win32:Trojan-gen. (ALWIL), Worm/Lolol (Grisoft), Win32.HLLW.Lolol.A (SOFTWIN), Trojan.Sdbot (ClamAV), W32/Lolol (Panda), Win32/Lolol.A (Eset)

Description added	May 27 2003
Behavior	P2P Worm

Technical details

Lolol is a worm virus spreading via the Kazaa file sharing network.

The worm has a powerful backdoor routine which connects to an IRC channel where it accepts commands from its "master" (person controlling the worm).

The worm itself is a Windows PE EXE file about 60KB in length and written in Microsoft Visual C++.

When the infected file is run an installation routine.

Installation

While installing the worm copies itself to the Windows system directory under the name "syscfg32.exe" and registers this file in two system registry auto-run keys:

HKLM\Software\Microsoft\Windows\CurrentVersion\Run
Configuration Loader = syscfg32.exe

HKLM\Software\Microsoft\Windows\CurrentVersion\RunServices
Configuration Loader = syscfg32.exe

Spreading

The "Lolol" worm copies itself to the following directories:

```
C:\program files\kazaa\my shared folder\
C:\program files\kazaa lite\my shared folder
C:\My Downloads\
```

Following are names "Lolol" copies itself under:

```
play station emulator crack.exe
play station emulator.exe
warcraft 3 serials.pif
warcraft 3 crack.exe
100 free essays school.pif
aol password cracker.exe
aim password cracker
aol cracker.exe
aim cracker.exe
steal usernames.exe
how to hack.exe
divx pro.exe
how to use a shell.pif
Virtua Girl (Full).exe
worldbook.exe
GTA 3 Serial.exe
GTA 3 Crack.exe
gta3.exe
driver.exe
virtua girl - adriana.pif
virtua girl - bailey short skirt.pif
```

...e.t.c. (there is a total of about 80 different names).

P2P-Worm.Win32.Mandragore

Aliases

P2P-Worm.Win32.Mandragore (Kaspersky Lab) is also known as: Worm.P2P.Mandragore (Kaspersky Lab), W32/Gnuman.worm (McAfee), Win32.Gnuman.8192 (Doctor Web), W32/GnutellaMan (Sophos), Win32/Gnuman.A (RAV), TROJ_GNUTELMAN.A (Trend Micro), Worm/Mandragore.1 (H+BEDV), W32/Gnuman.A (FRISK), Win32:GnuMan (ALWIL), I-Worm/Gnuman (Grisoft), Worm.Gnutella.Mandragore.A (SOFTWIN), Worm.Gnutella.MG (ClamAV), VBS/Gnutella (Panda), Win32/Gnuman.A (Eset)

Description added	Feb 27 2001
Behavior	P2P Worm

Technical details

This worm is Win32 application 8192 bytes of length, it is able to infect Win32 systems only. To spread from computer to computer the worm uses the Gnutella peer-to-peer (P2P) file sharing network (see http://gnutella.wego.com).

On infected computers the worm registers itself as Gnutella network node, listens to traffic of file requests and replies positive on these requests. The worm reports the file name that is being searched, but with EXE extension. If a remote user gets that reply and download the file, it gets a copy of the worm to its machine. The worm is not able to run by itself on remote computer, a user has to start the file to activate the worm routines.

While installing itself to the system the worm copies itself to Windows CurrentUser startup directory with "Gspot.exe" name and sets hidden and system attributes for that copy.

On next Windows startup the worm is automatically run by Windows (being placed in Startup folder), runs two threads (background processes) and stays in Windows memory. Under Win9x the worm also registers itself as a hidden (service) process (not visible in task list).

The worm's threads performs two actions:

The 1st thread reports "I'm Gnutella node, and here is file you are looking for."

The 2nd thread sends "the filename you are looking for" with ".exe" extension, and with worm code in it.

The worm code contains "copyright" text strings:

> [Gspot 1-]
> freely shared by mandragore/29A

P2P-Worm.Win32.Mareta

Aliases

P2P-Worm.Win32.Mareta (Kaspersky Lab) is also known as: Worm.P2P.Mareta (Kaspersky Lab), W32/Dabyrev (McAfee), Win32.HLLW.Marietta (Doctor Web), Win32/Dabyrev.A (RAV), PE_DABYREV.A (Trend Micro), W32/Dabyrev (FRISK), Win32:Mareta-UPX (ALWIL), Win32/Dabyrev.A (Grisoft), Win32.P2P.Mareta.A@mm (SOFTWIN), Worm Generic (Panda), Win32/Dabyrev.A (Eset)

Description added	Jan 15 2004
Behavior	P2P Worm

Technical details

This worm spreads via the Kazaa file-sharing network by infecting files.

The worm itself is a Windows PE EXE file, written in Delphi and packed using UPX. The packed file is 43008 bytes and the unpacked file is 209KB in size.

The worm changes the Internet browser home page.

Installation

When launched, the virus copies itself to the C:\ root directory and adds its own name to the following system registry key:

```
[HKLM\Software\Microsoft\Windows\CurrentVersion\Run]
```

thus ensuring the worm file will be launched every time Windows is restarted.

Signs of infection

The worm will cause the following message to be displayed:

```
[Marietta Virus]
[Mr. Splash]

    Hi and remember: pornography is _very bad_! HAPPY NEW YEAR!
```

P2P-Worm.Win32.Relmony.a

Aliases

P2P-Worm.Win32.Relmony.a (Kaspersky Lab) is also known as: Worm.P2P.Relmony.a (Kaspersky Lab), W32/Relmony.worm.a!p2p (McAfee), W32.HLLW.Relmony (Symantec), Win32.HLLW.Money.1 (Doctor Web), W32/Relmony-A (Sophos), Win32/HLLW.Relmony (RAV), WORM_RELMONY.A (Trend Micro), Worm/Relmony.A (H+BEDV), W32/Relmony.A (FRISK), Win32:RealMoney (ALWIL), Worm/Relmony.A (Grisoft), Win32.HLLW.RelMony.A (SOFTWIN), W32/P2PWorm.Gen (Panda), Win32/Relmony.A (Eset)

Description added	Aug 29 2002
Behavior	P2P Worm

Technical details

Relmony is an Internet worm that spreads in the Kazaa and Morpheus peer-to-peer file exchange networks. The Relmony worm replicates by copying itself into the "shared folders" on victim client machines which comprise these networks.

The Relmony worm is a Windows application (PE EXE file) about 29KB in size. It is written in Visual Basic.

Installation
Relmony copies itself to the Windows auto-startup directories with the following names (shown at the end of each string):

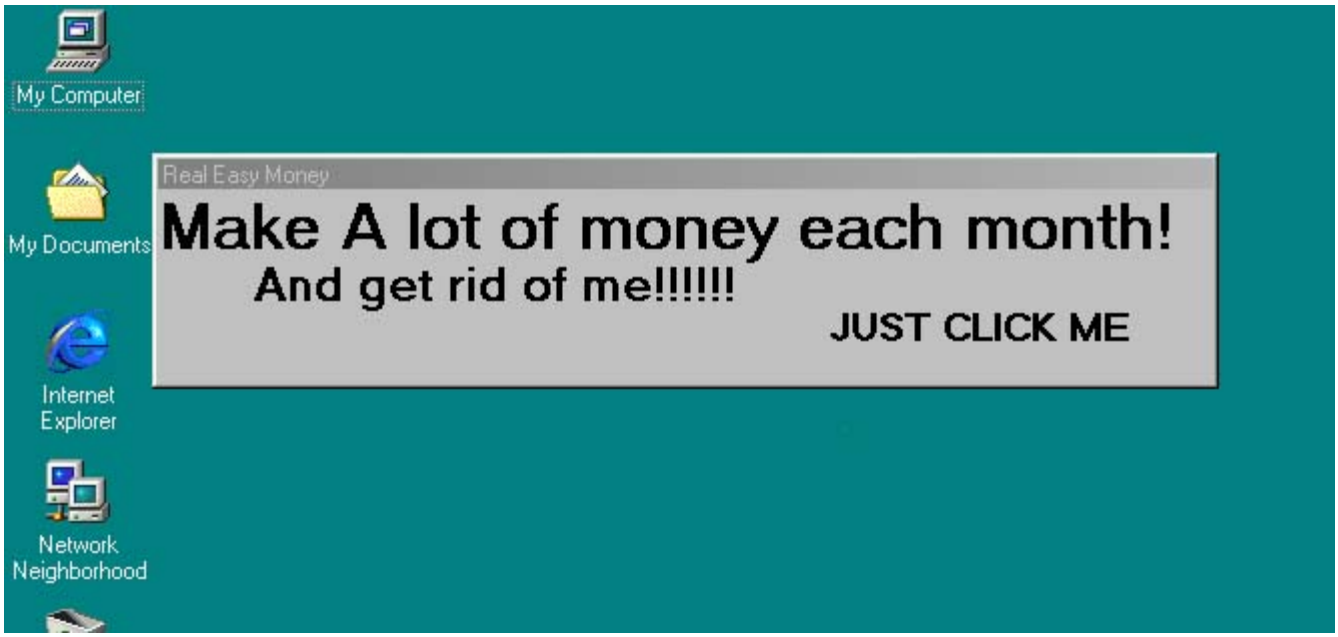
C:\WINNT\system32\config\systemprofile\StartMenu\Programs\Startup**system.exe**
C:\Documents and Settings\All Users\Start Menu\Programs\Startup**system.exe**
C:\WINDOWS\Start Menu\Programs\Startup**system.exe**

Replication
Relmony copies itself to P2P directories under the following names:

Note 1 - there is a typo for the spelling of the ***Morpheus*** network name

C:\Program Files\KaZaA\My Shared Folder\free_hot_porn_for_sale_pussy_hot-sex-butt-black-young-kiddy-music-movie-sum-of-fears.exe
C:\Program Files\KaZaA\My Shared Folder\free_hot_porn_for_sale_pussy_hot-sex-butt-black-young-kiddy-music-movie-sum-of-fears_3.exe
C:\Program Files\KaZaA\My Shared Folder\free_hot_porn_for_sale_pussy_hot-sex-butt-black-young-kiddy-music-movie-sum-of-fears_.exe
C:\Program Files\KaZaA\My Shared Folder\free_hot_porn_for_sale_pussy_hot-sex-butt-black-young-kiddy-music-movie-sum-of-fears_4.exe
C:\Program Files\Morpeus\My SharedFolder\free_hot_porn_for_sale_pussy_hot-sex-butt-black-young-kiddy-music-movie-sum-of-fears.exe
C:\Program Files\Morpeus\My Shared Folder\free_hot_porn_for_sale_pussy_hot-sex-butt-black-young-kiddy-music-movie-sum-of-fears_2.exe
C:\Program Files\Morpeus\My Shared Folder\free_hot_porn_for_sale_pussy_hot-sex-butt-black-young-kiddy-music-movie-sum-of-fears_.exe
C:\Program Files\Morpeus\My Shared Folder\free_hot_porn_for_sale_pussy_hot-sex-butt-black-young-kiddy-music-movie-sum-of-fears_4.exe

Other
After being installed the Relmony worm creates a window with the following text appearing:



This window slowly moves from the top-left desktop corner to the bottom-right.

***Clicking on this window and the worm runs the **join.php** script from the **http://www.ignifuge.com/getpaid** server.

The Relmony worm then creates a small blue button in top left desktop corner with the word *Money* written on it. ***Clicking on this button runs the same **PHP-script (join.php>** from the same server.

The button - *Money*

P2P-Worm.Win32.Scranor

Aliases

P2P-Worm.Win32.Scranor (Kaspersky Lab) is also known as: Worm.P2P.Scranor (Kaspersky Lab), W32/Scranor.worm (McAfee), W32.Narcs (Symantec), Win32.Scran.12800 (Doctor Web), Worm:Win32/Scranor.A (RAV), WORM_SCRANOR.A (Trend Micro), Worm/Scranor (H+BEDV), W32/Scranor.A (FRISK), Win32:Scranor (ALWIL), Worm/Sranor.A (Grisoft), Win32.Worm.P2P.Scranor.A (SOFTWIN), W32/Scranor.A.worm (Panda), Win32/Scranor.A (Eset)

Description added	Nov 17 2004
Behavior	P2P Worm

Technical details

This worm spreads via the Kazaa and iMesh file-sharing networks, and also via IRC.

The worm itself is a Windows PE EXE file, approximately 12KB in size.

Installation

Once launched, the worm creates a folder called "Sys32i" in the Program Files directory, and copies itself to this file as "Scran.exe".

This file is registered in the system registry as a key to enable autorun:

```
[HKLM\Software\Microsoft\Windows\CurrentVersion\Run]
  W32.Scran = %ProgramDir%\sys32i\Scran.exe
```

This ensures that the worm will be launched each time the system is rebooted.

The worm creates several more copies of itself under the following names:

```
Age of Empires crack.exe
Age of Empires.exe
CD Key.exe
Counter Strike 6.exe
Counter Strike.exe
Grand Theft Auto 3 CD2 ISO.exe
Half-Life.exe
Hotmail account cracker.exe
Hotmail Hack.exe
KeyGen.exe
Microsoft Office.exe
Norton Anti Virus 2004.exe
Norton Anti Virus 2005.exe
Norton Anti Virus Crack.exe
Norton Firewall.exe
Norton Internet Security 2004.exe
Partition Magic 8.exe
Playstation 2.exe
Resident Evil.exe
Scran.cpl
Tomb Raider.exe
Trojan Remover.exe
Windows XP Home.exe
Yahoo Hack.exe
ZoneAlarm Firewall Pro.exe
```

This folder will be shown in the system registry as Local Content for Kazaa and iMesh:

```
[HKCU\Software\Kazaa\LocalContent]
[HKCU\Software\Kazaa\Transfer]
  "dir0" = "012345:%ProgramDir%\sys32i"\

[HKCU\Software\iMesh\Client\LocalContent]
  "dir0" = "012345:%ProgramDir%\sys32i\"
```

These files will then be accessible to other users of the P2P networks.

The worm creates an identifier "W32.Scran-Worm" to flag its presence in the system.

Propagation via IRC

The worm searches the victim machine for an IRC client. If it detects one, it will change the contents of the "script.ini" file so that the worm will be passed to all users who enter IRC channels used by the infected machine.

Other

The worm will download a file named "botnet.jpg" from http://www.freewebs.com. This file will be saved in the C: root directory as "botnet.exe". This file contains the latest version of Backdoor.Win32.Rbot.gen.

On the 1st January, the worm will cause a dialogue box containing the following text to be displayed on the screen:

```
Ha?
Happy New Year W32.Scran!!
```

P2P-Worm.Win32.SdDrop.a

Aliases

P2P-Worm.Win32.SdDrop.a (Kaspersky Lab) is also known as: Worm.P2P.SdDrop.a (Kaspersky Lab), W32/Sddrop.worm.a!p2p (McAfee), W32.HLLW.Kamesh (Symantec), Win32.SdDrop.1 (Doctor Web), W32/SdDrop-A (Sophos), Win32/HLLW.SdDrop.A (RAV), WORM_SDDROP.A (Trend Micro), Worm/SdDrop.P2P.A (H+BEDV), W32/SdDrop.A (FRISK), Win32:SdDrop-C (ALWIL), Worm/Sddrop (Grisoft), Win32.HLLW.Sddrop.A (SOFTWIN), Worm.P2P.SdDrop (ClamAV), W32/P2P.Sddrop (Panda), Win32/Sddrop.A (Eset)

Description added	Jan 12 2004
Behavior	P2P Worm

Technical details

This worm spreads via the KaZaA and iMesh filesharing networks. It drops and runs Backdoor.Sdbot.gen. The worm is compressed using ASPack and is approximately 25Kb in size.

Installation
On execution, the worm copies itself to %System%\Xms32.exe. It extracts the file Backdoor.Sdbot.gen and drops it to %System%\Xms32.tmp.exe. The worm then creates the folder %Windir%\sCache32 and copies itself to this folder under the following file names:

2 Find MP3 8.2.0.exe
AC3-MP3 converter.exe
ACDSee 5.5b.exe
ACDSee Classic 2.79.exe
Ad-aware 6.5 (new)Download Accelerator Plus 6.3.exe
Adobe Acrobat Reader 5.6.exe
Adobe PhotoShop 7.1 crack.exe
All Editor 3.0b.exe
AOL Instant Messenger 6.1.exe
Auction Sentry (new).exe
AudioLabel CD Labeler 3.0 (+crack).exe
Battlefied1942 Pack4 (crack+bloodpatch).exe
BearShare 5.1.1.exe
C&C Generals Pack2 (new patch).exe
Complete UK Music Database 4.2.exe
DirectDVD 4.9.exe
DivX Bundle 6.2.exe
DivX edit (new).exe
DivX Video Bundle 5.5.1.exe
DvD Rip guide (+tools) st0rm.exe
Dynamite Downloads.exe
Easy CD Creator Software Update.exe
FlashFXP (keygen).exe
FreeRip 4.30.exe
Genie Stream 3.2.4.exe
GetRight 5.5 + crack.exe
Global DiVX Player 2.0.1.exe
Gothic 2 (m-patch).exe
Grokster 2.0.exe
Hacker Tutorial (by ph3Akz).exe
Half-Life keygen (+ogc hack).exe
HL keys (working).exe
I.G.I. 2 (new crack).exe
ICQ Lite beta (b2253).exe
ICQ Pro 2003a beta (b4600).exe
iMesh 4.1 beta.exe

iSnipeIt 5.0c.exe
James Bond 007 Nightfire crack.exe
Kazaa Media Desktop 2.5.exe
Kazaa Skins 1.8.exe
KaZooM MP3 Kazaa Accelerator 2.5.exe
Medal Of Honor (Allied Assault) crack.exe
Microangelo 6.0b.exe
mIRC 6.x addon patch.exe
mIRC s3th war-script.exe
Morpheus 2.6.exe
MP3 cut pro 3.0.exe
MSN Messenger 5.5.10.exe
Need for Speed 6 (new cars + crack).exe
NeoNapster 3.92.exe
Nero Burning ROM 5.8.2.4.exe
Network Cable + ADSL Speed 2.0 (beta).exe
New Nvidia (geForce) drivers (beta).exe
Nimo Codec Pack 9.0 (stable).exe
Nvidia Detonator XP Drivers (Windows XP/2000).exe
Operation Flashpoint (bloopatch).exe
Patch Creator 3.5a.exe
PhotoShow 3.1.exe
Pop-Up Stopper 4.0 (beta).exe
Ps2 to Pc tutorial (+tool).exe
QuickTime 7.2 (new).exe
Raven Shield 5.32 crack.exe
RealJukebox Basic 2.8.exe
RealOne Free Player 2.8.exe
RemoteSpy 1.5.exe
Sim City 4 crack.exe
Splinter Cell crack.exe
TitJiggle (flash game).exe
Trillian 0.8 + plugins.exe
UniversalFlood (4.8b).exe
Unreal2 (2.8) crack.exe
UT2003 multi-crack (new).exe
Warcraft3 battle.net(2.5) crack.exe
Window Washer 4.8.exe
WinMX 3.5.1.exe
WinRAR 3.8.exe
WinZip 8.3b (crack).exe
WinZip 9.0 SR-1.exe
Wippit 2.1 (beta).exe
WS_FTP LE 6.0.exe
XViD bundle (codec+tutorial).exe

The worm registers itself in the system registry auto-run key:

```
HKCU\Software\Kazaa\LocalContent
HKCU\Software\iMesh\Client\LocalContent
 "Dir? 012345:"="%Windir%\sCache32"
 "DisableSharing"="0"
```

so that other KaZaA or iMesh users can download files from the %Windir%\sCache32 folder.

P2P-Worm.Win32.Spear.a

Aliases

P2P-Worm.Win32.Spear.a (Kaspersky Lab) is also known as: Worm.P2P.Spear.a (Kaspersky Lab), W32/Spear.worm.a!p2p (McAfee), W32.HLLW.Yoohoo (Symantec), Win32.HLLW.Spreader.1 (Doctor Web), W32/Speedup-Fam (Sophos), Win32/HLLW.Yoohaa (RAV), WORM_REDERPS.A (Trend Micro), Worm/Spear.B (H+BEDV), W32/Spear.G (FRISK), Win32:Spear (ALWIL), Worm/Spear.A (Grisoft), Win32.Worm.Spear.A (SOFTWIN), Worm.P2P.Spear.J (ClamAV), W32/Spear (Panda), Win32/Spear.A (Eset)

Description added	Aug 29 2002
Behavior	P2P Worm

Technical details

Spear is an Internet worm that spreads in the Kazaa, Morpheus, BearShare and eDonkey2000 peer-to-peer (P2P) file exchange networks. It replicates by copying itself into the 'shared folders' used on all client machines comprising these networks.

The Spear worm is a Windows application (PE EXE file) about 40-70KB in size (depending on its version) and is written in Delphi. Some instances of this worm are compressed by the UPX file compression utility.

Spear does not manifest itself in any way.

The worm copies itself to P2P directories using the following names:

host_faker.exe
host_spoofer.exe
ip_spoofer.exe
ip_faker.exe
ident_spoofer.exe
ident_faker.exe
tripod_hacker.exe
tripod_cracker.exe
hotmailhacker.exe
hotmailcracker.exe
hotmail_account_sniffer.exe aimhacker.exe
aimcracker.exe
icqhacker.exe
icqcracker.exe
msnhacker.exe
msncracker.exe
winxp_hacker.exe
winxp_cracker.exe
winxphack.exe
winxp_crack.exe
win2k_serial.exe
yahoo_cracker.exe
yahoo_hacker.exe
divx_fix.exe
divx_repair.exe
ftp_hacker.exe
ftp_cracker.exe
porn_account_hacker.exe
porn_account_cracker.exe
catherine_zeta_jones_nude.exe
catherine_zeta_jones_naked.exe
catherine_zeta_jones_anal.exe
pamela_anderson_anal.exe
pamela_anderson_nude.exe pamela_anderson_naked.exe
buttman.exe

sarah_michelle_gellar_nude.exe
sarah_michelle_gellar_naked.exe
sandra_bullock_nude.exe
sandra_bullock_naked.exe
anastasia_anal.exe
anastasia_naked.exe
anastasia_nude.exe
shakira_anal.exe
shakira_assfucked.exe
shakira_naked.exe
shakira_nude.exe
shakira_paparazzi_collection.exe
XP_keygen.exe
PS2_emulator_bleem.exe
xbox_emulator_beta.exe
linux_root.exe
win2k_pass_decryptor.exe
Win2k_reboot_exploit.exe
IIS_shellbind_exploit.exe
AdvZip Recovery.exe
AIM Pass stealer.exe
AMI BIOS Cracker.exe
Counter Strike_CD_Keygen.exe
Delphi 5 Keygen.exe
Delphi 6 Keygen.exe
Half_life Cd keygen.exe
Hotmail Hacker.exe
ICQ_Hackingtools.exe
invisible_IP.exe
kazaa.exe
edonkey_serverlist.exe
kmd151_en.exe
Linux_rootaccess.exe
msn_IP_finder.exe
Office key Gen.exe
Autocad 2002 Crack.exe
OfficeXP_Keygen.exe
Office XP Crack.exe
PS1 BootCD.exe
PS2 BootCD.exe
XP_Box_emulator.exe
Sub7_masterpwd.exe
Windows_Keygen_allver.exe
WinXP_Keygen.exe
Winzip_Pass_Cracker.exe
Word_Pass_Cracker.exe
XP DVD Plugin.exe
XP ScreenSaver.exe
Yahoo_mail_cracker.exe
Pokemon.exe
Digimon.exe
exegen.exe

P2P-Worm.Win32.SpyBot.a

Aliases

P2P-Worm.Win32.SpyBot.a (Kaspersky Lab) is also known as: Worm.P2P.SpyBot.a (Kaspersky Lab), W32/Spybot.worm.gen.a (McAfee), W32.Spybot.Worm (Symantec), Win32.HLLW.SpyBot (Doctor Web), W32/Spybot-Fam (Sophos), Win32/HLLW.SpyBot.A (RAV), Possible_Virus (Trend Micro), Worm/Spybot.43552 (H+BEDV), W32/Spybot.A (FRISK), Win32:SpyBot-GEN4 (ALWIL), Worm/Spybot (Grisoft), Win32.P2P.SpyBot.D9B5D8A7 (SOFTWIN), Trojan.Spybot.gen-2 (ClamAV), W32/Spybot.gen.worm (Panda), Win32/SpyBot.A (Eset)

Description added	May 27 2003
Behavior	P2P Worm

Technical details

SpyBot is a peer-to-peer worm with backdoor capabilities that can also spread via computers infected with some Backdoor programs. The worm is a Windows PE EXE file that is written in Visual C++.

Installation

While installing itself the worm copies itself to the Windows system directory and sets the *Hidden* attribute for its copy. This file is then registered in the system registry in the following auto-run key entries:

```
HKLM\Software\Microsoft\Windows\CurrentVersion\Run
HKLM\Software\Microsoft\Windows\CurrentVersion\RunOnce
```

On Windows 9x machines the worm hides itself from the task list.

SpyBot also tries to kill some firewalls and anti-virus programs.

Spreading

During the installation process, SpyBot copies itself to the **kazaabackupfiles** subdirectory in the Windows system directory and registers it as a subdirectory for Kazaa shared files.

Additionally, upon request by the worm's master (controller), the worm searches the Internet for hosts infected with the malicious programs **Backdoor.Kuang and Backdoor.SubSeven** and uploads itself to these hosts.

Backdoor

The backdoor routine allows a remote master (person or people controlling the worm's backdoor functions) to perform the following actions:

- get detailed computer information including the names of the running processes
- steal cached passwords in Windows 9x
- download a file from a Web site
- delete, rename, or execute a file
- perform DoS attack on remote computer
- scan ports and IP addresses

Other

The SpyBot worm can run a hidden HTTP server on infected machines. It also establishes a keyboard spy (code that records all key strokes a user makes on an infected machine) and, upon its master's request, sends the log file of all keyboard actions to the master.

P2P-Worm.Win32.Surnova.a

Other versions: .k, .p, .t

Aliases

P2P-Worm.Win32.Surnova.a (Kaspersky Lab) is also known as: Worm.P2P.Surnova.a (Kaspersky Lab), W32/Supova.worm!p2p (McAfee), W32.Supova.Worm (Symantec), Win32.HLLW.Supernova.40960 (Doctor Web), W32/Surnova-A (Sophos), Win32/Supova.A.worm (RAV), WORM_SURNOVA.A (Trend Micro), Worm/Surnova.P2P (H+BEDV), W32/Supova.H@p2p (FRISK), Win32:Surnova-C (ALWIL), Worm/Surnova (Grisoft), Win32.Worm.Supova.I (SOFTWIN), Worm.P2P.Surnova.A (ClamAV), W32/Supova (Panda), Win32/Surnova.Z (Eset)

Description added	Jul 30 2002
Behavior	P2P Worm

Technical details

This is a worm that replicates using Windows Messenger and Kazaa network software. It replicates by copying itself to the Kazaa shared folder and by sending its copies via the Windows Messenger.

Installation
When the worm is launched for the first time, it tries to copy itself to the Windows directory with one of the following names:

Alles-ist-vorbei.exe Desktop-shooting.exe Hello-Kitty.exe BigMac.exe Cheese-Burger.exe Blaargh.exe

The worm sets its copy to be executed automatically when Windows starts by writing the following registry value:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run Supernova=(one of the file names specified above)

The worm also shows a fake error message.

Replication: Kazaa network

Surnova tries to obtain the name of the Kazaa shared directory from the system registry. If it doesn't exist it uses the Media folder located in the Windows directory instead of the Kazaa shared directory name. Then it copies itself to that directory under the following names:

```
Windows XP key generator.exe
Windows XP serial generator.exe
Key generator for all windows XP versions.exe
Warcraft 3 ONLINE key generator.exe
Half-life ONLINE key generator.exe
Quake 4 BETA.exe
Grand theft auto 3 CD1 crack.exe
GTA3 crack.exe
Battle.net key generator (WORKS!!).exe
Warcraft 3 battle.net serial generator.exe
Half-life WON key generator.exe
Star wars episode 2 downloader.exe
Winzip 8.0 + serial.exe
Winrar + crack.exe
Britney spears nude.exe
Macromedia MX key generator (all products).exe
```

P2P-Worm.Win32.Surnova.k

Other versions: .a, .p, .t

Aliases

P2P-Worm.Win32.Surnova.k (Kaspersky Lab) is also known as: Worm.P2P.Surnova.k (Kaspersky Lab), W32/Supova.worm!p2p (McAfee), W32.Supova.Worm (Symantec), Win32.HLLW.Supernova.45056 (Doctor Web), W32/Surnova-H (Sophos), Win32/Supova.G.worm (RAV), WORM_SURNOVA.K (Trend Micro), Worm/Surnova.K (H+BEDV), W32/Spuova.M@p2p (FRISK), Win32:Supov (ALWIL), Worm/Surnova (Grisoft), Win32.Worm.Supova.K (SOFTWIN), W32/Supova.K (Panda), Win32/Surnova.K (Eset)

Description added	Oct 24 2007
Behavior	P2P Worm

Technical details

This network worm spreads via file-sharing networks. It propagates by creating copies of itself in publicly accessible Kazaa directories, and also sends copies of itself via Windows Messenger. It is a Windows PE EXE file. It is 45056 bytes in size.

Installation

When launched, the worm causes the following error message to be displayed:

The worm then copies its executable file to the Windows root directory under one of the following names:

```
%WinDir%\BigMac.exe
%WinDir%\Alles-ist-vorbei.exe
%WinDir%\Desktop-shooting.exe
%WinDir%\Hello-Kitty.exe
%WinDir%\Cheese-Burger.exe
%WinDir%\Blaargh.exe
```

In order to ensure that the worm is launched automatically when the system is rebooted, the worm adds a link to its executable file to the system registry:

```
[HKLM\Software\Microsoft\Windows\CurrentVersion\Run]

"Supernova" = "%WinDir%\<name of worm file>.exe"
```

Payload

The worm copies its executable file to the following folder:

```
%WinDir%\Media
```

under the following names:

```
Windows XP key generator.exe
Windows XP serial generator.exe
Key generator for all windows XP versions.exe
Warcraft 3 ONLINE key generator.exe
Half-life ONLINE key generator.exe
Quake 4 BETA.exe
```

```
Grand theft auto 3 CD1 crack.exe
GTA3 crack.exe
Battle.net key generator (WORKS!!).exe
Warcraft 3 battle.net serial generator.exe
Half-life WON key generator.exe
Star wars episode 2 downloader.exe
Winzip 8.0 + serial.exe
Winrar + crack.exe
Britney spears nude.exe
Macromedia MX key generator (all products).exe
KaZaA media desktop v2.0 UNOFFICIAL.exe
Microsoft key generator, works for ALL microsoft products!!.exe
Microsoft Windows XP crack pack.exe
Hack into any computer!!.exe
DivX codec v6.0.exe
DivX newest version.exe
DivX.exe
DivX pro key generator.exe
Key generator for over 1,000 applications (really!).exe
DivX patch - Increases quality.exe
KaZaA spyware remover.exe
Age of empires 2 crack.exe
Norton antivirus 2002.exe
Macromedia Dreamweaver MX Key Generator.exe
Macromedia Flash MX Key Generator.exe
Microsoft Office XP (english) key generator.exe
Microsoft Office XP.iso.exe
CloneCD + crack.exe
CloneCD all-versions key generator.exe
XBOX emulator (WORKS!!).exe
Gamecube Emulator (WORKS!!).exe
Xbox.info.exe
Spiderman CD 1 of 2.exe
Spiderman CD 2 of 2.exe
Blade 2 [DVD Quality].exe
```

The worm also copies its executable file under the names shown above to the folder which the following registry key parameter links to:

```
[HKLM\Software\Kazaa\LocalContent]

"Dir0"
```

The worm also spreads via a vulnerability in MSN Messenger which makes it possible to download files to the victim machine without the knowledge or consent of the user. In order to do this, the worm sends a message with a malcrafted header to all MSN contacts. The copy of the worm is accompanied by one of the following messages:

```
Hehe, check this out :-)
Funny, check it out (h)
LOL!! See this :D
LOL!! Check this out :)
Hehe, this is fun :-)
```

The worm also deletes all files from the C: root directory.

Removal instructions

If your computer does not have an up-to-date antivirus, or does not have an antivirus solution at all, follow the instructions below to delete the malicious program:

1. Use Task Manager to terminate the worm process.
2. Delete the original worm file (the location will depend on how the program originally penetrated the victim machine).
3. Delete the following system registry key value:

   ```
   [HKLM\Software\Microsoft\Windows\CurrentVersion\Run]

   "Supernova" = "%WinDir%\<name of worm file>.exe"
   ```

4. Delete the copies of the worm:

   ```
   %WinDir%\BigMac.exe
   %WinDir%\Alles-ist-vorbei.exe
   %WinDir%\Desktop-shooting.exe
   %WinDir%\Hello-Kitty.exe
   %WinDir%\Cheese-Burger.exe
   %WinDir%\Blaargh.exe
   ```

5. Delete all copies of the worm from the hard disk.
6. Update your antivirus databases and perform a full scan of the computer (download a trial version of Kaspersky Anti-Virus).

P2P-Worm.Win32.Surnova.p

Other versions: .a, .k, .t

Aliases

P2P-Worm.Win32.Surnova.p (Kaspersky Lab) is also known as: Worm.P2P.Surnova.p (Kaspersky Lab), W32/Supova.worm!p2p (McAfee), W32.Supova.Worm (Symantec), Win32.HLLW.Generic.51 (Doctor Web), W32/Surnova-G (Sophos), Win32/Supova.G.worm (RAV), WORM_SURNOVA.P (Trend Micro), Worm/Surnova.P (H+BEDV), W32/Spuova.Q@p2p (FRISK), Win32:Ultranova (ALWIL), Worm/Surnova (Grisoft), Win32.Worm.Supova.P (SOFTWIN), Worm Generic (Panda), Win32/Surnova.P (Eset)

Description added	Oct 24 2007
Behavior	P2P Worm

Technical details

This network worm spreads via file-sharing networks. It propagates by creating copies of itself in publicly accessible Kazaa directories, and also sends copies of itself via Windows Messenger. It is a Windows PE EXE file. It is 45056 bytes in size.

Installation

When launched, the worm causes the following error message to be displayed:

The worm then copies its executable file to the Windows root directory under one of the following names:

```
%WinDir%\Look-at-This!!!!.exe
%WinDir%\Look-at-My-Pussy.exe
%WinDir%\How-Are-You.exe
%WinDir%\YoUMaD.exe
%WinDir%\You-Are-WeirD.exe
%WinDir%\Blaargh.exe
```

In order to ensure that the worm is launched automatically when the system is rebooted, the worm adds a link to its executable file to the system registry:

```
[HKLM\Software\Microsoft\Windows\CurrentVersion\Run]

"Ultranova" = "%WinDir%\<name of worm file>.exe"
```

Payload

The worm copies its executable file to the following folder:

```
%WinDir%\Media
```

under the following names:

```
Windows XP key generator.exe
Windows XP serial generator.exe
Key generator for all windows XP versions.exe
Warcraft 3 ONLINE key generator.exe
Half-life ONLINE key generator.exe
Quake 4 BETA.exe
```

```
Grand theft auto 3 CD1 crack.exe
GTA3 crack.exe
Battle.net key generator (WORKS!!).exe
Warcraft 3 battle.net serial generator.exe
Half-life WON key generator.exe
Star wars episode 2 downloader.exe
Winzip 8.0 + serial.exe
Winrar + crack.exe
Britney spears nude.exe
Macromedia MX key generator (all products).exe
KaZaA media desktop v2.0 UNOFFICIAL.exe
Microsoft key generator, works for ALL microsoft products!!.exe
Microsoft Windows XP crack pack.exe
Hack into any computer!!.exe
DivX codec v6.0.exe
DivX newest version.exe
DivX.exe
DivX pro key generator.exe
Key generator for over 1,000 applications (really!).exe
DivX patch - Increases quality.exe
KaZaA spyware remover.exe
Age of empires 2 crack.exe
Norton antivirus 2002.exe
Macromedia Dreamweaver MX Key Generator.exe
Macromedia Flash MX Key Generator.exe
Microsoft Office XP (english) key generator.exe
Microsoft Office XP.iso.exe
CloneCD + crack.exe
CloneCD all-versions key generator.exe
XBOX emulator (WORKS!!).exe
Gamecube Emulator (WORKS!!).exe
Xbox.info.exe
Spiderman CD 1 of 2.exe
Spiderman CD 2 of 2.exe
Blade 2 [DVD Quality].exe
```

The worm also copies its executable file under the names shown above to the folder which the following registry key parameter links to:

```
[HKLM\Software\Kazaa\LocalContent]

"Dir0"
```

The worm also spreads via a vulnerability in MSN Messenger which makes it possible to download files to the victim machine without the knowledge or consent of the user. In order to do this, the worm sends a message with a malcrafted header to all MSN contacts. The copy of the worm is accompanied by one of the following messages:

```
Hehe, check this out :-)
Funny, check it out (h)
COOL! See this :D
COOL! Check this out :)
Hehe, this is fun :-)
```

The worm also creates a file with a random name of 11 numbers and with an .exe extension in %WinDir%. This files contains the following text:

```
W32.Ultranova
-----------------------------------------------------
      'Patch the leaks or the ship will sink'
-----------------------------------------------------
```

The worm also deletes all files from the C: root directory.

Removal instructions

If your computer does not have an up-to-date antivirus, or does not have an antivirus solution at all, follow the instructions below to delete the malicious program:

1. Use Task Manager to terminate the worm process.
2. Delete the original worm file (the location will depend on how the program originally penetrated the victim machine).
3. Delete the following system registry key value:

   ```
   [HKLM\Software\Microsoft\Windows\CurrentVersion\Run]

   "Ultranova" = "%WinDir%\<name of worm file>.exe"
   ```

   Delete the copies of the worm:

   ```
   %WinDir%\Look-at-This!!!!.exe
   %WinDir%\Look-at-My-Pussy.exe
   %WinDir%\How-Are-You.exe
   %WinDir%\YoUMaD.exe
   %WinDir%\You-Are-WeirD.exe
   %WinDir%\Blaargh.exe
   ```

4. Delete all copies of the worm from the hard disk.
5. Update your antivirus databases and perform a full scan of the computer (download a trial version of Kaspersky Anti-Virus).

P2P-Worm.Win32.Surnova.t

Other versions: .a, .k, .p

Aliases

P2P-Worm.Win32.Surnova.t (Kaspersky Lab) is also known as: Worm.P2P.Surnova.t (Kaspersky Lab), W32/Supova.worm!p2p (McAfee), W32.Supova.Worm (Symantec), Win32.HLLW.Supernova.45056 (Doctor Web), W32/Surnova-G (Sophos), Win32/Supova.G.worm (RAV), WORM_SURNOVA.T (Trend Micro), Worm/Surnova.G (H+BEDV), W32/Spuova.W@p2p (FRISK), Win32:Surnova (ALWIL), Worm/Surnova (Grisoft), Win32.P2P.Surnova.T@mm (SOFTWIN), Win32.Supova.worm (ClamAV), Win32/Surnova.T (Eset)

Description added	Oct 24 2007
Behavior	P2P Worm

Technical details

This network worm spreads via file-sharing networks. It propagates by creating copies of itself in publicly accessible Kazaa directories, and also sends copies of itself via Windows Messenger. It is a Windows PE EXE file. It is 46080 bytes in size.

Installation

When launched, the worm causes the following error message to be displayed:

The worm then copies its executable file to the Windows root directory under one of the following names:

```
%WinDir%\I-Love-You-Guys!.exe
%WinDir%\Look-at-My-Pussy.exe
%WinDir%\How-Are-You.exe
%WinDir%\YoUMaD.exe
%WinDir%\You-Are-WeirD.exe
%WinDir%\Blaargh.exe
```

In order to ensure that the worm is launched automatically when the system is rebooted, the worm adds a link to its executable file to the system registry:

```
[HKLM\Software\Microsoft\Windows\CurrentVersion\Run]

"Buttsnova" = "%WinDir%\<name of worm file>.exe"
```

Payload

The worm copies its executable file to the following folder:

```
%WinDir%\Media
```

under the following names:

```
Windows XP key generator.exe
Windows XP serial generator.exe
Key generator for all windows XP versions.exe
Warcraft 3 ONLINE key generator.exe
Half-life ONLINE key generator.exe
Quake 4 BETA.exe
```

```
Grand theft auto 3 CD1 crack.exe
GTA3 crack.exe
Battle.net key generator (WORKS!!).exe
Warcraft 3 battle.net serial generator.exe
Half-life WON key generator.exe
Star wars episode 2 downloader.exe
Winzip 8.0 + serial.exe
Winrar + crack.exe
Britney spears nude.exe
Macromedia MX key generator (all products).exe
KaZaA media desktop v2.0 UNOFFICIAL.exe
Microsoft key generator, works for ALL microsoft products!!.exe
Microsoft Windows XP crack pack.exe
Hack into any computer!!.exe
DivX codec v6.0.exe
DivX newest version.exe
DivX.exe
DivX pro key generator.exe
Key generator for over 1,000 applications (really!).exe
DivX patch - Increases quality.exe
KaZaA spyware remover.exe
Age of empires 2 crack.exe
Norton antivirus 2002.exe
Macromedia Dreamweaver MX Key Generator.exe
Macromedia Flash MX Key Generator.exe
Microsoft Office XP (english) key generator.exe
Microsoft Office XP.iso.exe
CloneCD + crack.exe
CloneCD all-versions key generator.exe
XBOX emulator (WORKS!!).exe
Gamecube Emulator (WORKS!!).exe
Xbox.info.exe
Spiderman CD 1 of 2.exe
Spiderman CD 2 of 2.exe
Blade 2 [DVD Quality].exe
```

The worm also copies its executable file under the names shown above to the folder which the following registry key parameter links to:

```
[HKLM\Software\Kazaa\LocalContent]

"Dir0"
```

The worm also spreads via a vulnerability in MSN Messenger which makes it possible to download files to the victim machine without the knowledge or consent of the user. In order to do this, the worm sends a message with a malcrafted header to all MSN contacts. The copy of the worm is accompanied by one of the following messages:

```
Hehe, check this out :-)
Funny, check it out (h)
COOL! See this :D
COOL! Check this out :)
Hehe, this is fun :-)
```

The worm also creates a file with a random name of 11 numbers and with an .exe extension in %WinDir%. This files contains the following text:

```
W32.Buttsnova
-----------------------------------------------------
      'Patch the leaks or the ship will sink'
-----------------------------------------------------
```

The worm also deletes all files from the C: root directory.

Removal instructions

If your computer does not have an up-to-date antivirus, or does not have an antivirus solution at all, follow the instructions below to delete the malicious program:

1. Use Task Manager to terminate the worm process.
2. Delete the original worm file (the location will depend on how the program originally penetrated the victim machine).
3. Delete the following system registry key value:

   ```
   [HKLM\Software\Microsoft\Windows\CurrentVersion\Run]

   "Buttsnova" = "%WinDir%\<name of worm file>.exe"
   ```

4. Delete the copies of the worm:

   ```
   %WinDir%\I-Love-You-Guys!.exe
   %WinDir%\Look-at-My-Pussy.exe
   %WinDir%\How-Are-You.exe
   %WinDir%\YoUMaD.exe
   %WinDir%\You-Are-WeirD.exe
   %WinDir%\Blaargh.exe
   ```

5. Delete all copies of the worm from the hard disk.
6. Update your antivirus databases and perform a full scan of the computer (download a trial version of Kaspersky Anti-Virus).

P2P-Worm.Win32.Tanked.a

Aliases

P2P-Worm.Win32.Tanked.a (Kaspersky Lab) is also known as: Worm.P2P.Tanked.a (Kaspersky Lab), W32/Sddrop.worm.b!p2p (McAfee), Trojan dropper (Symantec), Win32.HLLW.Tanked.12 (Doctor Web), W32/Kwbot-D (Sophos), TrojanDropper:Win32/Assasin (RAV), WORM_KWBOT.D (Trend Micro), Worm/Tanked.A (H+BEDV), W32/Tanked.A (FRISK), Win32:Tanked (ALWIL), Worm/Tanked.A (Grisoft), Win32.Worm.P2P.Pac.A (SOFTWIN), Worm.P2P.Tanked.D (ClamAV), W32/Tanked.A (Panda), Win32/Tanked.A (Eset)

Description added	May 27 2003
Behavior	P2P Worm

Technical details

Tanked is a worm virus spreading via the Kazaa file sharing network.

The worm has a powerful backdoor routine that connects to an IRC channel and listens to commands from its "master".

The worm itself is a Windows PE EXE file about 100KB in length and written in Microsoft Visual C++. The worm is compressed by the UPX file compression utility and then encrypted with the "Krypton" Win EXE file encryptor.

When the infected file is run, the installation routine gains control.

Installation
While installing the worm copies itself to the Windows system directory under different names (see below) and registers the file in two system registry auto-run keys.

Worm-copy names are:

```
"Tanked.11":    "system32.exe"
"Tanked.13":    "winsys.exe"
"Tanked.14":    "cmd32.exe"
```

The registry keys are:

```
"Tanked.11":

    HKLM\Software\Microsoft\Windows\CurrentVersion\Run
      SystemSAS = system32.exe

    HKLM\Software\Microsoft\Windows\CurrentVersion\RunServices
      SystemSAS = system32.exe

"Tanked.13":

    HKLM\Software\Microsoft\Windows\CurrentVersion\Run
      WinSys = winsys.exe

    HKLM\Software\Microsoft\Windows\CurrentVersion\RunServices
      WinSys = winsys.exe

"Tanked.14":

    HKLM\Software\Microsoft\Windows\CurrentVersion\Run
      CMD = cmd32.exe

    HKLM\Software\Microsoft\Windows\CurrentVersion\RunServices
      CMD = cmd32.exe
```

Spreading
The worm copies itself to the Kazaa directory with following names:

```
'Battlefield1942_bloodpatch.exe'
'Unreal2_bloodpatch.exe'
'UT2003_bloodpatch.exe'
'AquaNox2 Crack.exe'
'NBA2003_crack.exe'
'FIFA2003 crack.exe'
'C&C Generals_crack.exe'
'UT2003_keygen.exe'
'UT2003_no cd (crack).exe'
'Age of Empires 2 crack.exe'
'Anno 1503_crack.exe'
'C&C Renegade_crack.exe'
'Diablo 2 Crack.exe'
'Gothic 2 licence.exe'
'GTA 3 Crack.exe'
'GTA 3 patch (no cd).exe'
```

```
'Hitman_2_no_cd_crack.exe'
'Mafia_crack.exe'
'Neverwinter_Nights_licence.exe'
'NHL 2003 crack.exe'
'WarCraft_3_crack.exe'
'Splinter_Cell_Crack.exe'
'Battlefield1942_keygen.exe'
'Winamp 3.8.exe'
'MediaPlayer Update.exe'
'UT2003_patch.exe'
'ACDSee 5.5.exe'
'DivX Video Bundle 6.5.exe'
'Global DiVX Player 3.0.exe'
'QuickTime_Pro_Crack.exe'
'KaZaA Lite (New).exe'
'iMesh 3.7b (beta).exe'
'iMesh 3.6.exe'
'KaZaA Hack 2.5.0.exe'
'DirectDVD 5.0.exe'
'Flash MX crack (trial).exe'
'Ad-aware 6.5.exe'
'WinZip 9.0b.exe'
'SmartFTP 2.0.0.exe' 'ICQ Lite (new).exe'
'ICQ Pro 2003b (new beta).exe'
'ICQ Pro 2003a.exe'
'AOL Instant Messenger.exe'
'Download Accelerator Plus 6.1.exe'
'Trillian 0.85 (free).exe'
'MSN Messenger 5.2.exe'
'Network Cable e ADSL Speed 2.0.5.exe'
'mIRC 6.40.exe'
'GetRight 5.0a.exe'
'Pop-Up Stopper 3.5.exe'
'Yahoo Messenger 6.0.exe'
'KaZaA Speedup 3.6.exe'
'Nero Burning ROM crack.exe'
'WindowBlinds 4.0.exe'
'Animated Screen 7.0b.exe'
'Living Waterfalls 1.3.exe'
'Matrix Screensaver 1.5.exe'
'Popup Defender 6.5.exe'
'Space Invaders 1978.exe'
'SmartRipper v2.7.exe'
'TweakAll 3.8.exe'
'DVD Copy Plus v5.0.exe'
'Serials 2003 v.8.0 Full.exe'
'Zelda Classic 2.00.exe'
'Need 4 Speed crack.exe'
'Links 2003 Golf game (crack).exe'
'Netfast 1.8.exe'
'Guitar Chords Library 5.5.exe'
'DVD Region-Free 2.3.exe'
'Cool Edit Pro v2.55.exe'
'Coffee Cup Free HTML 7.0b.exe'
'Clone CD 5.0.0.3.exe'
'Clone CD 5.0.0.3 (crack).exe'
'Nimo CodecPack (new) 8.0.exe'
'Business Card Designer Plus 7.9.exe'
'Steinberg_WaveLab_5_crack.exe'
'Hot Babes XXX Screen Saver.exe'
'FreeRAM XP Pro 1.9.exe'
'IrfanView 4.5.exe'
'Audiograbber 2.05.exe'
'WinOnCD 4 PE_crack.exe'
'Final Fantasy VII XP Patch 1.5.exe'
'BabeFest 2003 ScreenSaver 1.5.exe'
'PalTalk 5.01b.exe'
'DirectX Buster (all versions).exe'
'DirectX InfoTool.exe'
'Unreal2_crack.exe'
'FlashGet 1.5.exe'
'Babylon 3.50b reg_crack.exe'
'mp3Trim PRO 2.5.exe'
```

Other

'Tanked' has "copyright" text strings:

```
"Tanked.11":

    T~Drone.11
    t69 [sd]v0.5b TankEd.11
    [sd]v0.5b TankEd.11 by [sd]

"Tanked.13":

    T~Drone.13
    t69 [sd]v0.5b TankEd.13
    [sd]v0.5b TankEd.13 by [sd]

"Tanked.14":

    T~Drone.14
    t69 [sd]v0.5b TankEd.14
    [sd]v0.5b TankEd.14 by [sd]
```

P2P-Worm.Win32.Tibick.f

Aliases

P2P-Worm.Win32.Tibick.f (Kaspersky Lab) is also known as: W32.Tibick (Symantec), Win32.HLLW.Tibic (Doctor Web), WORM_TIBICK.C (Trend Micro), Worm/Tibick.f.2 (H+BEDV), Worm/Tibick.F (Grisoft), Win32.Worm.P2P.Tibick.F (SOFTWIN), Worm.P2P.Tibick.F (ClamAV), W32/Tibick.C.worm (Panda), Win32/Tibick.G (Eset)

Detection added	Jan 17 2005
Description added	Jan 27 2005
Behavior	P2P Worm

Technical details

This worm spreads via file-sharing networks. The worm itself is a Windows file approximately 14KB in size, packed using UPX. The unpacked file is approximately 35KB in size.

Installation

Once launched, the worm copies itself to the Windows system directory as 'svcnet.exe':

```
%System%\svcnet.exe
```

It then registers itself in the system registry:

```
[HKLM\Software\Microsoft\Windows\CurrentVersion\Run]
[HKCU\Software\Microsoft\Windows\CurrentVersion\Run]
"Shellapi32" = "svcnet.exe"
```

This ensures that a copy of the worm will be run each time the victim machine is rebooted.

Propagation via P2P

The worm creates a new directory called 'msview' in the Windows system file. It then copies itself to this folder under the following names:

- 321 Studios GamesXCopy 1.0.8 Crack.exe
- 3D Slot Car Racing Game 1.0.exe
- 3D Studio Max 6 Crack.exe
- ABBY FineReader Pro 7.0 Crack.exe
- acdsee 7.0.61 Crack.exe
- ACDSee PowerPack 7.0.43 Crack.exe
- ACDSee v7.0 Powerpack 7.0 Crack.exe
- Ad-aware Pro Crack.exe
- Ad-aware Professional.exe
- Ad-aware.exe
- Adobe Acrobat Reader crack.exe
- Adobe Acrobat Reader.exe
- Adobe After Effects PRO v6.5 Crack.exe
- Adobe Golive v6.0 Keygen.exe
- Adobe Illustrator v10.0 Time Limit Crack.exe
- Adobe ImageReady v1.0 crack.exe
- Adobe PageMaker v7.0 Keygen.exe
- Adobe Photoshop 7 keygen.exe
- Adobe Photoshop CS 8 Crack .exe
- Adobe Photoshop CS Crack .exe
- Adobe Photoshop Universal Crack .exe
- Adobe Serial Generator v2.0.exe
- Adult Tetris 2 Crack .exe
- Age of Empires II The Age of Kings NO CD crack.exe
- Age Of Mythology - The Titans no cd crack.exe
- Age Of Mythology no cd crack.exe
- Agnitum Outpost Firewall 2.5.369 Crack.exe
- Ahead Nero Burning 6.6.0.3 Ultra Edition Keygen .exe
- AlbumWrap Extractor v1.0.exe
- AlbumWrap.exe
- Alcohol 120% v1.9.2 build 1705 Crack.exe
- Alias Acclaim crack.exe
- All Macromedia Products Keygen.exe
- All-in-One Secretmaker.exe
- Anti-Trojan 4.0.exe
- AnyDVD 3.9.2.1 Crack.exe

- AnyDVD 4.0.4.1 Keygen.exe
- AOL Instant Messenger (AIM).exe
- AquaZone Desktop Garden 1.0.1.1 full Crack.exe
- Ares Galaxy.exe
- Ares Lite.exe
- Ashampoo WinOptimizer Platinum Suite 2 2.01.exe
- Avant Browser.exe
- Babylon Pro 5x Crack.exe
- Backyard Baseball 2003 no cd crack.exe
- Backyard Wrestling 2 - There Goes the Neighborhood crack.exe
- Battlefield 1942 no cd crack.exe
- Battlefield Vietnam crack.exe
- Battlefield Vietnam Multiplayer Online Crack.exe
- Besieger DreamCatcher Interactive crack.exe
- BitComet.exe
- BitSpirit 1.2.0 RC3.exe
- Blindwrite Suite 4.5.3 Crack.exe
- Blinx 2 - Masters of Time & Space Microsoft crack.exe
- Blitzkrieg - Burning Horizon CDV Software GmbH crack.exe
- C&C Generals Crack.exe
- Call Of Duty no cd crack.exe
- CCALG - Credit Card Generator.exe
- CD to MP3 Freeware 1.5 .exe
- Chicken Invaders 2 2.60 .exe
- City of Heroes NCsoft crack.exe
- Civilization III crack.exe
- Classic NES Series - The Legend of Zelda GBA Nintendo crack.exe
- Clone DVD 2 Crack.exe
- CloneCD 5.x Crack.exe
- CloneCD All Version KeyGen.exe
- CloneDVD v1.x crack.exe
- CloneDVD v3.x Retail Crack.exe
- CloneDVD2 v2.x Crack.exe
- Command & Conquer - Generals no cd crack.exe
- Command & Conquer - Generals Zero Hour no cd crack.exe
- Command and Conquer - Generals Zero Hour crack.exe
- Cool Edit 2000 1.1.exe
- CopyToDVD 3.0.3 Crack.exe
- Corel Draw Graphics Suite 12.0 Crack.exe
- Counter-Strike Condition Zero Keygen.exe
- Crusader Kings Paradox Entertainment crack.exe
- Cubase Audio XT 3.X crack.exe
- CWShredder 2.12 .exe
- CyberLink PowerDVD v6.0 Deluxe7 Crack .exe
- Dark Age Of Camelot - Trials Of Atlantis no cd crack.exe
- Dark Matter - The Baryon Proj crack.exe
- dBpowerAmp Music Converter.exe
- DC++ 0.668.exe
- Deus Ex Invisible War NO CD Crack.exe
- DFX Audio Enhancement 2.0.1 Crack.exe
- Diablo 2 NO CD crack.exe
- Dialupass 2.43 Crack.exe
- DivX Player (with DivX Codec).exe
- DivX Player Crack.exe
- dMSN mercury messenger 1.7.0.6.exe
- Doom 3 Crack.exe
- Doom 3 NO CD Crack.exe
- Doom 3 SDK Keygen.exe
- Dope Wars Crack.exe
- Download Accelerator Plus 7.3.exe
- Download Accelerator Plus V7.1 Crack.exe
- Download Accelerator Plus v7.2 Premium Crack.exe
- Download Accelerator Plus.exe
- Dr Divx Crack.exe
- Dr.Divx 1.0.6 Build 105 Crack.exe
- Dragon Ball Z - Budokai 3 crack.exe
- Dragon Ball Z - Supersonic Warriors crack.exe
- Dragon Warrior VIII crack.exe
- DRIV3R crack.exe
- Drug Wars - Underworld 1.3.exe
- Dungeon Lords DreamCatcher Interactive crack.exe
- Dungeon Siege no cd crack.exe
- DVD Decrypter 3.5.1.0.exe
- DVD Region-Free 5.5 Crack.exe
- DVD Shrink 3.2.0.15.exe
- DVDXCopy Platinum 4.0.3.8 Crack.exe
- Easy CD-DA Extractor 7.1.3.1 Crack.exe
- Easy CD-DA Extractor 7.13.2 Keygen.exe
- eIMAGE Recovery 3.0.exe
- eMule 0.44b.exe
- eMule.exe
- Enter the Matrix Atari crack.exe
- ESPN NFL 2K5 Sega crack.exe
- Exe Icon Changer 3.753.exe
- F.E.A.R. crack.exe
- Fable Microsoft crack.exe
- Far Cry crack.exe
- Fifa 2005 Crack.exe

- Final Fantasy VII - Advent Children crack.exe
- Final Fantasy XI - USA no cd crack.exe
- Final Fantasy XII crack.exe
- Fire Emblem - Seima no Kouseki crack.exe
- FlashFXP 2 RC2 Crack.exe
- FlashFXP All Version KeyGen.exe
- FlashFXP v1.4.1 Crack.exe
- FlashFXP v1.4.3 Crack.exe
- FlashFXP v2.0 Crack.exe
- FlashFXP v2.1 crack.exe
- FlashFXP v2.2 crack.exe
- Free Internet TV 3.2 Crack.exe
- Freedom Force no cd crack.exe
- Front Mission 4 crack.exe
- FrontPage XP 2002 Crack.exe
- FTP Server Serv-U 5.1 Coporate Edition Crack.exe
- Full Spectrum Warrior crack.exe
- Goblin Commander - Unleash the Horde crack.exe
- Gran Turismo 4 SCEA crack.exe
- Grand Theft Auto - San Andreas crack.exe
- Grand Theft Auto 3 no cd crack.exe
- Grand Theft Auto III no cd crack.exe
- Grand Theft Auto San Andreas NO CD crack.exe
- Grand Theft Auto Vice City NO CD crack.exe
- Grokster.exe
- Gunbound Trainer.exe
- Half-Life 2 Crack.exe
- Half-Life 2 Keygen.exe
- Half-Life 2 NO CD Crack.exe
- Halo - Combat Evolved - Microsoft no cd crack.exe
- Halo 2 crack.exe
- Harry Potter and the Prisoner of Azkaban Adventure EA Games crack.exe
- Harry Potter and the Sorcerers Stone no cd crack.exe
- HeadStrong WebClicker 2.56.exe
- Heroes of Might and Magic IV no cd crack.exe
- Hidden and Dangerous 2 NO CD Crack.exe
- HijackThis.exe
- Icewind Dale 2 no cd crack.exe
- ICQ 4.exe
- ICQ Pro 2003b.exe
- ImageSlurp 2.43.exe
- iMesh.exe
- Internet Download Manager 4.03.exe
- Internet Download Manager v4.02 Crack.exe
- IsoBuster Professional v1.7.0.0 Crack.exe
- Jedi Academy NO CD Crack.exe
- JetAudio Basic.exe
- Joint Operations - Typhoon Rising NovaLogic crack.exe
- Juiced Acclaim crack.exe
- Kaspersky Anti-Hacker v1.7 Crack.exe
- Kaspersky AntiVirus Crack (License Keygen.exe
- Kazaa Download Accelerator Pro.exe
- Kazaa Download Manager 3.0.exe
- KaZaA Lite Plus 1.0.exe
- Kingdom Hearts II crack.exe
- K-Lite Codec Pack v2.31 Full Crack.exe
- K-Lite Mega Codec Pack 1.13 Keygen.exe
- Knights Apprentice Memoricks Adventures Games crack.exe
- LimeWire (International).exe
- LimeWire Download Manager 4.2.6.exe
- LimeWire server scanner.exe
- LimeWire.exe
- Longhorn Transformation Pack 8.0.exe
- Lord of the Rings The Battle for Middle-earth 1.00 Crack.exe
- LostGoggles.exe
- LOTR NO CD Crack.exe
- Macromedia ColdFusion MX crack.exe
- Macromedia Contribute v2.0 crack.exe
- Macromedia Director 8 Crack.exe
- Macromedia Dreamweaver 4.0 Patch.exe
- Macromedia Dreamweaver MX 2004 7.0 Crack.exe
- Macromedia Dreamweaver MX v6.0 crack.exe
- Macromedia Dreamweaver UltraDev 4.0 Patch.exe
- Macromedia Fireworks 4.0 Patch.exe
- Macromedia Flash 5 Crack.exe
- Macromedia Flash All Versions keygen.exe
- Macromedia Flash MX v6.0 crack.exe
- Macromedia Flash SWF-Unprotect v2.0.exe
- Macromedia FreeHand v10 Loader.exe
- Madden NFL 2003 no cd crack.exe
- Madden NFL 2005 EA crack.exe
- Mafia no cd crack.exe
- MagicScore maestro 3.5 Keygen.exe
- Malice Mud Duck Productions crack.exe
- Mario Pinball Land Puzzle Nintendo crack.exe
- Mario Tennis crack.exe
- Matrix Screensaver.exe
- Max Payne 2 Fall Of Max Payne no cd crack.exe

- Max Payne 2 NO CD Crack.exe
- Max Payne 2 The Fall of Max Payne NO CD crack.exe
- MaxPayne 2 The Fall Of Max Payne Crack.exe
- McAfee VirusScan 9.0 Crack .exe
- McFarlanes Evil Prophecy crack.exe
- Medal Of Honor - Allied Assault BreakThrough no cd crack.exe
- Medal Of Honor - Allied Assault no cd crack.exe
- Medal of Honor Pacific Assault crack.exe
- Medieval - Total War no cd crack.exe
- Mega Man Anniversary Collection crack.exe
- Metal Gear Acid PSP crack.exe
- Metal Gear Solid 3 - Snake Eater crack.exe
- Microsoft Flight Simulator 2004 - A Century Of Flight no cd crack.exe
- Microsoft Office 2000 Regmaker.exe
- Microsoft Office XP Activation Crack.exe
- Microsoft Office XP Activation Killer.exe
- Microsoft Office XP Professional Crack.exe
- Microsoft Office XP Professional Serial.exe
- Microsoft Office XP Universal Activator v1.0.exe
- Microsoft Windows Media Player.exe
- Microsoft Windows Xp Profesional Sp 2 Keygen.exe
- Microsoft Windows XP Professional (Corp key) Keygen.exe
- Midnight Club 3 - DUB Edition crack.exe
- mIRC 6.X No CD Crack.exe
- Monopoly 3 Crack.exe
- Morpheus.exe
- Mortal Kombat 4 Crack.exe
- Mozilla Firefox.exe
- MP3 Doctor 5.11.15 Crack.exe
- mp3DirectCut 1.38 Keygen.exe
- MS Office XP Activation Crack.exe
- MS Zoo Tycoon no cd crack.exe
- MSN advert remover.exe
- MSN Messenger (Windows XP).exe
- MSN Toolbar advert remover.exe
- MSN Toolbar.exe
- MusicMatch Jukebox Plus 9.00 Crack.exe
- MVP Baseball 2004 EA crack.exe
- MyIE2.exe
- NBA Live 2003 crack.exe
- NBA Live 2004 crack.exe
- NCAA Football 2005 EA crack.exe
- Need For Speed 5 - no cd.exe
- Need for Speed Hot Pursuit 2 CD KeyGenerator.exe
- Need for speed underground - nocd.exe
- Need for Speed Underground 2 crack.exe
- Need for Speed Underground 2 NO CD crack.exe
- Need for Speed Underground Crack.exe
- Need for Speed4 - NOCD.exe
- NeedforspeedUnderground-nocd.exe
- Nero 6 Ultra Edition 6.6.0.1 Crack.exe
- Nero 6 Ultra Edition Crack.exe
- Nero 6 Ultra Edition KeyGen.exe
- Nero 6 Ultra Edition.exe
- Nero 6.6.0.1 Crack.exe
- Nero 6.6.0.3 Ultra Crack.exe
- Nero Burning Rom 6.6.0.3 Crack.exe
- Nero Burning Rom Reloaded 6.6.0.1 Crack.exe
- Nero Burning ROM v6.x crack.exe
- Nero Reloaded 6.6.0.1 Crack.exe
- Nero Ultra Edition 6.6.0.1 Crack.exe
- NetPumper Crack.exe
- NetPumper.exe
- Ninja Gaiden Tecmo crack.exe
- NOD32 AntiVirus 2.12.1 Crack.exe
- Norman Virus Control 5.70 Crack.exe
- norton 2005 Crack.exe
- Norton AntiSpam 2004 Crack .exe25-01-2005
- Norton AntiVirus 2004 crack.exe
- Norton AntiVirus 2004 Professional activation Keygen .exe
- Norton AntiVirus 2004 Professional Edition Keygen .exe
- norton AntiVirus 2005 Crack.exe
- norton internet security 2005 Crack.exe
- Norton Personal Firewall 2005 retail Crack.exe
- nVidia nTune 2005 Keygen.exe
- Office 2003 Pro Crack.exe
- Onimusha 3 - Demon Siege Adventure Capcom crack.exe
- Paris Hilton Sex-E Screensaver 1.0.exe
- Partition Magic 8.0.exe
- PhotoShop CS 8.0 & ImageReady CS 8.0 Crack.exe
- PhotoShop CS v8.0 Crack.exe
- PINNACLE STUDIO PLUS V9.3 Crack.exe
- Plus! Media Center Edition Crack.exe
- Pocket Tanks 1.0.exe
- PornSnatcher 2.31.exe
- PowerDVD v5.9 Deluxe Crack.exe
- Psi-Ops - The Mindgate Conspiracy Midway crack.exe
- Purge Jihad Freeform Interactive LLC crack.exe

- Quake 3 - The Arena NO CD Crack.exe
- QuickTime.exe
- RealPlayer crack (keygen.exe
- RealPlayer Crack.exe
- RealPlayer.exe
- Red Dead Revolver crack.exe
- RegClean 4.1a.exe
- RegCleaner 4.30.780.exe
- Registry Mechanic 3.0 Keygen.exe
- Registry Mechanic Crack.exe
- Registry Mechanic.exe
- Resident Evil 4 GC Adventure crack.exe
- Rise of Nations - Thrones & Patriots crack.exe
- Risk II 1.0.exe
- RM to MP3 Converter 1.21.exe
- RoboForm crack.exe
- RoboForm.exe
- Roller Coaster Tycoon no cd crack.exe
- Rollercoaster Tycoon 3 3 Crack.exe
- RollerCoaster Tycoon and Attractions No CD Crack.exe
- Serials 2000 v7.1 Plus (build 06.16.04) Keygen.exe
- SeXstazy 3.0.2.11.exe
- Shadow Ops - Red Mercury crack.exe
- ShellShock - Nam 67 crack.exe
- Shockwave Player.exe
- Silent Storm - Sentinels _No Company crack.exe
- Sim City 4 - Rush Hour no cd crack.exe
- Sim City 4 Deluxe no cd crack.exe
- Sim Theme Park World no cd crack.exe
- Sims 2 Crack.exe
- Sniff-em 1.12.exe
- Snood Crack.exe
- Snood.exe
- Soldat 1.1.4.exe
- Soldier of Fortune II- Double Helix No CD Crack.exe
- SolSuite 2004 - Solitaire Card Games Suite Crack.exe
- SolSuite 2004 - Solitaire Card Games Suite.exe
- Sonic the Hedgehog 3 crack.exe
- Spider-Man 2 crack.exe
- Spider-Man 2 GC crack.exe
- Sponge Bob Square Pants - Operation Krabby Patty no cd crack.exe
- Spy Sweeper 3.2 147 Crack.exe
- Spybot - Search and Destroy.exe
- SpyHunter Crack.exe
- SpyHunter.exe
- Spyware doctor 2.1 Keygen.exe
- Spyware Doctor 2.1.0.254 Crack.exe
- Spyware Doctor Crack.exe
- Spyware Doctor V3 Keygen.exe
- Spyware Doctor v3.0.0.288 Crack.exe
- Spyware Doctor.exe
- SpywareBlaster.exe
- Star Wars - Jedi Knight - Jedi Academy no cd crack.exe
- Star Wars - Knights of the Old Republic crack.exe
- Star Wars Galactic Battlegrounds- Clone Campaigns no cd crack.exe
- Star Wars Jedi Knight II - Jedi Outcast no cd crack.exe
- Star Wars Jedi Knight II- Jedi Outcast no cd crack.exe
- Star Wars Knights of the Old Republic II - The Sith Lords crack.exe
- Starcraft - Battlechest no cd crack.exe
- Strip Poker 2004 Crack.exe
- Super dvd Creator 7.5 7.5 Crack.exe
- Super Mario Kamek - Magikoopa's Revenge 1.2.exe
- Sygate Personal Firewall PRO v5.5 Build 2577 Crack.exe
- Symantec Ghost 8.0 Crack.exe
- Symatec System Center V9.0.0.338 Crack.exe
- System Mechanic 5.0c.exe
- The Chronicles of Riddick - Escape From Butcher Bay crack.exe
- The Elder Scrolls III - Morrowind Game of the Year Edition Bethesda Softworks crack.exe
- The Legend of Zelda - Four Swords Adventures crack.exe
- The Legend of Zelda - The Minish Cap crack.exe
- The Legend of Zelda (working title) crack.exe
- The lord of the rings the battle for middle earth Crack.exe
- The Lord of the Rings The Battle for Middle-Earth Crack.exe
- The Lord of the Rings The Battle for Middle-earth crack.exe
- The Lord of the Rings The Return of The King crack.exe
- The Sims - Hot Date Expansion Pack no cd crack.exe
- The Sims - Makin Magic Expansion Pack no cd crack.exe
- The Sims - Superstar Expansion Pack no cd crack.exe
- The Sims - Unleashed Expansion Pack no cd crack.exe
- The Sims - Vacation Expansion Pack no cd crack.exe
- The Sims 2 crack.exe
- The Sims Clock 1.0.exe
- The Sims Deluxe no cd crack.exe
- The Sims Double Deluxe no cd crack.exe
- The Sims no cd crack.exe
- The Sims Vacation no cd crack.exe
- The Suffering crack.exe
- The Suffering Midway crack.exe

- Thief - Deadly Shadows crack.exe
- Tiger Woods PGA Tour 2004 crack.exe
- Tom Clancys Ghost Recon - Desert Siege no cd crack.exe
- Tom Clancys Splinter Cell crack.exe
- Tom Clancys Splinter Cell Pandora Tomorrow crack.exe
- Tom Clancy's Splinter Cell Pandora Tomorrow crack.exe
- Tony Hawks Underground crack.exe
- Total Commander v6.03a PowerPack 25 Crack.exe
- Trillian crasher.exe
- Trillian Pro v3.0.950 Crack.exe
- Trillian.exe
- Tweak-XP Pro 4.0.2 Crack.exe
- Unreal Tournament 2003 no cd crack.exe
- Unreal Tournament 2004 crack (keygen.exe
- Unreal Tournament 2004 Crack.exe
- Unreal Tournament 2004 NO CD crack.exe
- Vampire - The Masquerade - Bloodlines crack.exe
- VirtualLab Data Recovery crack.exe
- VirtualLab Data Recovery.exe
- Virtuosa Phoenix Edition Crack.exe
- Warcraft III - Reign Of Chaos no cd crack.exe
- Warez P2P.exe
- WebRoot Spy Sweeper 3.5.0.189 Crack.exe
- Webroot Spy Sweeper Crack.exe
- Webroot Spy Sweeper.exe
- WebSite Watcher v4.02 Crack.exe
- Winace 2.x Crack.exe
- Winamp 5.03 Full Crack.exe
- Winamp Full.exe
- windows server 2003 crack.exe
- Windows Server 2003 SP1 Build 1039-2l Crack.exe
- Windows XP Activation Crack.exe
- Windows XP home edition Activation.exe
- Windows XP Pro 64-bit Crack.exe
- Windows XP Professional crack.exe
- Windows XP SP2 KeyGen.exe
- WinDVD Platinum 5.0.26.23 Crack.exe
- WinMX.exe
- WinRAR 3.30 Corporate Ed Crack.exe
- WinRAR 3.x Crack.exe
- WinRAR All KeyGen.exe
- WinRAR crack (keygen.exe
- WinRAR v3.20 Final Keygen.exe
- WinRAR v3.30 Final Keygen.exe
- WinRAR v3.41 Final Keygen.exe
- WinRAR.exe
- WinZip 9.x Crack.exe
- WinZip All KeyGen.exe
- WinZip All Versions keygen.exe
- Winzip Keygen.exe
- WinZip Self-Extractor v2.2 keygen.exe
- WinZip Self-Extractor v2.2 Patch.exe
- WinZip v8.0 Keygen.exe
- WinZIP v9.0 Keygen.exe
- WinZip v9.0 Registration.exe
- WinZip.exe
- World of Warcraft crack.exe
- Worms Armageddon NO CD crack.exe
- WWE Day of Reckoning GC crack.exe
- WWE SmackDown! vs. Raw crack.exe
- XBOX X-Fer Ripper and Transfer.exe
- XP Slipstreamer v1.0 Crack.exe
- Yahoo Messenger.exe
- ZeroSpyware Lite.exe
- ZipGenius.exe
- Zone Alarm Security Suite 5.5.062 Crack.exe
- ZoneAlarm crack (keygen.exe
- ZoneAlarm.exe
- Zoo Tycoon - Complete Collection no cd crack.exe
- Zoo Tycoon - Dinosaur Digs no cd crack.exe
- Zoo Tycoon no cd crack.exe
- Zoo Tycoon.exe

The worm then checks the victim machine for a P2P client, such as KaZaa, Morpheus, iMesh, eMule, wareo, DC++, and changes the client's configuration so that resources shared by default include %System%\msview (the file created by the worm).

The worm may connect to IRC servers in order to update itself.

P2P-Worm.Win32.Togod

Aliases

P2P-Worm.Win32.Togod (Kaspersky Lab) is also known as: Worm.P2P.Togod (Kaspersky Lab), W32/Togod.worm (McAfee), W32.HLLW.Togod (Symantec), Win32.HLLW.Togod (Doctor Web), W32/ToGod-A (Sophos), Win32/HLLW.Togod (RAV), WORM_TOGOD.A (Trend Micro), Worm/Togod (H+BEDV), W32/Togod (FRISK), Win32:Trojan-gen. (ALWIL), Worm/Togod (Grisoft), Win32.HLLW.Togod.A (SOFTWIN), Worm Generic (Panda), Win32/Togod.A (Eset)

Description added	Nov 12 2002
Behavior	P2P Worm

Technical details

Togod is an Internet worm spreading in the KaZaa peer-to-peer file sharing network. The worm replicates by copying itself into KaZaa shared folder.

Togod is a Windows application (PE EXE file) about 100KB in size (compressed by UPX, the decompressed size is about 175KB), written in Delphi.

The worm copies itself to the KaZaa directory using the following names:

```
borland delphi 6 enterprise.exe
paltalk crack.exe
paltalk.exe
visual basics .NET.exe
visual basics 6.exe
visual c++.exe
c++ compiler.exe
anal whore getting it from 2 guys in the ass.gif.exe
blond slut gets in every hole.gif.exe
porno slideshow.gif.exe
Star wars episode 2.mpg.exe
Britney spears naked.gif.exe
Windows XP Pro with cd key.exe
Windows xp cd key keygen.exe
borland software keygen.exe
microsoft apps keygen.exe
kiddie porn 9 year old.gif.exe
kiddie porn 14 year old.gif.exe
Adobe photoshop 7.exe
Adobe Photoshop 6.exe
Macromedia Flash 6 MX.exe
The Matrix Reloaded MOVIE.exe
counter strike.exe
half life with cd key.exe
counter strike cd key.exe
command and conquer renegade keygen.exe
password cracker.exe
hotmail password stealer.exe
aol password stealer.exe
CloneCD.exe
CloneCD Keygen.exe
Conceal PC Firewall.exe
Credit Card Generator.exe
Adult Password Generator.exe
DSL Uncapper.exe
hacking tools 2002.exe
Ghost Recon.exe
ICQ hack.exe
lesians fucking.mpeg.exe
Macromedia Flash MX.exe
Macromedia Flash 5.exe
Kazaa advertisement remover.exe
Kazaa ad remover.exe
Max Payne Full iso.exe
Max Payne.exe
Microsoft Visual C++ 7.0 iso.exe
norton antivirus 2002.exe
Nero cd burning 5.5 full.exe
Microsoft Office XP Professional full.exe
X Box Xbox emulator.exe
Quake 4 beta.exe
Norton firewall 2002.exe
Blackice firewall.exe
Return To Castle wolfenstein iso.exe
Soldier Of Fortune 2 full iso.exe
Star wars episode 2 attack of the clones.exe
Warcraft 3 full iso.exe
Warez finder (download and verify).exe
XXX password stealer.exe
ZoneAlarm pro firewall.exe
AOL password stealer.exe
Hotmail password stealer.exe
Yahoo password stealer.exe
xxx-playboy.exe.jpg
xxx site password stealer.exe
```

```
hackers hand book.exe
```

The Togod worm then displays a fake error message:

```
Error
 Error loading RCDATA
```

The worm also creates a randomly named EXE file in the Windows directory where it writes the code for "Backdoor.Lithium" and executes it.

Togod also contains the text:

```
 Hello to all the av's i hope to god norton doesnt detect this first... that
would be sad.
 Hell yeah kaspersky!
```

P2P-Worm.Win32.VB.bh

Other versions: .dg

Aliases

P2P-Worm.Win32.VB.bh (Kaspersky Lab) is also known as: Worm.P2P.VB.bh (Kaspersky Lab), W32/Generic.worm!p2p (McAfee), W32.SillyP2P (Symantec), Win32/HLLW.VB.BH (RAV), WORM_VB.BH (Trend Micro), Worm/VB.AR (Grisoft), W32/VB.F.worm (Panda)

Description added	Jul 29 2004
Behavior	P2P Worm

Technical details

This worm spreads via P2P networks as a PE file.

The worm itself is a Windows PE EXE file, 32KB in size and is written in Visual Basic.

Installation

When launched, the worm copies itself to the C:\Windows\System32\ directory under its current name and hides the file in the Windows system directory.

The worm then registers this file in the system registry, to ensure that the file is launched each time Windows is started:

```
[HKLM\Software\Microsoft\Windows\CurrentVersion\Run\]
    Windows = <file name>
```

Propagation

The worm copies itself to the following directories:

```
C:\My Shared Folder\
C:\Windows\My Shared Folder\
C:\Windows\Share\
C:\My Downloads\C:\Windows\My Downloads\
```

DoS attacks

When launched, the worm conducts DoS attacks on the following sites:

```
www.microsoft.com
www.aol.com
www.yahoo.com
www.google.com
```

by sending packets of maximum size (64 bytes) using the ping utility.

It will only do this between 0000 and 1800 and from 1900 to 2400.

Presence in the system

If the worm is launched between 1800 and 1900 according to the local system clock, it will create a directory named Shared in the C:\ root directory, and will copy itself to this directory.

P2P-Worm.Win32.VB.dg

Other versions: .bh

Aliases

P2P-Worm.Win32.VB.dg (Kaspersky Lab) is also known as: W32/Generic.worm!p2p (McAfee), WIN.SCRIPT.WORM.Virus (Doctor Web), W32/Kilati.A.worm (Panda)

Detection added	Jul 15 2005 07:21 GMT
Description added	Aug 10 2005
Behavior	P2P Worm

Technical details

This worm is written in Visual Basic and is 266,240 bytes in size. Embedded in the file are two other executables. The first one is MSWINSCK.OCX, which is the winsock control module used in VB applications. This file is 109,248 bytes in size. The second second executable is also written in VB. It functions as the worm's webserver, and it is 32,768 bytes in size.

Installation

The worm arrives via P2P networks or as a link to itself via the MSN messaging network.

When executed the worm creates the following files:

```
• list.ini - created in the system directory, this file contains data for its
spreading routine.
• MSWINSCK.OCX - created in the system directory. This file is the winsock
control module used in Visual Basic programs. It does this so to make sure that
the worm and its components can function properly. This file is not malicious.
• kernel32.exe - created in the system directory. It acts as a webserver.
• killILLUMINATI.exe - a copy of the worm which is created in the system directory.
• msn_addons.exe - another copy of the worm, this file is created in C:\
• Message.txt - this file contains a message, it's created in C:\
```

The worm adds a key to the registry to ensure it will be executed at Windows startup.

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run]
Windows32="C:\%sysdir%\killILLUMINATI.exe"
```

When executed for the first time it displays a fake error message

Propagation

This worm tries to spread via MSN Messenger and P2P networks.

P2P spreading:

The worm looks for the existence of the following directories:

```
C:\Program Files\Shareaza\Downloads
C:\Program Files\Morpheus\My Shared Folder
C:\My Shared Folder
```

```
C:\Program Files\XoloX\Downloads
C:\Program Files\Tesla\Files
C:\Program Files\Gnucleus\Downloads
C:\Program Files\ICQ\shared files
C:\My Downloads
C:\Program Files\\Edonkey2000\incoming
C:\Program Files\overnet\incoming
C:\Program Files\limewire\shared
C:\Program Files\winmx\shared
C:\Program Files\Warez P2P Client\My Shared Folder
C:\My Shared Folder
C:\Program Files\Files\Kazaa Lite\My Shared Folder
C:\Program Files\\bearshare\shared
C:\Program Files\Edonkey2000\\incoming
C:\program files\\kazaa\my shared folder
```

If it finds any of the above directories it will copy itself under all of the following filenames:

```
Halo PC NO CD Crack (Scanned With Norton AV 2005).exe
UT 2003 NO CD Crack (Scanned With Norton AV 2005).exe
UT 2004 NO CD Crack (Scanned With Norton AV 2005).exe
DOOM 3 NO CD Crack (Scanned With Norton AV 2005).exe
Far Cry NO CD Crack (Scanned With Norton AV 2005).exe
Deus Ex 2 NO CD Crack (Scanned With Norton AV 2005).exe
Call Of Duty NO CD Crack (Scanned With Norton AV 2005).exe
Half Life 2 NO CD Crack (Scanned With Norton AV 2005).exe
Need For Speed Underground NO CD Crack (Scanned With Norton AV 2005).exe
Need For Speed Underground 2 NO CD Crack (Scanned With Norton AV 2005).exe
Max Payne 2 NO CD Crack (Scanned With Norton AV 2005).exe
Red Alert 2 NO CD Crack (Scanned With Norton AV 2005).exe
Tony Hawk Underground NO CD Crack (Scanned With Norton AV 2005).exe
Tony Hawk Underground 2 NO CD Crack (Scanned With Norton AV 2005).exe
The Sims 2 NO CD Crack (Scanned With Norton AV 2005).exe
Quake 3 NO CD Crack (Scanned With Norton AV 2005).exe
Enter The Matrix NO CD Crack (Scanned With Norton AV 2005).exe
Fifa 2005 NO CD Crack (Scanned With Norton AV 2005).exe
C&C Renegade NO CD Crack (Scanned With Norton AV 2005).exe
FiC&C Generals NO CD Crack (Scanned With Norton AV 2005).exe
Man Hunt NO CD Crack (Scanned With Norton AV 2005).exe
Halo CE NO CD Crack (Scanned With Norton AV 2005).exe
GTA Vice City NO CD Crack (Scanned With Norton AV 2005).exe
GTA 3 NO CD Crack (Scanned With Norton AV 2005).exe
GTA San Andreas NO CD Crack (Scanned With Norton AV 2005).exe
Age Of Mythology NO CD Crack (Scanned With Norton AV 2005).exe
Age Of Mythology The Titans NO CD Crack (Scanned With Norton AV 2005).exe
Age Of Empires 2 NO CD Crack (Scanned With Norton AV 2005).exe
Empire Earth NO CD Crack (Scanned With Norton AV 2005).exe
True Crime Streets Of LA NO CD Crack (Scanned With Norton AV 2005).exe
Hitman 2 NO CD Crack (Scanned With Norton AV 2005).exe
Hitman 3 NO CD Crack (Scanned With Norton AV 2005).exe
Splinter Cell NO CD Crack (Scanned With Norton AV 2005).exe
Splinter Cell PT NO CD Crack (Scanned With Norton AV 2005).exe
Rome Total War NO CD Crack (Scanned With Norton AV 2005).exe
Star Wars Battle Front NO CD Crack (Scanned With Norton AV 2005).exe
Men Of Valor Vietnam NO CD Crack (Scanned With Norton AV 2005).exe
Battle Field 1942 NO CD Crack (Scanned With Norton AV 2005).exe
Call Of Duty 2 NO CD Crack (Scanned With Norton AV 2005).exe
Civilization 3 NO CD Crack (Scanned With Norton AV 2005).exe
Colin McRae Rally 4 NO CD Crack (Scanned With Norton AV 2005).exe
Colin McRae Rally 2005 NO CD Crack (Scanned With Norton AV 2005).exe
Half Life NO CD Crack (Scanned With Norton AV 2005).exe
Elder Scrolls 3 Morrowind NO CD Crack (Scanned With Norton AV 2005).exe
Lord Of The Rings ROTK NO CD Crack (Scanned With Norton AV 2005).exe
Medal Of Honor Allied Assault NO CD Crack (Scanned With Norton AV 2005).exe
Mech Warrior 4 NO CD Crack (Scanned With Norton AV 2005).exe
NBA Live 2004 NO CD Crack (Scanned With Norton AV 2005).exe
NBA Live 2005 NO CD Crack (Scanned With Norton AV 2005).exe
Never Winter Nights NO CD Crack (Scanned With Norton AV 2005).exe
Never Winter Nights 2 NO CD Crack (Scanned With Norton AV 2005).exe
NHL 2004 NO CD Crack (Scanned With Norton AV 2005).exe
NHL 2005 NO CD Crack (Scanned With Norton AV 2005).exe
Postal 2 NO CD Crack (Scanned With Norton AV 2005).exe
Red Faction NO CD Crack (Scanned With Norton AV 2005).exe
Red Faction 2 NO CD Crack (Scanned With Norton AV 2005).exe
Simpsons Hit And Run NO CD Crack (Scanned With Norton AV 2005).exe
Soldier Of Fortune 2 NO CD Crack (Scanned With Norton AV 2005).exe
Star Wars KOTOR NO CD Crack (Scanned With Norton AV 2005).exe
Tom Clancy's Ghost Recon NO CD Crack (Scanned With Norton AV 2005).exe
Tom Clancy's Rainbow Six NO CD Crack (Scanned With Norton AV 2005).exe
Tron 2.0 NO CD Crack (Scanned With Norton AV 2005).exe
Unreal 2 NO CD Crack (Scanned With Norton AV 2005).exe
Yu Gi Of Power Of Chaos NO CD Crack (Scanned With Norton AV 2005).exe
Halo PC Keygen (Scanned With Norton AV 2005).exe
UT 2003 Keygen (Scanned With Norton AV 2005).exe
UT 2004 Keygen Crack (Scanned With Norton AV 2005).exe
DOOM 3 Keygen (Scanned With Norton AV 2005).exe
Far Cry Keygen (Scanned With Norton AV 2005).exe
Deus Ex 2 Keygen (Scanned With Norton AV 2005).exe
Call Of Duty Keygen (Scanned With Norton AV 2005).exe
Half Life 2 Keygen (Scanned With Norton AV 2005).exe
Need For Speed Underground Keygen (Scanned With Norton AV 2005).exe
Need For Speed Underground 2 Keygen (Scanned With Norton AV 2005).exe
Max Payne 2 Keygen(Scanned With Norton AV 2005).exe
Red Alert 2 Keygen (Scanned With Norton AV 2005).exe
Tony Hawk Underground Keygen (Scanned With Norton AV 2005).exe
Tony Hawk Underground 2 Keygen (Scanned With Norton AV 2005).exe
The Sims 2 Keygen (Scanned With Norton AV 2005).exe
Quake 3 Keygen (Scanned With Norton AV 2005).exe
Enter The Matrix Keygen (Scanned With Norton AV 2005).exe
Fifa 2005 Keygen (Scanned With Norton AV 2005).exe
C&C Renegade Keygen (Scanned With Norton AV 2005).exe
C&C Generals Keygen (Scanned With Norton AV 2005).exe
Man Hunt Keygen (Scanned With Norton AV 2005).exe
Halo CE Keygen (Scanned With Norton AV 2005).exe
GTA Vice City Keygen (Scanned With Norton AV 2005).exe
GTA 3 Keygen (Scanned With Norton AV 2005).exe
```

GTA San Andreas Keygen (Scanned With Norton AV 2005).exe
Age Of Mythology Keygen (Scanned With Norton AV 2005).exe
Age Of Mythology The Titans Keygen (Scanned With Norton AV 2005).exe
Age Of Empires 2 Keygen(Scanned With Norton AV 2005).exe
Empire Earth Keygen (Scanned With Norton AV 2005).exe
True Crime Streets Of LA Keygen (Scanned With Norton AV 2005).exe
Hitman 2 Keygen (Scanned With Norton AV 2005).exe
Hitman 3 Keygen (Scanned With Norton AV 2005).exe
Splinter Cell Keygen (Scanned With Norton AV 2005).exe
Splinter Cell PT Keygen (Scanned With Norton AV 2005).exe
Rome Total War Keygen (Scanned With Norton AV 2005).exe
Star Wars Battle Front Keygen (Scanned With Norton AV 2005).exe
Men Of Valor Vietnam Keygen (Scanned With Norton AV 2005).exe
Battle Field 1942 Keygen (Scanned With Norton AV 2005).exe
Call Of Duty 2 Keygen (Scanned With Norton AV 2005).exe
Civilization 3 Keygen (Scanned With Norton AV 2005).exe
Colin McRae Rally 4 Keygen (Scanned With Norton AV 2005).exe
Colin McRae Rally 2005 Keygen (Scanned With Norton AV 2005).exe
Half Life Keygen (Scanned With Norton AV 2005).exe
Elder Scrolls 3 Morrowind Keygen (Scanned With Norton AV 2005).exe
Lord Of The Rings ROTK Keygen (Scanned With Norton AV 2005).exe
Medal Of Honor Allied Assault Keygen (Scanned With Norton AV 2005).exe
Mech Warrior 4 Keygen (Scanned With Norton AV 2005).exe
NBA Live 2004 Keygen(Scanned With Norton AV 2005).exe
NBA Live 2005 Keygen (Scanned With Norton AV 2005).exe
Never Winter Nights Keygen(Scanned With Norton AV 2005).exe
Never Winter Nights 2 Keygen(Scanned With Norton AV 2005).exe
NHL 2004 Keygen (Scanned With Norton AV 2005).exe
NHL 2005 Keygen (Scanned With Norton AV 2005).exe
Postal 2 Keygen (Scanned With Norton AV 2005).exe
Red Faction Keygen (Scanned With Norton AV 2005).exe
Red Faction 2 Keygen (Scanned With Norton AV 2005).exe
Simpsons Hit And Run Keygen (Scanned With Norton AV 2005).exe
Soldier Of Fortune 2 Keygen (Scanned With Norton AV 2005).exe
Star Wars KOTOR Keygen (Scanned With Norton AV 2005).exe
Tom Clancy's Ghost Recon Keygen (Scanned With Norton AV 2005).exe
Tom Clancy's Rainbow Six Keygen (Scanned With Norton AV 2005).exe
Tron 2.0 Keygen (Scanned With Norton AV 2005).exe
Unreal 2 Keygen (Scanned With Norton AV 2005).exe
Yu Gi Of Power Of Chaos Keygen (Scanned With Norton AV 2005).exe
McAfee Keygen (Scanned With Norton AV 2005).exe
PC Cillin Keygen (Scanned With Norton AV 2005).exe
Kaspersky Keyfile Generator (Scanned With Norton AV 2005).exe
Sophos AntiVirus Keygen (Scanned With Norton AV 2005).exe
AVG Keygen ALL VERSIONS (Scanned With Norton AV 2005).exe
Panda AV 2005 Keygen (Scanned With Norton AV 2005).exe
F-Secure Keyfile Generator (Scanned With Norton AV 2005).exe
Avast AntiVirus Keygen (Scanned With Norton AV 2005).exe
F-Prot AntiVirus Keygen (Scanned With Norton AV 2005).exe
VET AntiVirus Keygen (Scanned With Norton AV 2005).exe
BIT Defender AntiVirus Keygen (Scanned With Norton AV 2005).exe
Norton AntiVirus 2005 Keygen.exe
Norton Internet Security 2005 Keygen.exe
Windows Xp Professional Keygen (Scanned With Norton AV 2005).exe
Windows Xp Home Keygen (Scanned With Norton AV 2005).exe
Flash FXP Keygen (Scanned With Norton AV 2005).exe
Tune Up 2004 Keygen (Scanned With Norton AV 2005).exe
Visual Basic 6 Keygen (Scanned With Norton AV 2005).exe
Visual C++ Keygen (Scanned With Norton AV 2005).exe
Office 2000 Keygen (Scanned With Norton AV 2005).exe
Office 2002 Keygen (Scanned With Norton AV 2005).exe
Office Xp Keygen (Scanned With Norton AV 2005).exe
Office 2003 Keygen (Scanned With Norton AV 2005).exe
Partition Magic 8 Keygen (Scanned With Norton AV 2005).exe
WinRAR Keygen (Scanned With Norton AV 2005).exe
Microsoft Longhorn 4051 Keygen (Scanned With Norton AV 2005).exe
Microsoft Longhorn 4071 Keygen (Scanned With Norton AV 2005).exe
Nero 6 Keygen (Scanned With Norton AV 2005).exe
Nero 7 Keygen (Scanned With Norton AV 2005).exe
Alcohol 120 % Keygen (Scanned With Norton AV 2005).exe
Macromedia Dreamweaver MX Keygen (Scanned With Norton AV 2005).exe
Bryce 5 Keygen (Scanned With Norton AV 2005).exe
Black ICE PC Protect Keygen (Scanned With Norton AV 2005).exe
Zone Alarm Pro 4.x Crack (Scanned With Norton AV 2005).exe
Zone Alarm Pro 5.x Crack (Scanned With Norton AV 2005).exe
Xenon Ultra - Xbox Emulator.exe
Game4 Ultra - Gamecube Emulator.exe
Bleem Next Gen - PS2 Emulator.exe
Doom 3 - RELOADED ISO FTP Info.exe
Half Life 2 - EMPORiO ISO FTP Info.exe
Need For Speed Underground 2 - RELOADED ISO FTP Info.exe
Quake 4 BETA 5.72 - RELOADED ISO FTP Info.exe
True Crimes Streets Of LA - RELOADED ISO FTP Info.exe
Unreal 3 BETA 2.654 - RELOADED ISO FTP Info.exe
Xbox Boot Disc ISO DVD.exe
Playstation 2 Boot Disc ISO DVD.exe
Gamecube Boot Disc ISO DVD.exe
Halo 2 [XBOX] - ISO FTP Info.exe
Fable [XBOX] - ISO FTP Info.exe
Perfect Dark Zero [XBOX] - ISO FTP Info.exe
Conker Live & Reloaded [XBOX] - ISO FTP Info.exe
Men Of Valor:Vietnam [XBOX] - ISO FTP Info.exe
Doom 3 [XBOX] - ISO FTP Info.exe
Splinter Cell PT [XBOX] - ISO FTP Info.exe
Splinter Cell Chaos Theory [XBOX] - ISO FTP Info.exe
Project Gotham 2 [XBOX] - ISO FTP Info.exe
Half Life 2 [XBOX] - ISO FTP Info.exe
Blinx 2 [XBOX] - ISO FTP Info.exe
Mortal Combat Deception [XBOX] - ISO FTP Info.exe
Tom Clancy's Ghost Recon 2 [XBOX] - ISO FTP Info.exe
Call Of Duty [XBOX] - ISO FTP Info.exe
Jade Empire [XBOX] - ISO FTP Info.exe
Oddworld Munch's Oddysee [XBOX] - ISO FTP Info.exe
Oddworld Strangers Wrath [XBOX] - ISO FTP Info.exe
Need For Speed Underground 2 [XBOX] - ISO FTP Info.exe
Mech Assault 2 [XBOX] - ISO FTP Info.exe
Ninja Gaiden [XBOX] - ISO FTP Info.exe
Tony Hawk Underground 2 [XBOX] - ISO FTP Info.exe

Sonic Mega Collection [XBOX] - ISO FTP Info.exe
Dead Or Alive Ultimate [XBOX] - ISO FTP Info.exe
Soul Calibur 2 [XBOX] - ISO FTP Info.exe
Spiderman 2 [XBOX] - ISO FTP Info.exe
Star Wars Battlefront [XBOX] - ISO FTP Info.exe
Star Wars KOTOR [XBOX] - ISO FTP Info.exe
Star Wars KOTOR 2 [XBOX] - ISO FTP Info.exe
Amped [XBOX] - ISO FTP Info.exe
Brute Force [XBOX] - ISO FTP Info.exe
Amped 2 [XBOX] - ISO FTP Info.exe
Buffy The Vampire Slayer [XBOX] - ISO FTP Info.exe
Buffy : Chaos Bleeds [XBOX] - ISO FTP Info.exe
Juiced [XBOX] - ISO FTP Info.exe
Colin Mcrae 2005 [XBOX] - ISO FTP Info.exe
Crash Bandicoot TWOC [XBOX] - ISO FTP Info.exe
Crazy Taxi 3 [XBOX] - ISO FTP Info.exe
Deus Ex 2:Invisible War [XBOX] - ISO FTP Info.exe
DRIV3R (Driver 3) [XBOX] - ISO FTP Info.exe
GTA San Andreas [XBOX] - ISO FTP Info.exe
GTA Double Pack [XBOX] - ISO FTP Info.exe
Enter The Matrix [XBOX] - ISO FTP Info.exe
Grabbed By The Ghoulies [XBOX] - ISO FTP Info.exe
Halo [XBOX] - ISO FTP Info.exe
Hitman Contracts [XBOX] - ISO FTP Info.exe
Hunter The Reckoning:The Redeemer [XBOX] - ISO FTP Info.exe
Hitman 2:Silent Assasin [XBOX] - ISO FTP Info.exe
Jet Set Radio Future [XBOX] - ISO FTP Info.exe
Jade Empire [XBOX] - ISO FTP Info.exe
Kung Fu Chaos [XBOX] - ISO FTP Info.exe
Lord Of The Rings ROTK [XBOX] - ISO FTP Info.exe
Lord Of The Rings TTA [XBOX] - ISO FTP Info.exe
Lord Of The Rings FOTH [XBOX] - ISO FTP Info.exe
Medal Of Honour:Dogs Of War [XBOX] - ISO FTP Info.exe
Medal Of Honour:Rising Sun [XBOX] - ISO FTP Info.exe
Medal Of Honour:Frontline [XBOX] - ISO FTP Info.exe
Morrowind:GOTY [XBOX] - ISO FTP Info.exe
Red Faction 2 [XBOX] - ISO FTP Info.exe
Rallysport Challenge 2 [XBOX] - ISO FTP Info.exe
The Simpsons Hit And Run [XBOX] - ISO FTP Info.exe
The Sims:Bustin' Out [XBOX] - ISO FTP Info.exe
Timesplitters 2 [XBOX] - ISO FTP Info.exe
True Crimes:Streets Of LA [XBOX] - ISO FTP Info.exe
Unreal Championship [XBOX] - ISO FTP Info.exe
Unreal Championship 2:Liandari Conflict [XBOX] - ISO FTP Info.exe
GTA San Andreas [PS2] - ISO FTP Info.exe
GTA 3 [PS2] - ISO FTP Info.exe
GTA Vice City [PS2] - ISO FTP Info.exe
Final Fantasy X [PS2] - ISO FTP Info.exe
Final Fantasy 10 [PS2] - ISO FTP Info.exe
Kill Zone [PS2] - ISO FTP Info.exe
Need For Speed Underground [PS2] - ISO FTP Info.exe
Need For Speed Underground 2 [PS2] - ISO FTP Info.exe
Prince Of Persia:Warrior Within [PS2] - ISO FTP Info.exe
Socom [PS2] - ISO FTP Info.exe
Golden Eye Rogue Agent [PS2] - ISO FTP Info.exe
Tom Clancy's Ghost Recon 2 [PS2] - ISO FTP Info.exe
Gran Turismo 4 [PS2] - ISO FTP Info.exe
Star Wars Galaxies [PS2] - ISO FTP Info.exe
Black And White:Next Generation [PS2] - ISO FTP Info.exe
Call Of Duty:Finest Hour [PS2] - ISO FTP Info.exe
Dragon Ball Z: Budokai 3 [PS2] - ISO FTP Info.exe
Ape Escape: Pumped & Primed [PS2] - ISO FTP Info.exe
Lord Of The Rings:The Third Age [PS2] - ISO FTP Info.exe
Metal Gear Solid 3 [PS2] - ISO FTP Info.exe
Silent Hill 4:The Room [PS2] - ISO FTP Info.exe
Tony Hawk Underground 2 [PS2] - ISO FTP Info.exe
Tony Hawk Underground 2 [GCN] - ISO FTP Info.exe
Need For Speed Underground 2 [GCN] - ISO FTP Info.exe
Paper Mario [GCN] - ISO FTP Info.exe
Super Mario Sunshine [GCN] - ISO FTP Info.exe
Luigi's Manshion [GCN] - ISO FTP Info.exe
Mario Kart Double Dash [GCN] - ISO FTP Info.exe
Mario Party 4 [GCN] - ISO FTP Info.exe
Mario Party 5 [GCN] - ISO FTP Info.exe
Metroid Prime [GCN] - ISO FTP Info.exe
Metroid 2 [GCN] - ISO FTP Info.exe
Pikmin [GCN] - ISO FTP Info.exe
Star Fox Adventures [GCN] - ISO FTP Info.exe
Lord Of The Rings:ROTK [GCN] - ISO FTP Info.exe
Lord Of The Rings:LOTR [GCN] - ISO FTP Info.exe
Mario Power Tennis [GCN] - ISO FTP Info.exe
Super Smash Bro's Melee [GCN] - ISO FTP Info.exe
Donkey Kong Country 2 [GCN] - ISO FTP Info.exe
Lord Of The Rings:The Third Age [GCN] - ISO FTP Info.exe
Golden Eye:Rogue Agent [GCN] - ISO FTP Info.exe
Viewtiful Joe [GCN] - ISO FTP Info.exe
The Urbz:Sims In The City [GCN] - ISO FTP Info.exe
The Sims:Bustin'Out [GCN] - ISO FTP Info.exe
Spyro A Heros Tale [GCN] - ISO FTP Info.exe
Shrek 2:Beg For Mercy [GCN] - ISO FTP Info.exe
Resident Evil 4 [GCN] - ISO FTP Info.exe
Call Of Duty:Finest Hour [GCN] - ISO FTP Info.exe
Yu-Gi-Oh! [GCN] - ISO FTP Info.exe
Sonic Adventure DX [GCN] - ISO FTP Info.exe
Sonic Adventure DX 2 [GCN] - ISO FTP Info.exe
Sonic Mega Collection [GCN] - ISO FTP Info.exe
1080 Avalanche [GCN] - ISO FTP Info.exe
F-Zero Racing [GCN] - ISO FTP Info.exe
Area 51 [GCN] - ISO FTP Info.exe
Batman:Vengence [GCN] - ISO FTP Info.exe
Batman:Bad Tommorow [GCN] - ISO FTP Info.exe
Capcom vs SNK 2 EO [GCN] - ISO FTP Info.exe
Dragon Ball Z Budokai 2 [GCN] - ISO FTP Info.exe
Final Fantasy Crystal Cronicles [GCN] - ISO FTP Info.exe
Legend Of Zelda For Swords [GCN] - ISO FTP Info.exe
Medal Of Honour Frontline [GCN] - ISO FTP Info.exe
NBA Live 2005 [GCN] - ISO FTP Info.exe
Simpsons Hit And Run [GCN] - ISO FTP Info.exe

Prince Of Persia:Warrior Within [GCN] - ISO FTP Info.exe
Zoocube [GCN] - ISO FTP Info.exe
Spiderman 2 [GCN] - ISO FTP Info.exe
Ape Escape 3 [PS2] - ISO FTP Info.exe
Backyard Wrestling 2 [PS2] - ISO FTP Info.exe
Black And White Next Gen [PS2] - ISO FTP Info.exe
Capcom vs SNK 2 [PS2] - ISO FTP Info.exe
Devil May Cry [PS2] - ISO FTP Info.exe
Devil May Cry 2 [PS2] - ISO FTP Info.exe
Dragon Ball Z Budokai 3 [PS2] - ISO FTP Info.exe
Hitman 3:Contracts [PS2] - ISO FTP Info.exe
King Of Fighters 2003 [PS2] - ISO FTP Info.exe
Midnight Club 3 [PS2] - ISO FTP Info.exe
Mortal Combat:Deception [PS2] - ISO FTP Info.exe
TimeSplitters 2 [PS2] - ISO FTP Info.exe
Moto GP3 [PS2] - ISO FTP Info.exe
Metal Gear Solid 3:Snake Eater [PS2] - ISO FTP Info.exe
Breath Of Fire Dragon Quest [PS2] - ISO FTP Info.exe
Half Life 2 Keygen - RELOADED.exe
Doom 3 Keygen - RELOADED.exe
UT 2004 Keygen - RELOADED.exe
UT 2003 Keygen - RELOADED.exe
Halo PC Keygen - RELOADED.exe
Halo CE Keygen - RELOADED.exe
Age Of Mythology Keygen - RELOADED.exe
Red Alert 2 Keygen - RELOADED.exe
C&C Generals Keygen - RELOADED.exe
Counter Strike:Source Keygen - RELOADED.exe
Need For Speed Underground 2 Keygen - RELOADED.exe
Call Of Duty Keygen - RELOADED.exe
Sacred Keygen - RELOADED.exe
War Craft 3 Keygen - RELOADED.exe
Medal Of Honour Allied Assault Keygen - RELOADED.exe
Battle Field 1942 Keygen - RELOADED.exe
Colin Mcrae 2005 Keygen - RELOADED.exe
Half Life 2 STEAM Keygen - RELOADED.exe
Far Cry Keygen - RELOADED.exe
Ghost Recon 2 Keygen - RELOADED.exe
Never Winter Nights 2 Keygen - RELOADED.exe
Diablo 2 Keygen - RELOADED.exe
Black And White Keygen - RELOADED.exe
Black And White Next Generation Keygen - RELOADED.exe
Quake 3 Keygen - RELOADED.exe
Battle Field Vietnam Keygen - RELOADED.exe
War Craft 3 Keygen - RELOADED.exe
Unreal 2 Keygen - RELOADED.exe
Rainbow Six 3 Keygen - RELOADED.exe
Call Of Duty 2 Keygen - RELOADED.exe
McAfee Anti-Virus - Software Keygen.exe
McAfee Firewall - Software Keygen.exe
McAfee Computer Security - Software Keygen.exe
Norton Anti-Virus - Software Keygen.exe
Norton Firewall Keygen - Software Keygen.exe
Norton Internet Security - Software Keygen.exe
Partition Magic 8 - Software Keygen.exe
Panda Titanium 4 - Software Keygen.exe
Windows XP - Software Keygen.exe
RAM Defrag 2.55 - Software Keygen.exe
Porn Cleanser - Software Keygen.exe
Powerpoint 2 DVD - Software Keygen.exe
Norton System Mechanic - Software Keygen.exe
Stopzilla 3.2 - Software Keygen.exe
Nero ALL Versions - Software Keygen.exe
NOD32 - Software Keygen.exe
Pocket DVD Studio - Software Keygen.exe
Get Right 5.1 - Software Keygen.exe
Ad-Aware Pro - Software Keygen.exe
JPEG Compresser 4.2 - Software Keygen.exe
Clone CD 5 - Software Keygen.exe
Cloney XXL - Software Keygen.exe
Panda Titanium AV 2005 - Software Keygen.exe
Flash FXP All Versions - Software Keygen.exe
Smart FTP 1.0 - Software Keygen.exe
Bullet Proof FTP ALL VERSIONS - Software Keygen.exe
Tune Up Utility 2004 - Software Keygen.exe
Registry Toolkit - Software Keygen.exe
Winrar 3.x - Software Keygen.exe
WinZIP ALL VERSIONS - Software Keygen.exe
Keyhole - Software Keygen.exe
Visual C# .NET - Software Keygen.exe
Visual Basic 6 - Software Keygen.exe
Delphi 7 - Software Keygen.exe
Visual C++ ALL VERSIONS - Software Keygen.exe
Hotmail Hacker Pro.exe
Hotmail Hacker Pro SE.exe
Yahoo Hacker Pro.exe
Yahoo Hacker Pro SE.exe
NetBIOS Hacker.exe
NetBIOS Auto Rooter.exe
Direct IP Hacker.exe
Exploit Compiler SE.exe
Sub 7 Special Edition (NO SERVER NEEDED).exe
Hackers Paradise.exe
Hackers Office.exe
Hacker Tools.exe
IP Hacker.exe
Port Scanner.exe
Super Fast IP Scanner.exe
Virus Generator.exe
Worm Generator.exe
Email Hacking Tool.exe
Linux (Hacking Tool).exe
Hacking Tool.exe
RPC DCOM Hacking Tool.exe
LSASS Hacking Tool.exe
Network Hacking Tool.exe
IP Nuker.exe
IP Flooder.exe

```
ICMP Flooder.exe
UDP Flooder.exe
TCP Flooder.exe
SYN Flooder.exe
Yahoo Booter.exe
Booter (Hack Tool).exe
MSN Chat Booter.exe
Chat Room Booter(Works).exe
Trojan Kit.exe
CIA Hacker Tool.exe
FBI Hacker Tool.exe
Hackers Black Book.exe
Hacking Exposed 5th Edition.exe
Hacking Exposed 4th Edition.exe
Hacking eBooks.exe
Master Hacker Tool.exe
Windows XP Hacker.exe
Website Defacer (Hack Tool).exe
```

These names are extracted from the file list.ini.

MSN spreading:

The worm tries to spread via the MSN network, it spreads as a link to the infected file.

The infected computer serves as host for this action.

First the worm contacts a specific page on www.showmyip.com to determine the infected computer's I.P. address.

Note: This page has been moved and therefore the worm is unable to parse the output.

The worm looks for online contacts and sends them the following message:

```
"please download this...its only small brb http:/[server]/msn_addons.exe"
```

[server] stands for I.P. address determined by the worm.

As the page has been moved this will look like this:

```
"please download this...its only small brb http:///msn_addons.exe"
```

It sends this message repeatedly.

Payload

The worm tries to hide the killILLUMINATI.exe process from processlisters.

The worm may alter the Internet Explorer startpage to one of the following pages:

```
http://www.pentagonstrike.co.uk/pentagon.swf
www.hugequestions.com/911.swf
http://download.911sb.org/911.swf
http://download.911sb.org/911.swf
http://download.911sb.org/911.swf
http://www.root.co.yu/pentagon/pentagon.swf
http://www.911weknow.com/911.swf
http://www.spycave.com/pentagon.swf
http://www.theundertow.tk/media/videos/_files/Pentagon.swf
http://911sharethetruth.com/extras/pentagon.swf
```

kernel32.exe opens 80/TCP and turns the computer into a webserver so that the recipient of the Instant Message is able to download the infected file from that computer.

kernel32.exe conducts a DoS attack on jamster.com.

Other

Message.txt located in C:\ contains the following message:

```
"The easiest way to gain control of the
population is to carry out acts of terror the
public will clamor for such laws if the personal
security is threatened."

- Joseph Stalin
```

Removal instructions

Ensure that your antivirus is up to date. If your system is infected, and you are unable to access your antivirus vendor's site, delete the "hosts" file

located in %sysdir%\drivers\etc and try again.

Perform a full system scan.

Kaspersky Anti-Virus users should delete all files detected as P2P-Worm.Win32.VB.dg. Reboot if necessary.

Other Malware

Other malware includes a range of programs that do not threaten computers directly, but are used to create viruses or Trojans, or used to carry out illegal activities such as DoS attacks and breaking into other computers.

DoS and DDoS Tools

These programs attack web servers by sending numerous requests to the specified server, often causing it to crash under an excessive volume of requests. If the server is not backed by additional resources, it will signal the failure to process requests by denying service. This is why such attacks are called Denial of Service attacks.

DoS programs conduct such attacks from a single computer with the consent of the user. Distributed Denial of Service (DDoS) attacks use a large number of infected machines without the knowledge or consent of their owners. DDoS programs can be downloaded onto victim machines by various methods. They then launch an attack either based on a date included in the code or when the 'owner' issues a command to launch the attack.

Worms can carry a DoS procedure as part of their payload. For instance, on August 20, 2001, the CodeRed worm launched a successful attack on the official web site of the President of the USA (www.whitehouse.gov). Mydoom.a contained DDoS code directed against SCO's corporate site. The company, a Unix developer, closed the site on February 1, 2004, shortly after the beginning of the DdoS attack and moved it to a different URL.

Hacker Tools and Exploits

These utilities are designed to penetrate remote computers in order to use them as zombies (by using backdoors) or to download other malicious programs to victim machines.

Exploits use vulnerabilities in operating systems and applications to achieve the same result.

Flooders

These utilities are used to flood data channels with useless packets and emails.

Constructors and VirTools

Virus writers use constructor utilities to create new malicious programs and Trojans. It is known that constructors to create macro-viruses and viruses for Windows are in existence. Constructors can be used to generate virus source code, object modules and infected files.

Some constructors come with a user interface where the virus type, objects to attack, encryption options, protection against debuggers and dissasemblers, text strings, multimedia effects etc. can be chosen from a menu. Less complex constructors have no interface, and read information about the type of virus to be built from the configuration file.

VirTools are all utilites created to simplify virus writing. They can also be used to analyze viruses to see how they can be used in hacking attacks.

Nukers

Hackers use these utilities to crash attacked machines by sending specially coded/phrased requests. These requests exploit vulnerabilities in applications and operating systems to cause fatal errors.

FileCryptors and PolyCryptors

These are hacker utilities used by virus writers use to encrypt malicious programs to prevent them being detected by antivirus software.

PolyEngines

Polymorphic generators are not viruses in the true sense of the word. They do not propagate by opening, closing or writing code into files or reading and writing sectors. These programs encrypt the body of the virus and generate a de-encryption routine.

Virus writers usually spread polymorphic generators as archived files. The main file in a generator archive is the object module which contains the actual generator. This module always contains an external function that calls the generator.

Trojan Programs

Trojans can be classified according to the actions which they carry out on victim machines.

- Backdoors
- General Trojans
- PSW Trojans
- Trojan Clickers
- Trojan Downloaders
- Trojan Droppers
- Trojan Proxies
- Trojan Spies
- Trojan Notifiers
- ArcBombs
- Rootkits

Backdoors

Today backdoors are the most dangerous type of Trojans and the most widespread. These Trojans are remote administration utilities that open infected machines to external control via a LAN or the Internet. They function in the same way as legal remote administration programs used by system administrators. This makes them difficult to detect.

The only difference between a legal administration tool and a backdoor is that backdoors are installed and launched without the knowledge or consent of the user of the victim machine. Once the backdoor is launched, it monitors the local system without the user's knowledge; often the backdoor will not be visible in the log of active programs.

Once a remote administration utilitiy has been successfully installed and launched, the victim machine is wide open. Backdoor functions can include:

- Sending/ receiving files
- Launching/ deleting files
- Executing files
- Displaying notification
- Deleting data
- Rebooting the machine

In other words, backdoors are used by virus writers to detect and download confidential information, execute malicious code, destroy data, include the machine in bot networks and so forth. In short, backdoors combine the functionality of most other types of Trojans in one package.

Backdoors have one especially dangerous sub-class: variants that can propagate like worms. The only difference is that worms are programmed to propagate constantly, whereas these 'mobile' backdoors spread only after a specific command from the 'master'.

General Trojans

This loose category includes a variety of Trojans that damage victim machines or threaten data integrity, or impair the functioning of the victim machine.

Multi-purpose Trojans are also included in this group, as some virus writers create multi-functional Trojans rather than Trojan packs.

PSW Trojans

This family of Trojans steals passwords, normally system passwords from victim machines. They search for system files which contain confidential information such as passwords and Internet access telephone numbers and then send this information to an email address coded into the body of the Trojan. It will then be retrieved by the 'master' or user of the illegal program.

Some PSW Trojans steal other types of information such as:

- System details (memory, disk space, operating system details)
- Local email client
- IP-address

- Registration details
- Passwords for on-line games

Trojan-AOL are PSW Trojans that steal passwords for aol (American Online) They are contained in a sub-groups because they are so numerous.

Trojan Clickers

This family of Trojans redirects victim machines to specified websites or other Internet resources. Clickers either send the necessary commands to the browser or replace system files where standard Internet urls are stored (e.g. the 'hosts' file in MS Windows).

Clickers are used:

- To raise the hit-count of a specific site for advertising purposes
- To organize a DoS attack on a specified server or site
- To lead the victim to an infected resource where the machine will be attacked by other malware (viruses or Trojans)

Trojan Downloaders

This family of Trojans downloads and installs new malware or adware on the victim machine. The downloader then either launches the new malware or registers it to enable autorun according to the local operating system requirements. All of this is done without the knowledge or consent of the user.

The names and locations of malware to be downloaded are either coded into the Trojan or downloaded from a specified website or other Internet location.

Trojan Droppers

These Trojans are used to install other malware on victim machines without the knowledge of the user. Droppers install their payload either without displaying any notification, or displaying a false message about an error in an archived file or in the operating system. The new malware is dropped to a specified location on a local disk and then launched.

Droppers are normally structured in the following way:

Main file contains the dropper payload
File 1 first payload
File 2 second payload
... as many files as the coder chooses to include

The dropper functionality contains code to install and execute all of the payload files.

In most cases, the payload contains other Trojans and at least one hoax: jokes, games, graphics and so forth. The hoax is meant to distract the user or to prove that the activity caused by the dropper is harmless, whereas it actually serves to mask the installation of the dangerous payload.

Hackers using such programs achieve two objectives:

1. Hidden or masked installation of other Trojans or viruses
2. Tricking antivirus solutions which are unable to analyse all components

Trojan Proxies

These Trojans function as a proxy server and provide anonymous access to the Internet from victim machines. Today these Trojans are very popular with spammers who always need additional machines for mass mailings. Virus coders will often include Trojan-proxies in Trojan packs and sell networks of infected machines to spammers.

Trojan Spies

This family includes a variety of spy programs and key loggers, all of which track and save user activity on the victim machine and then forward this information to the master. Trojan-spies collect a range of information including:

- Keystrokes
- Screenshots
- Logs of active applications
- Other user actions

These Trojans are most often used to steal banking and other financial information to support online fraud.

Trojan Notifiers

These Trojans inform the 'master' about an infected machine. Notifiers confirm that a machine has been successfully infected, and send information about IP-address, open port numbers, the email address etc. of the victim machine. This information may be sent by email, to the master's website, or by ICQ.

Notifiers are usually included in a Trojan 'pack' and used only to inform the master that a Trojan has been successfully installed on the victim machine.

Rootkits

A rootkit is a collection of programs used by a hacker to evade detection while trying to gain unauthorized access to a computer. This is done either by replacing system files or libraries, or by installing a kernel module. The hacker installs the rootkit after obtaining user-level access: typically this is done by cracking a password or by exploiting a vulnerability. This is then used to gather other user IDs until the hacker gains root, or administrator, access to the system.

The term originated in the Unix world, although it has since been applied to the techniques used by authors of Windows-based Trojans to conceal their actions. Rootkits have been used increasingly as a form of stealth to hide Trojan activity, something that is made easier because many Windows users log in with administrator rights.

ArcBombs

These Trojans are archived files coded to sabotage the de-compressor when it attempts to open the infected archived file. The victim machine will slow or crash when the Trojan bomb explodes, or the disk will be filled with nonsense data. ArcBombs are especially dangerous for servers, particularly when incoming data is initially processed automatically: in such cases, an ArcBomb can crash the server.

There are three types of ArcBombs: incorrect header in the archive, repeating data and a series of identical files in the archive.

An incorrect archive header or corrupted data can both cause the de-compressor to crash when opening and unpacking the infected archive.

A large file containing repeating data can be packed into a very small archive: 5 gigabytes will be 200 KB when packed using RAR and 480 KB in ZIP format.

Moreover, special technologies exist to pack an enormous number of identical files in one archive without significantly affecting the size of the archive itself: for instance, it is possible to pack 10^{100} identical files into a 30 KB RAR file or a 230 KB ZIP file.