

Re: McAfee's Naming Convention of Computer Viruses, Worms and Trojans

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.security.virus/2003-12/1360.html>

From: David H. Lipman (*DLipman~nospam~_at_Verizon.Net*)

Date: 12/19/03

Date: Fri, 19 Dec 2003 14:45:51 -0500

I have been a regular of 'alt.comp.virus' for over 10 years and a lurker before that.

Dave

"Bill Sanderson" <Bill_Sanderson@msn.com.plugh.org> wrote in message
news:OxFT5FmxDHA.556@TK2MSFTNGP11.phx.gbl...

| The name is familiar, but I don't know from where.

| The only ALT group I follow is alt.internet.wireless--which is really about
| wireless internetworking, rather than Internet access via wireless!

| "David H. Lipman" <DLipman~nospam~@Verizon.Net> wrote in message
| news:usOiwBmxDHA.2396@TK2MSFTNGP09.phx.gbl...

| > I don't know if you know Nick Fitzgerald.

| > He is a regular on 'alt.comp.virus' and sometimes posts on

| 'alt.comp.anti-virus'.

| >

| > Dave

| >

| >

| >

| > "Bill Sanderson" <Bill_Sanderson@msn.com.plugh.org> wrote in message
| > news:%23sAFo6lxDHA.1736@TK2MSFTNGP09.phx.gbl...

| > | Thanks - that is very useful. And, there is some standardization--CARO.

| > |

| > | CARO doesn't seem to be published on the web that I can spot.

| > |

| > | Here's Symantec's description of the naming issue:

| > |

| > |

| <http://securityresponse.symantec.com/avcenter/reference/virus.and.vulnerability.pdf>

| > |

| > |

| > | The most current formulation of the CARO conventions seems to be the

| Nick

| > | Fitzgerald article on page 7 of this Virus Bulletin:

|> |
|> | <http://www.virusbtn.com/magazine/archives/pdf/2003/200301.pdf>
|> |
|> | Here's an article in about the same time frame complaining about the
| naming
|> | issue:
|> |
|> | http://reviews-zdnet.com.com/4520-7297_16-4207801.html
|> |
|> | This is not a simple issue apparently. It still appears to me that
| there is
|> | some politics issue here—and that there needs to be a dual standard—a
|> | proper "scientific name" for each critter, and a generic "common name"
| for
|> | use in giving information to users when something is detected.
|> |
|> |
|> |
|> |
|> |
|> |
|> | "David H. Lipman" <DLipman~nospam~@Verizon.Net> wrote in message
|> | news:OW7p9lcxDHA.556@TK2MSFTNGP11.phx.gbl...
|> |> The following information is from NAI/McAfee and is posted for
| reference
|> | only and they own
|> |> the rights to this information.
|> |>
|> |> Dave
|> |> ~ ~ ~ ~ ~ ~ ~ ~
|> |> UNDERSTANDING VIRUS NAMES
|> |>
|> |> Our anti-virus software typically follows
|> |> industry-wide naming conventions to identify
|> |> the viruses that it detects and cleans.
|> |> Occasionally, some virus names deviate from
|> |> strict industry standards.
|> |>
|> |> The first virus with a given set of
|> |> characteristics that mark it as a distinctly
|> |> new entity receives a "family" name. Virus
|> |> researchers draw the family name from some
|> |> identifying quirk or notation in the virus,
|> |> such as a text string, or a payload effect.
|> |>
|> |> A family name can also include a numeric string
|> |> that designates the byte size of the virus.
|> |> Researchers use this name as convenient
|> |> shorthand to distinguish closely allied virus
|> |> variants.
|> |>

|> |> Names for variants within a virus family
|> |> consist of the family name and a suffix –
|> |> BadVirus.a, for example. The suffix continues
|> |> in alphabetical order until it reaches z. Then
|> |> it begins again with aa and continues to az.
|> |> Still later variants receive the suffix ba
|> |> through bz, and so forth, until the suffix
|> |> reaches zz. If yet another variant appears
|> |> after that, it will have the suffix aaa.
|> |>
|> |> As new virus strains appeared, industry naming
|> |> conventions evolved to include more
|> |> information. Some names, for instance, include
|> |> parts that identify the platform on which the
|> |> virus can run.
|> |>
|> |> Among anti-virus vendors, virus names can
|> |> include a prefix, an infix and a suffix.
|> |>
|> |>
|> |> PREFIX
|> |>
|> |> The prefix designates the type of file that the
|> |> virus infects or the platform on which
|> |> potentially harmful software can run. Viruses
|> |> that infect DOS executables do not receive a
|> |> prefix. Our naming convention includes the
|> |> following prefixes:
|> |>
|> |> A97M/ Macro virus that infects Microsoft
|> |> Access 97 files.
|> |>
|> |> APM/ Macro virus or Trojan-horse program
|> |> that infects Ami Pro document and
|> |> template files.
|> |>
|> |> Bat/ Batch-file virus or Trojan-horse
|> |> program. These viruses usually run
|> |> as batch or script files that
|> |> affect a particular program that
|> |> interprets the script or batch
|> |> commands they include. They are
|> |> very portable and can affect nearly
|> |> any platform that can run batch or
|> |> script files. The files themselves
|> |> often have a BAT extension.
|> |>
|> |> CSC/ Corel Script virus or Trojan-horse
|> |> program that infects Corel Draw
|> |> document files, template files, and
|> |> scripts.

|> |>
|> |> IRC/ Internet Relay Chat script virus.
|> |> This virus type can use early
|> |> versions of the mIRC client
|> |> software to distribute a virus or
|> |> payload.
|> |>
|> |> JS/ Script virus or Trojan-horse
|> |> program written in JavaScript
|> |> language.
|> |>
|> |> JV/ Potentially harmful Java
|> |> application or applet.
|> |>
|> |> Linux/ Virus or Trojan-horse program
|> |> compiled for Linux OS in ELF file
|> |> format.
|> |>
|> |> LWP/ Potentially harmful software for
|> |> Lotus WordPro.
|> |>
|> |> MacHC/ Virus or Trojan-horse program for
|> |> Apple Macintosh HyperCard scripting
|> |> language.
|> |>
|> |> MacOS/ Virus or Trojan-horse program for
|> |> Apple Macintosh OS Versions 6-9.
|> |>
|> |> MSIL/ Application written using Microsoft
|> |> Intermediate Language framework,
|> |> also known as .NET.
|> |>
|> |> P98M/ Macro virus or Trojan-horse program
|> |> that infects Microsoft Project
|> |> documents and templates.
|> |>
|> |> PalmOS/ Virus or Trojan-horse program for a
|> |> Palm Pilot.
|> |>
|> |> PDF/ File-infector of Adobe PDF files.
|> |>
|> |> Perl/ Script virus or Trojan-horse
|> |> program written in Perl language.
|> |>
|> |> PHP/ Script virus or Trojan-horse
|> |> program written in PHP language.
|> |>
|> |> PP97M/ Macro virus. Infects Microsoft
|> |> PowerPoint 97 files.
|> |>
|> |> SunOS/ Potentially harmful software for

|> |> Sun Solaris.
|> |>
|> |> SWF/ Potentially harmful software for
|> |> Shockwave.
|> |>
|> |> Unix/ Program or a shell script for a
|> |> version of UNIX.
|> |>
|> |> V5M/ Macro or script virus, or
|> |> Trojan-horse program that infects
|> |> Visio VBA (Visual Basic for
|> |> Applications) macros or scripts.
|> |>
|> |> VBS/ Script virus or Trojan-horse
|> |> program written in Visual Basic
|> |> Script language.
|> |>
|> |> W16/ File-infector virus that runs in
|> |> 16-bit Microsoft Windows
|> |> environments (Windows 3.1x).
|> |>
|> |> W2K/ Potentially harmful software for
|> |> 32-bit Microsoft Windows
|> |> environments, specifically Windows
|> |> NT, 2000 or XP.
|> |>
|> |> W32/ File-infector or boot-sector virus
|> |> that runs in 32-bit Microsoft
|> |> Windows environments (Windows 95,
|> |> Windows 98 or Windows NT).
|> |>
|> |> W95/ File-infector virus that runs in
|> |> Microsoft Windows 95, Windows 98
|> |> and Windows ME environments.
|> |>
|> |> W97M/ Macro virus that infects Microsoft
|> |> Word 97 files.
|> |>
|> |> WHLP/ Potentially harmful software for
|> |> 32-bit Microsoft Windows
|> |> environments that targets Windows
|> |> HLP files.
|> |>
|> |> WM/ Macro virus that infects Microsoft
|> |> Word 95 files.
|> |>
|> |> X97M/ Macro virus that infects Microsoft
|> |> Excel 97 files.
|> |>
|> |> XF/ Macro virus that infects Microsoft
|> |> Excel 95 or 97 via Excel formulas.

|> |>
|> |> XM/ Macro virus that infects Microsoft
|> |> Excel 95 files.
|> |>
|> |>
|> |> PREFIX FOR TROJAN-HORSE CLASSES
|> |>
|> |> A name such as "BackDoor-" denotes potentially
|> |> harmful software that belongs to a class of
|> |> similar Trojan-horse programs. The class name
|> |> is followed by extra characters to denote a
|> |> family (such as BackDoor-JZ) or a name (such as
|> |> BackDoor-Sub7).
|> |>
|> |> AdClicker-
|> |> Repeatedly accesses web sites that
|> |> are funded by advertising.
|> |>
|> |> Adware- Installs advertising software but
|> |> does not ask permission.
|> |>
|> |> BackDoor-
|> |> Provides remote access or control
|> |> through the Internet or network.
|> |>
|> |> Dialer- Dials a phone number without asking
|> |> for permission.
|> |>
|> |> DDoS- Operates as a Distributed Denial of
|> |> Service component.
|> |>
|> |> Del- Deletes files.
|> |>
|> |> Downloader-
|> |> Downloads software from the
|> |> Internet, usually to deliver
|> |> backdoors, password stealers, and
|> |> sometimes viruses.
|> |>
|> |> Exploit- Uses a vulnerability or a software
|> |> defect.
|> |>
|> |> FDoS- Denotes a Flooding Denial of
|> |> Service component.
|> |>
|> |> KeyLog- Logs keystrokes for immediate or
|> |> future transmission to the
|> |> attacker.
|> |>
|> |> Kit- Denotes a program designed for
|> |> creating a virus or Trojan-horse

|> |> program.
|> |>
|> |> MultiDropper–
|> |> Drops several Trojan–horse program
|> |> or viruses (often several different
|> |> 'backdoors').
|> |>
|> |> Nuke– Uses defects in software on a
|> |> remote computer to bring it down.
|> |>
|> |> ProcKill–
|> |> Terminates the processes of
|> |> anti–virus and security products.
|> |> May also delete files associated
|> |> with such applications.
|> |>
|> |> PWS– Steals a password.
|> |>
|> |> Reboot– Reboots the computer.
|> |>
|> |> Reg– Modifies the Registry in an
|> |> undesirable fashion without asking
|> |> questions. For example, reduces the
|> |> security settings or creates
|> |> abnormal associations or sets.
|> |>
|> |> Spam– Acts as a spamming tool.
|> |>
|> |> Spyware– Monitors browsing habits or other
|> |> behavior and sends the information
|> |> out, often for unsolicited
|> |> advertising.
|> |>
|> |> Uploader–Sends files or other data from the
|> |> computer.
|> |>
|> |> Vtool– Denotes a program used by virus
|> |> writers or hackers for developing
|> |> software.
|> |>
|> |> Zap– Wipes all or part of a hard disk.
|> |>
|> |>
|> |> INFIX
|> |>
|> |> These designations usually appear in the middle
|> |> of a virus name. AVERT assigns these
|> |> designations, which differ from industry
|> |> conventions.
|> |>
|> |>
|> |> .cmp. Companion file that the virus adds

|> |> to an existing executable file. Our
|> |> anti-virus software deletes the
|> |> companion file to prevent later
|> |> infections.
|> |>
|> |> .mp. Legacy multi-partite virus for
|> |> DOS.
|> |>
|> |> .ow. Overwriting virus. This identifies
|> |> a virus that overwrites data in a
|> |> file, thereby irreparably
|> |> corrupting it. This file must be
|> |> deleted.
|> |>
|> |>
|> |> SUFFIX
|> |>
|> |> These designations usually appear as the last
|> |> part of a virus name. A virus name can have
|> |> more than one suffix. One might designate a
|> |> variant, for example, while others give
|> |> additional information.
|> |>
|> |> @M Slow mailer. This virus uses an
|> |> e-mail system to spread. It usually
|> |> replies to an incoming message
|> |> once, or attaches itself to an
|> |> outgoing message, or sends to just
|> |> one e-mail address.
|> |>
|> |> @MM Mass mailing distribution. This
|> |> virus might use standard techniques
|> |> to propagate itself, but also uses
|> |> an e-mail system to spread.
|> |>
|> |> .a - .zzz Virus variants.
|> |>
|> |>
|> |> In accordance with the CARO (Computer
|> |> Anti-virus Research Organization) naming
|> |> convention, the vendor-specific suffices can be
|> |> preceded by a "!" character. Our software uses
|> |> the following suffices:
|> |>
|> |>
|> |> apd Appended virus. A virus that
|> |> appends its code to the file it
|> |> infects, but fails to provide for
|> |> correct replication.
|> |>
|> |>
|> |> bat Software component in BAT

|> |> language.
|> |>
|> |> cav Cavity virus. This designates a
|> |> virus that copies itself into
|> |> "cavities" (for example, areas of
|> |> all zeroes) in a program file.
|> |>
|> |> cfg Configuration component of an
|> |> Internet Trojan-horse program
|> |> (frequently of a 'BackDoor-').
|> |>
|> |> cli Client-side component of an
|> |> Internet Trojan-horse program
|> |> (frequently of a 'BackDoor-').
|> |>
|> |> dam Damaged file. A file that is
|> |> damaged or corrupted by an
|> |> infection.
|> |>
|> |> demo Program that demonstrates
|> |> potentially harmful action, such as
|> |> an example of how an exploit
|> |> works.
|> |>
|> |> dr Dropper file. This file introduces
|> |> the virus into the host program.
|> |>
|> |> gen Generic detection. Native routines
|> |> in our software detect this virus
|> |> without using specific code
|> |> strings.
|> |>
|> |> ini An mIRC or pIRCH script when it is
|> |> a component of another virus.
|> |>
|> |> intd "Intended" virus. This virus has
|> |> most of the usual virus
|> |> characteristics but cannot
|> |> replicate correctly.
|> |>
|> |> irc IRC component of potentially
|> |> harmful software.
|> |>
|> |> js Potentially harmful software
|> |> component in JavaScript.
|> |>
|> |> kit Virus or Trojan-horse program
|> |> created from a 'virus construction
|> |> kit'.
|> |>
|> |> p2p Potentially harmful software that

|> |> uses peer-to-peer communication to
|> |> function. For example, Gnutella and
|> |> Kazaa.
|> |>
|> |> sfx Self-extracting installation
|> |> utility for Trojan-horse programs.
|> |>
|> |> src Viral source code. This ordinarily
|> |> cannot replicate or infect files,
|> |> but some virus droppers add this to
|> |> files as part of the infection
|> |> cycle. Our products routinely flag
|> |> files with additional code of this
|> |> sort for deletion.
|> |>
|> |> sub Substitution virus. It substitutes
|> |> the host file with itself, so that
|> |> all infected hosts are of the same
|> |> size and are a pure virus. (That
|> |> is, a subclass of overwriting
|> |> viruses.)
|> |>
|> |> svr Server-side component of an
|> |> Internet Trojan-horse program,
|> |> often of a 'backdoor'.
|> |>
|> |> vbs Potentially harmful software
|> |> component written in Visual Basic
|> |> Script language.
|> |>
|> |> worm A non-parasitic virus that copies
|> |> itself, or a virus that propagates
|> |> through a network by copying to
|> |> remote computers or by sending
|> |> itself out via any means of file
|> |> transmission such as remote shares,
|> |> peer-to-peer, instant messaging,
|> |> IRC file transfers, FTP, and SMTP.
|> |>
|> |>
|> |> **GENERIC DETECTIONS**
|> |>
|> |> Our software detects a huge amount of
|> |> potentially harmful software proactively and
|> |> generically. In most cases, such objects are
|> |> successfully cleaned even without AVERT ever
|> |> receiving a sample. Such detection is denoted
|> |> by "Generic" in the name or a "gen" suffix.
|> |>
|> |> To submit a sample to AVERT, visit the AVERT
|> |> home page. See "CONTACTING MCAFEE SECURITY &

|> |> NETWORK ASSOCIATES".
|> |>
|> |>
|> |> HEURISTIC DETECTIONS
|> |>
|> |> Our software detects a huge amount of new
|> |> potentially harmful software heuristically.
|> |> Such detection is flagged using the "New"
|> |> prefix to the name (for example "New Worm" and
|> |> "New Win32").
|> |>
|> |> To submit any sample that was detected
|> |> heuristically, visit the AVERT home page. See
|> |> "CONTACTING MCAFEE SECURITY & NETWORK
|> |> ASSOCIATES".
|> |>
|> |>
|> |>
|> |>
|> |>
|> |>
|> |
|> |
|>
|>
|
|