MacOS/SevenDust

Type	Virus
SubType	Macintosh
Discovery Date	06/01/1998
Length	varies
Minimum DAT	N/A (11/28/2005)
Updated DAT	4638 (11/28/2005)
Minimum Engine	N/A
Description Added	12/13/2002
Description Modified	12/13/2002 11:07 AM (PT)

Risk Assessment:

Corporate User
Low
Home User
Low

Overview:

This is a virus detection. Viruses are programs that self-replicate recursively, meaning that infected systems spread the virus to other systems, which then propagate the virus further. While many viruses contain a destructive payload, it's quite common for viruses to do nothing more than spread from one system to another.

Aliases:

- 666
- Graphics Accelerator
- Mac/SevenD
- Mac/Sevendust
- MDEF 666
- MDEF 9806
- MDEF E

Characteristics:

This is a family of seven viruses that infect Apple Macintosh applications by modifying MDEF resource. Some variants drop a system extension (ex., called '666' or 'Graphics Accelerator'), some introduce a new INIT resource in the System file.

The variant known as 'Graphics Accelerator' (variant .f) first appeared on the Info-Mac shareware archives. The file's author claimed that it was a custom extension that would speed up graphics routines in applications written for Motorola 68000-series processors, but run on computers with PowerPC processors. A file description included with it read:

"Enclosed you will find my custom Graphics Accelerator that helps PPC macs speed graphics programs up that use 68K code. It uses a custom blitting subroutine, and it should work on PPC apps as well. Please include it in your Graphics/Utilities directory. Thank you very much."

This file was pulled from the site in September 1998. The source code for some SevenDust variants was circulated in the Internet so this family has many variants most likely written by different people. Latest strains are the first polymorphic viruses to appear on the Mac OS platform.

Symptoms:

Presence of '666' or '\001Graphics Accelerator' in the Extensions folder. Note that the extension dropped by the virus has an invisible character in front which makes it difficult to distinguish the file from a legitimate video driver from ATI that has 'Graphics Accelerator' name! The latest variant may drop its extension under different names but always has the first invisible character.

Variants .a-.d do not have any damaging payload. But computers infected with the most common variant (aka 'Graphics Accelerator') erase all non-application files started during the sixth hour of the 6th or 12th day of any month.

Method of Infection:

Members of this family hit MDEF and INIT resources. Infected applications have MDEF resource, the System has INIT. There are seven known variants:

Variant .a
Only hits MDEF 666 and INIT 666 resources. Drops extension '666'. Size is 850 bytes.

Variant .b
Only hits MDEF 666 and INIT 666 resources. Drops extension '666'. Size is 1342 bytes.

Variant .c
Hits MDEF and INIT resources with random IDs (from 1 to 255). Drops extension '666'. Carries 'BACH' string for self-recognition. Size is 1576 bytes.

Variant .d
Hits MDEF and INIT resources with random IDs (from 1 to 255). Drops extension '666'. Carries 'BACH' string for self-recognition. Size is 2036 bytes.

Variant .e
Also known as MDEF-E virus. Hits MDEF and INIT resources with random IDs. Carries "JSBACH" string (apparently an abbreviation for Johann Sebastian Bach). When this variant infects an MBDF resource it saves its original contents in the encrypted form along with the encrypted virus body.

Variants .f-.g
Hit MDEF and INIT resources with random IDs and carry "JS" string for self-recognition. When this variant infects some MBDF resource it saves its original contents in the encrypted form along with the encrypted virus body. Drop extension '\001Graphics Accelerator', 'ExtensionConflicts' or introduce an INIT in the System file. Dropped extension file carries the virus body in the INIT 33 resource. These variants will modify 'WIND' resource to complicate removal (so-called symbiotic property). The 'MENU' resource is overwritten with the character 'f' (hexadecimal 66).

Note: Even though this virus strain used '666' label there is no reason to believe that it has any relation to the Spanish 29A virus writing group (hexadecimal for 666 is 0x29A).

Removal:

Please use the latest updates of Virex for cleaning. If this threat is detected on a Macintosh please use Virex to repair it.
If the infected object was found on a non-Apple file server it can be cleaned using Virex from a Macintosh client.
Infected Emails (usually in BinHex format) will be currently either deleted or quarantined depending on the configuration of mail scanner. Quarantined mails should be transferred to a Macintosh and cleaned using Virex.