# Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

## Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials: Network, Endpoint, and Cloud (Security 401)"
at http://www.giac.org/registration/gsec

# The FunLove Virus Worm

Douglas Dodge
GSEC Level One
12/2/2000

## FunLove Virus – My personal experience

I was sitting at my PC at work last Tuesday morning, November 28, 2000, trying to decide what subject to write my GSEC practical assignment on. The only related security experience I have had to speak of to this point was being without e-mail for three days due to the "ILoveYou" outbreak. That subject was well represented. What else could I write about? Suddenly my Internet connection is taken down. Next e-mail is inaccessible, quickly followed by my Window NT shared network drives. What is going on? It's not long before the Systems Administrator comes by to tell me, "the systems have a virus." People around me start running virus scans and immediately my co-worker reports: "I have 569 FunLove virus file infections on my PC!" (It was later determined that this machine was one of the "host" machines which I will define later.) The security department does not currently employ me, however my Administrator is aware of my interest and SANS security certification. I jumped at a chance to volunteer to help out, and my offer was quickly accepted. I was taken behind the secured doors of the company's computer room to the command center. Administrators were calling in to a conference call from all over the country reporting virus activity. As I'm listening to the issues everyone is wrestling with and watching the operators unplugging every server connection in the room, I'm remembering predictions and recommendation I have learned throughout my SANs course work. I am amazed at how accurate these turn out to be. I also now know what I want to write my SANs practical assignment on.

## FunLove Virus - What is it?

The name of the virus we are wrestling with is called FunLove. This virus is not new as it was discovered and documented around 11/9/99. However on November 28, 2000 it is new to my company. FunLove first appeared from Newsgroup Posting. FunLove is known by the alias: FLCSS, W32.FunLove.4099, W32/FLCSS, W32/FunLove.4099.dr, WIN32.FLC, WIN32.FunLove.4070. There are no known Variants located in my research. One article suggested that due to FunLove virus complexity variations are unlikely. The virus patches files with an infection length of:

- WIN 9X file length increases 4099 bytes
- WIN NT file length increase minimum 4099 or more up to 7000 bytes.

FunLove is described as a memory resident WIN32 virus. It is not encrypted or polymorphic. FunLove replicates under Windows 9X and Windows NT systems. It infects applications with an extension of: .exe, .scr, or .ocx. It does not infect files that

© SANS Institute 2000 - 2005 Author retains full rights.

have one of the following four characters in the beginning of their names: aler, amon, avp, avpe, avpm, f-pr, navw, scan, smss, ddhe, dpla, mpla. These are names associated with anti-virus programs, as well as other applications. There are a large number of infections around the world, over 1000 reported in: US, Canada, UK, China, Czech, and Singapore. The FunLove virus is easy to detect but difficult to remove. As I prepare to send this, one week after infection cleanup we are still having isolated FunLove infections reported in our system. FunLove does not destroy files but rather adds the name of an obscure rock band "Fun Loving Criminal" into the infected files. When an infected file is run in DOS mode this name is displayed and the computer is reset. On WIN 9X and WIN NT infected applications will drop the program file flcss.exe into the system folder which will assure it is run again at boot time. Once an infected machine is rebooted the machine becomes a "host" and spreads the virus to local and shared network drives. For this reason it is recommended that if you discover a file with this virus infection to turn your machine off and boot from emergency repair disk only.

## FunLove Virus - How to detect it

To detect FunLove virus one or more of the following may be observed:

- Increase in size by 4099 WIN 9X or a variable length of at least 4099 under WIN NT
- Band name message as described above is displayed and system is reset from DOS
- Existence of file flcss.exe in system folder and/or running flcss service on WIN NT (I was able to display NT services on a host machine see flcss started and running.)
- Activity on local hard drive or over shared network drives with everything shutdown (I witnessed this too, as everything was shutdown and display of system monitor shows CPU at 20% usage, as the virus was busy scanning and infecting files).
- Certified ActiveX control gives warning that signature no longer matches the file. This happens only if your web browser is set to this higher level of security. Lower security setting will allow infection to occur undetected.
- Application or system performance is degraded or crashes.
- Virus protection software alerts to FunLove virus file infection.

## FunLove Virus - How it works

When an infected file is run, the virus becomes memory resident and drops a file called flcss.exe into the system folder. The machine becomes a virus "host" once the machine is rebooted. This flcss.exe file then runs as a separate process and directly infects all: .exe, .ser, .ocr files including those in subfolders at a random rate of infection. Due to flcss files location it will be re-executed whenever system is restarted. This file runs as a hidden Windows application under WIN 9X or as a Windows service under WIN NT. The infection scans all local and shared network drives from C: to Z: looking for files with the specified extension to infect. This infection is possible over shared network drive connections even without any one being logged on. It is for this reason that FunLove is

© SANS Institute 2000 - 2005 Author retains full rights.

considered a virus worm. In addition under WIN NT the virus patches the files NTOSKRNL.EXE and NTLDR. If user is logged in with administrative rights or equivalent, the virus changes file attributes of these files from Hidden to Archive, then modifies only 2 bytes in a security API called SeAccessCheck. This gives full access to all users to each file regardless of its protection. Therefore the person with lowest rights can now modify all files even those requiring the highest authority, and thus spread the virus. This infection is not detected during boot time. This and the virus's ability to attack over shared network drives, makes it is very difficult to remove. To prevent further infections it is recommended that all network cables be unplugged as soon as possible to protect clean machines from infection.

## FunLove Virus - A closer look at the file infection

During infection the virus code is appended to the end of a target file. It then patches this file with 8 bytes of code at the startup. These 8 bytes pass control by jumping to the virus code, which has been appended. Once the virus is activated the virus starts and restores the first 8 bytes that make up the start up routine and allows the main code to begin. This makes it very difficult to determine that a program is infected, since it will appear to run as normal. (Note in researching FunLove virus some authors classify the FunLove virus as a Trojan. It is easy to see why based on the way it disguises and runs it's payload. However more recent articles describe the virus as a Worm since it can infect machines through shared drive connections even without people being logged on.) Over time infections can degrade performance, corrupt Windows applications, cause system instability and sometimes crashes. Because the virus infects ActiveX controls .ocx files it is possible to get infection from web-browser that supports ActiveX, or web server that contains web pages infected with embedded ActiveX controls. Anyone downloading and executing ActiveX controls will be infected if the ActiveX control is unsigned and browser security is set to low. If however the infected ActiveX control is signed and browser security is set higher, the virus infection will cause a warning to be issues and an option to not run the ActiveX control given.

## FunLove Virus - How to clean it up

The following links and downloads will provide a detailed description and cleanup procedure:
http://vil.nai.com/VIL/virusRemovalInstructions.asp?virus_k=10419
Note: There is a download file "Cleaning Windows NT NTFS systems" or go to
http://vil.mcafee.com/dispVirus.asp?virus_k=10419&
Note: There is a very helpful download text (.RTF) file located on the above link titled: Removal of the FUNLOVE virus Worm in an Enterprise Environment, see also
http://download.nai.com/products/mcafee-avert/flclean.htm

© SANS Institute 2000 - 2005 Author retains full rights.

Briefly the .RTF file above describes four phases of virus cleanup. It is interesting to note that the cleanup process recommends preparing for cleanup by unplugging network cables, and identify host machines that are attaching, before considering removing any infected files. The document stresses that it is important to keep clean machines unplugged from any network until all systems are cleaned. The virus in any infected system can infect the network and shared space as fast as it can be cleaned. The cleanup phases described are:

- First Phase is inoculation by creating the folder flcss.exe in C: \winnt\system32 for WIN NT or in C:\windows\system for WIN 9X. If this folder already exists the virus dropper will not be written.
- Second Phase is identifying infected machines. In our case anti-virus software was able to detect infections.
- Third Phase is containment. Any infected machine without flcss.exe needs to have infected files cleaned only. Any machine with flcss.exe (more common) must proceed to Fourth Phase.
- Fourth Phase is eradication. This requires following specific cleaning instructions found at the above link to remove.

## FunLove Virus – I'm not the only one

FunLove virus is not a new virus but it continues to plague corporations throughout the world. I have personally observed and now experienced this virus. The Internet was full of reported cases of FunLove infection: A few have been listed below:

- Pleasant Valley High School (Chico, CA) reports having to return to "old school" pencil and paper administration due to FunLove infections.
- VA Office of Information Technology - numerous FunLove infections
- Princeton University - numerous FunLove infections
- Drexel University- numerous FunLove infections
- John Hopkins University - numerous FunLove infections
- Singapore schools closed due to FunLove infections

The FunLove virus does not just impact schools. The FunLove infection which received the most press during my research was:

- Dell Computer Corporation announces that it closed its Limerick factory and halted PC production for two days. Dell had to check 12,000 PCs for FunLove infection including recalling 500 it had already shipped to homes.
- SANS NewsBites Vol. 1 Number 35 reports "Dell recalls Computers possibly infected with FunLove virus".

## FunLove Virus – References

F-Secure Corporation. "F-Secure Virus Descriptions". F-Secure Computer Virus Information Pages: FunLove.

© SANS Institute 2000 - 2005, Author retains full rights.

URL: http://www.datafellows.com/v-descs/funlove.htm

Network Associates, Inc. “Variants / Aliases”. McAfee – AVERT.
URL: http://vil.nai.com/VIL/virusVariantAndAliases.asp?virus_k=10419

Network Associates, Inc. “Profile”. McAfee – AVERT. September 30, 2000.
URL: http://vil.nai.com/VIL/virusChar.asp?virus_k=10419

Network Associates, Inc. “ McAfee – AVERT.
URL: http://vil.nai.com/VIL/virusRemovalInstructions.asp?virus_k=10419

ZDNet. “How it Works” . ZDNet: Help & How-To: How it Works. October 2, 2000.
URL: http://www.zdnet.com/zdhelp/stories/main/0,5594,2393098-2,00.html

SYMANTEC.”W32.Funlove.4099”. AntiVirus Research Center. November 8, 2000.
URL: http://www.symantec.com/avcenter/venc/data/w32.funlove.4099.html

Network Associates Inc. “VIRUS ALERT: Network Associates Accelerates FunLove to ‘Medium Risk, on Watch’. November 12, 1999.
URL: http://www8.techmall.com/techdocs/TS991112-5.html

© SANS Institute 2000 - 2005 Author retains full rights.

© SANS Institute 2000 - 2005 Author retains full rights.