VIRUS ANALYSIS 1

Warped Logic?

Peter Szor
Symantec Corporation

In early April 2001 the news coming from the marketing departments of certain anti-virus vendors was yet again spreading faster than the actual worm to which it referred. A new *Logo* worm had been written and mass-mailed to some of the anti-virus companies by its creator. It never became wild though, and there is definitely more than one reason for that.

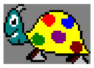
Its author is female and she calls herself Gigabyte. Yes, that is right. It is actually written by a female virus writer – this is pretty rare. At least this is the claim made in stories of virus writer meetings published in various places on the Web.

Gigabyte has a background of creating other malware and in particular she authored *MIRC* worms. As we will see, she tried to use her existing *MIRC* knowledge to create the Logo/Logic worm.

The actual worm is created in *Super Logo*, a reincarnation of the old *Logo* language for *Windows* platforms. It is claimed to be 'the Windows platform for kids'! Well, when I was 14, I came across several *Logo* implementations for various 8-bit computers.

I must admit that back then I only dreamed about the graphical capabilities that *Super Logo* provides on modern *Windows* computers. Our 8-bit school computer had a top screen resolution of about 118x72 dots in black and white. Since that is not a challenge any more, people try to write a worm in *Super Logo*. Logical, isn't it? Let's see how it was done.

Turtle Torture



The *Logo* language's primary purpose is to provide drawing with a 'Turtle'. The Turtle is the pen and its 'head' can be turned around and instructed to draw. For instance, *Super Logo* uses the following commands: HIDETURTLE, FORWARD, PENUP, PENDOWN, WAIT, etc. The set of commands can be formed as subroutines and saved in a *Logo* project file with an .LGP extension.

The actual project file is a pre-tokenized binary format but the set of commands, as well as variable names, remain easily 'readable' and stored as *Pascal*-style strings. The project file can be loaded and executed with the *Super Logo* interpreter. Furthermore, even the demo version shows the easy-to-understand source of any project files.

Up until now, many European schools teachers have been using *Logo* to teach the programming basics to young students. The original *Logo* language has been very well extended in *Super Logo* to compete with other existing implementations. It can deal with multiple graphical objects at the same time and move them around on screen with complete mouse support.

However, it is easy to find out that the *Super Logo* language does supports neither mailing nor embedded executables. Furthermore, it does not support the 'Spawning' of other executables or scripts. Fortunately.

Unfortunately, *Super Logo* does support a PRINTTO 'XYZ' command. XYZ can be a complete path to a file. With that statement a *Logo* program might modify, for example, WINSTART.BAT, overwriting its content with:

```
“@cls
@echo You think Logo worms don’t exist?
Think again!”.
```

Get the point? When the LOGIC.LGP project is loaded and executed, the worm will draw 'LOGIC' on the screen and then it prints 'Logic, the Logo worm © Gigabyte' to the *Logo* prompt. The project file will be executed by clicking on it once *Super Logo* is active.

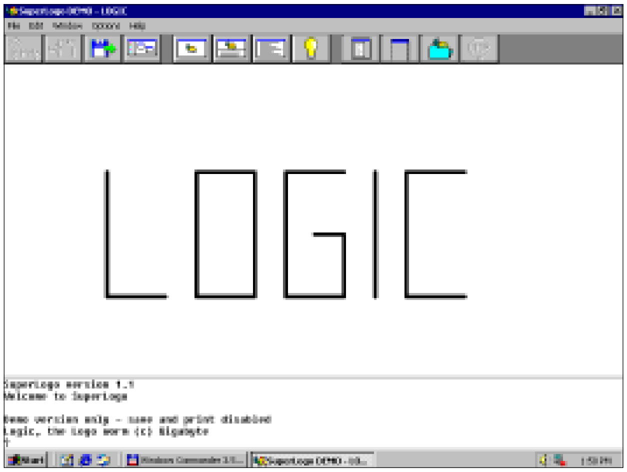
The worm will make sure that a STARTUP.VBS file is created in one of the *Windows* startup folders and as such executed automatically the next time when *Windows* is booted. Furthermore, the worm also tries to modify the shortcuts (if any) of some of the common *Windows* applications such as NOTEPAD.EXE to start the VBS file without the need of a reboot.

This VBS file would propagate the 4,175 byte-long LOGIC.LGP worm project file to the first 80 entries of the *Outlook* address book – a pretty standard VBS email propagation. The subject of the email is 'Hey friends!' and the body of the message reads 'Hello! Look at my new SuperLogo program! Isn't it cool?'. The worm, however, has a set of bugs: the actual project file will always be in E:\MIRC\DOWNLOAD\LOGIC.LGP.

On most machines *MIRC* would be more likely to be installed on the C: drive. On the top of that, the VBS-based propagation will fail if the LOGIC.LGP file has not arrived via *MIRC* first. Oh, well.

I can hear you say that this would never work, but the worm actually supports *MIRC* propagation by using the /DCC send command in the SCRIP.INI of the active *MIRC* directory. The Logic worm only checks for SCRIPT.INI in a few specific locations but it might get it right. The SCRIPT.INI file will have an accurate drive letter for the path of the LOGIC.LGP file.

Assuming that the LOGIC.LGP attachment arrives beforehand via an *MIRC* infection, and that the file is then placed in the MIRC\DOWNLOAD directory, the SCRIPT.INI modification will propagate the LOGIC.LGP file to anybody in the active IRC channels. Thus, a machine needs to have *MIRC* installed. It needs to be compromised via *MIRC* first.



```
SuperLogo version 1.1
Welcome to SuperLogo

Demo version only - save and print disabled
Logic, the Logo worm (c) Gigabyte
```

If all that happens, it is likely to email its project file as long as the *MIRC* directory is on the E: drive, as it was on the worm's creator's machine. So what we can say about this new creation is that it is certainly not an intended worm, but it is a buggy one.

Conclusion

The Logo/Logic worm was an interesting one for me to investigate in many ways. There are several possible endings to this on-going story. It's clear that innocent project files might well become the platforms of tomorrow's worms from one day to the next.

Having said that, corporations might not get hit by a *Super Logo* worm easily (especially if they do not run *Super Logo* in the first place) but they might well run a set of interpreter-based logic in many hitherto uninfected applications.

As ever, people need to think before they click. That's all very well, but they will not necessarily know all the bad things they should not click on at any given point in time. Just to be sure, let's add yet another extension to our extension list!

Logo/Logic

Aliases:	Logic worm.
Type:	*MIRC*, VBS worm replication initiated from *Super Logo* project file.
Activation:	Worm displays LOGIC in big letters on each execution.
Removal:	Delete infected files and restore from backups.

No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form without the prior written permission of the publishers.