

Infectable Objects Part Five - HTML and Other Scripts

Robert Vibert 2001-04-18

Infectable Objects, Part Five - HTML and Other Scripts

by Robert Vibert

last updated April 18, 2001

One of the more interesting developments in the virus world has been the extension of viruses from compiled executable files into script files. Just as was the case with macros, which infected previously safe document files, there is now an expanding range of script file types that can contain malicious code.

At least as far back as 1989, virus researchers were discussing the experimental viruses that could be created in scripting languages such as that supplied with the Lotus 1-2-3 spreadsheet application. These experimental viruses were never seen in the wild, and most of these discussions were conducted amongst specialists.

Today, the scene is very different, with regular discoveries of new script file types that can contain viral code. While many viruses have been written using a scripting language, it is not as common for them to try to infect an existing script the way that other viruses infect executable code in compiled EXE and COM files. Instead, most of these viruses make use of scripting languages as an intermediate step in their spread.

All the same, the threats posed by these viruses are just as serious. LoveLetter, the most well known virus/worm written in Visual Basic Script, has the dubious distinction of causing the most damage ever seen from a single piece of malicious code.

The script types that can be affected or used by viruses include the normally innocuous batch file (.BAT), the configuration files used by IRC programs (.INI) and the ubiquitous HTML and kindred files on millions of web sites worldwide.

Holy Hot-Buttered Popcorn, Batman!

One of the earliest examples of a script virus was found in early 1993. Batman, as it was called, used a batch file containing binary code to create a virus executable, run it and then delete it. It is a simple virus, but does go memory resident and can cause performance issues, as it will fill up the RAM memory of a PC if run multiple times. Of course, no bad turn goes unrewarded in

the virus world, as copy-cat batch file viruses appeared as time went by.

By late 1993, the Carbuncle virus, which used a batch file to help spread infections, had been found. Later batch file viruses include Winstart, which contains binary data in the batch file to create a .COM virus, and SayNay, which added the trick of dropping assembler code into a file.

By November 1996, batch file viruses were starting to get more complex, although not seen in any great quantities. Highjaq appeared as a .BAT file, a .COM file, and a device driver and infects .ARJ archive files.

In the fall of 98, the Shiver virus appeared, making use of a batch file to trigger the Regedit program to modify a registry key that would disable MS Excel's macro virus protection.

In mid-99, the Coke virus made its showing. It uses a batch file to drop a virus executable, run it and then clean up all traces of infection, including the batch file itself.

Not Safe to Chat Any More?

While batch file-based viruses were not commonly seen, the same cannot be said for viruses that attacked the configuration files of popular IRC (Internet Relay Chat) programs.

In the fall of 97, users of the mIRC program started to notice some strange behaviour with a Script.INI file that was being sent to them by others on a chat channel. Since then numerous viruses have targeted this file. IRC enables viruses to travel around via DCC - Direct Client-to-Client connection. DCC permits the exchange of files with the user having little awareness of what was actually arriving. The damage caused by viruses using Script.INI included setting up the victim's PC as a file server, granting access to the files on the PC to others in a chat channel, and blanking out sections of WIN.INI and SYSTEM.INI files, rendering the system unstable at best. Less serious payloads include forcing the victim off the channel when a keyword is used. Users with version 5.31 or later of the mIRC client software are essentially protected against these viruses due to configuration changes made with regard to the handling of DCC.

As not everyone has upgraded to the latest version of mIRC, there are still cases of viruses and Trojans such as Fono and DMSsetup occurring in the IRC channels. As well, authors still create malware to exploit both the mIRC and pIRCH chat programs.

Have a Cuppa?

In September of '98, StrangeBrew, the first virus for Java, made its debut. As it infected other class files and replicates, there is no doubt it was a Java virus. However, like BeanHive, the second Java virus, it has rarely, if ever, been seen outside a lab. BeanHive needs to be linked to the Internet so it can download code each time it runs. It infects using a novel technique of storing not the code itself in the infected file, but a just a loader component. At present, these are reportedly the only two pure Java viruses.

JavaScript, on the other hand, is a different case. JS/Judgement is a good example of a JavaScript virus. It looks for mIRC and creates two files: default.INI and default2.INI, then modifies the MIRC.INI file to load the two new INI files. These new INI files provide back doors into mIRC and control over the computer. It then creates a file called WIN.JS and configures Windows to auto-load this file on startup.

The best known of the JavaScript viruses appeared in the fall of 1999. JS/Kak uses JavaScript and ActiveX code to infect machines. Kak has been one of the more prolific viruses, as it exploits a security vulnerability in MS Outlook Express. Kak spreads itself via embedded code in e-mail messages.

JS/Logo, another script virus, takes a different approach. When one views a web page containing the JS/Logo Trojan, the JavaScript code in the page tries to use the MS Internet Explorer Scriptlet.typelib security vulnerability to create a file, LOGO.HTA, in the victim's startup folder. If successful, the virus will then activate upon system reboot.

Viruses on Web Pages?

In addition to JS/Logo, there a few viruses that infect the common web page HTML file formats. Several examples attack any HTML, HTT, and HTM files on your local drive. The HTML.NoWarn and HTML.Internal viruses infect by writing themselves to the beginning of the infected file, with the NoWarn variant not affecting the rest of the file. The viruses themselves are written in Visual Basic.

The PHP.Newworld virus made the headlines briefly in early 2001. It appends an include instruction to the end of an infected file to point to virus code. It attacks PHP (Hypertext Preprocessor scripting), HTML, HTM, and HTT files. This infection technique means that it

cannot spread itself to other computers, somewhat limiting its reach..

PHP/Sysbat, another example of viruses using web code, appends text to the end of the Config.SYS , Autoexec.Bat and all .SYS files in the C:\Windows\command directory on systems running a PHP interpreter. Again, it has not been widespread; however, it suggests a path that virus authors may explore in the future.

The JS/Seeker virus comes in a file called Runme.hta and attacks the Windows registry. Other viruses that use the HTA format include BubbleBoy, Hopper, and Kak.

Scraps

Some viruses make use of one file format to transport their code written in a scripting language. The most well-known example of this is the Love Stages virus, which uses the Shell Scrap Object - SHS and SHB file types - to transport its VBS code. Shell Scrap objects can contain any code.

Script.Inf is a piece of malware that infects Windows INF files. Windows will run the script commands in an INF file. Like other viruses, Script.Inf makes use of a few other steps when infecting, creating a TXT file and then appending it to the AUTOEXEC.BAT file so it runs at system startup.

For Corel scripts, there is the CSC/CSV or Gala virus. It searches for Corel Script files, which have the CSC extension and infects them by writing code to the beginning of the file. Corel Script is similar to Visual Basic, which made it relatively easy for someone to produce a virus that could draw upon the examples in existence.

This is the End

This is the last article in this series on the types of objects that can be infected or carry infections. Even as I was writing each installment, I discovered that more and more types of files were falling victim to viruses. Although we've covered many types, there are still more out there that can and will be infected.

One of the common requests I received from readers of this series was for the location of the definitive listing of file extensions to scan with anti-virus products. The reality is that this list is

like Eldorado - an unattainable, fictional utopia. The best approach is also the simplest - if using a virus scanner, have it inspect all file types and extensions. While some scanners are not able to intelligently decipher the type of all files encountered, and extensions mean little these days as virus authors routinely use double extensions and other tricks to disguise their creations, scanning all files is the only way to be certain that viruses lurking in extensions you would not normally associate with malware are most likely to be found. Trying to remember which files to scan and which not to is a waste of time and effort. There are some speed issues that will arise with the approach of scanning all files. Some anti-virus scanners are better at this work than others, and only by experimenting with your own configuration will you discover which works best for you.

The table below is extracted from my book, The Enterprise Anti-Virus Book, and contains a listing of script related file types which could contain infected code.

Infectable Object	Description
.ASP	Active-X components of Active server pages
.BAT	DOS Batch files
.CSH	C Shell Script
.CHM	MS Compiled HTML Help
.CLA(SS)	JAVA file
.CSC	Corel Script
.CSS	Cascading Style Sheet
.HT?	HTML variant
.HTM	HTML variant
.HTA	HTML variant
.HTML	HTML variant
.HTT	Hypertext Template
.INI	mIRC - SCRIPT.INI
.INI	pIRCH - EVENTS.INI
.JS	JavaScript source
.JSE	JavaScript Encoded Script File
.MHT	HTML code
.MHTML	HTML code

.SCT	Windows Script Component
.sh	Bourne shell or Korn Script
.SHB	Shell Scrap object
.SHTML	HTML file
.VB	VBScript File
.VBS	Visual Basic script file
.VBE	Visual Basic encoded script
.VBX	Visual Basic Extension
.WBT	Windows Batch file
.WSC	Windows Script Component
.WSF	Windows Script File
.WSH	Windows Scripting Host Settings File
.XML	Extensible Markup Language (HTML extension)
.XSL	Extensible style sheet language
Shell scripts (Unix)	
PERL (Unix)	
Lotus 1-2-3 script	

Relevant Links

[Infectable Objects Part 1 - DOS](#)

Robert Vibert

[Infectable Objects Part 2 - Windows Infectable](#)

Robert Vibert

[Infectable Objects Part 3 - Win Apps](#)

Robert Vibert

[Infectable Objects Part 4 - Viruses in Archive Files and Compressed Files](#)

Robert Vibert

[Guidelines for Safer Computing](#)

Sophos

[Java_Bean](#)

Trend Micro

Java_StrangeBrew

Trend Micro

[Privacy Statement](#)

Copyright 2006, SecurityFocus