A Solution to Computer Infection with 1KB Folder Virus - Taking School Teaching and Office Scenarios as an Example

Hao Wu, Xianghui Liu, Xiufeng Yao

Beijing Polytechnic, 100176

starcraftwh@163.com

Abstract. The "1KB" folder virus (Worm. Script. VBS. Autorun. be), also known as the "Storm 1" virus, is harmless but deceptive. It can hide files and folders in the USB flash drive and generate some fake "exe format" folders, mislead users to click and trigger the virus.The purpose of this paper is to analyze its emergence, reasons for existence and relevant solutions in school teaching and office computers.

Keywords: 1kb virus;Teaching;to work in an office;Solution.

1. The Operating Principle of Viruses and the Reasons for Their Spread and Retention in School Computers

1.1 Operating principle of "1kb" folder virus

When we use a USB flash disk in computers in many public places, such as schools, we often find that when the USB flash disk is connected to another computer, the files in it will disappear strangely, and the folders will become 1kb.Faced with this situation, many people will doubt that their files are really lost.If there are many or important things in it, we will regret it.If there is not much content in it, many people will resolutely perform formatting operations.However, if you right click the drive letter and select Properties to view the size of the memory, you will find that its capacity has not changed.This actually shows that the files inside are still there.

In fact, the memory itself did not have a problem, but was infected with this virus, which is also known as the "1kb" folder virus of "Storm One".This virus is actually a simple script virus, or a script file with the extension ". vbs".After the computer is infected, point to this script file through AutoRun.inf on the disk.At this point, the virus will automatically run and infect the root directory of this disk. These directories become shortcuts and then point to the vbs file.For the folder in the disk directory, the virus first changes the attribute of the original folder to "System"+"Hidden", and then generates an. exe file with the same name to disguise it as the original folder, so that it can continue to spread.Sometimes, this virus will also infect other partitions of the hard disk.

1.2 Reasons for the spread and retention of viruses in school computers

School teaching and office computers often copy files through a USB flash disk.Especially for the computers used in the classroom, different teachers will copy the courseware for each class, and sometimes students will use it for some operations such as data transmission.If the virus exists in the storage medium of a teacher or student, it will spread when he connects the USB flash disk to a computer in the class or office.Other teachers or students will take the virus to other places after connecting the computer to the USB flash drive.The teacher's USB drive may bring the virus to other classrooms, offices or even homes.Students' USB drives will also bring the virus to dormitories, libraries or other places.The computers in the school are often in the same LAN.There is also a potential risk of virus outbreaks within the LAN.

Because the virus is extremely hidden, it is often not found by people.In addition, teachers and students in school often contact a fixed number of computers.A teacher will use the same computer in the same class for at least one semester.On the computer that has been infected with the virus, after the USB drive is accessed, the disguised folder exists as a virus file with the extension of

"EXE".This file looks like a real folder. Double click it to enter the next level.Therefore, users will not notice it for a long time.The virus also survived.

2. Solution after infecting "1kb" folder virus

2.1 Use conventional anti-virus software for anti-virus processing

The operating mechanism of the virus is not complicated and the harm is not great.However, for many organizations, most computer users are ordinary workers who have no technical foundation and cannot understand the operating principle of this virus.The computer they use may be infected with a virus for a long time before they realize it.Therefore, for most people, anti-virus software can be used for processing.In addition, there are also many companies that have launched some special killing tools on the Internet, such as 360, Kingsoft, Rising, and so on.These anti-virus software or special tools can be installed or downloaded for direct use.

However, it should be noted that some anti-virus software will change the folder and file attributes that have been tampered with back after anti-virus, that is, change the "hidden" status of folder and file attributes back to the normal status.Some anti-virus software will not repair the properties of folders and files, and users need to change the settings themselves.

2.2 Script for processing

In view of the feature that the virus will modify folder and file attributes, we can write a script file aimed at forcefully recovering file attributes.

Create a new Notepad text document (.txt) on the desktop. At this time, the computer system should set the display file extension status.Setting method: Open "My Computer" -- click "Tools" -- select "Folder Options" -- switch to the "View" tab -- see "Hide extensions of known file types" in the "Hide files and folders" option in the "Advanced Settings" displayed below, and remove the check in the front box.Then click OK (if the file extension in the system is displayed, do not modify it).

Open the newly created notepad document, and enter the following content (a script code based on HTML language):

```
<HTA:APPLICATION
  ID="Enter your desired nickname"
  APPLICATIONNAME="Folder Attribute Batch Modification Tool"
  BORDER="thin"
  BORDERSTYLE="normal"
  CAPTION="yes"
  CONTEXTMENU="no"
  INNERBORDER="no"
  MAXIMIZEBUTTON="no"
  MINIMIZEBUTTON="yes"
  NAVIGABLE="yes"
  SCROLL="auto"
  SELECTION="no"
  SHOWINTASKBAR="yes"
  SINGLEINSTANCE="yes"
  SYSMENU="yes"
  VERSION="Beta 1.0"
  WINDOWSTATE="normal"
/>
<HTML>
<HEAD>
```

```
<TITLE>Folder attribute batch modification tool - By: input your desired nickname at will</TITLE>
<meta http-equiv="Content-Type" content="text/html; charset=gb2312">
<STYLE TYPE="text/css">
</STYLE>
<SCRIPT LANGUAGE="javascript" TYPE="text/javascript">
window.onload = config;
var $ = document.getElementById;
var fso = new ActiveXObject("Scripting.FileSystemObject");
function config()
{
  if(!fso)
  {
    Alert ("Error: Cannot create the required object!");
    window.close();
    return;
  }
  If (! Window.confirm ("Do you want to change the properties of all folders under the root directory of the mobile disk to" Normal "?)
  {
    window.close();
    return;
  }
  Document. write ("<b>Folder Attribute Batch Modification Tool</b></br></br>");
  var all = new Enumerator(fso.Drives);
  while(!all.atEnd())
  {
    var i = all.item();
    if(i.DriveType == 1 && i.IsReady)
    {
      Document. write ("<i>An available mobile disk is detected"+i.DriveLetter+"("+i.VolumeName+")</i></br>");
      clear(i.DriveLetter + ":\\");
    }
    all.moveNext();
  }
  Document. write ("</br>-- By:<b>casually enter your desired nickname</b>["+new Date(). toLocaleString()+"]");
}
function clear(driverpath)
{
  var driver = fso.GetFolder(driverpath);
  var folders = new Enumerator(driver.SubFolders);
  document.write("<ul>");
  while(!folders.atEnd())
  {
    var i = folders.item();
    i.Attributes = 0;
    Document. write ("<li>change folder " "+i.Name+" "attribute+"</li>");
    folders.moveNext();
  }
```

```
     document.write("</ul>");
     Document. write ("<i>Change the properties of all folders under directory " "+driverpath+" 
"!</i></br></br>");
    }
    </SCRIPT>
    </HEAD>
    <BODY>
    </BODY>
    </HTML>
```

Save the Notepad document and exit, and change its ". txt" extension to ". hta".Just run, and the hidden folder will come back.The shortcut that cannot be deleted can be deleted directly.This ensures the normal use of the USB stick.After that, we can use anti-virus software to clean up the virus.Of course, to ensure that the virus will not repeat again, you can create a file named "autorun. inf" in the disk as immunity.Because the virus itself wants to run automatically, it will also produce this file, and the computer does not allow two files with the same name to exist at the same time. We will occupy the file name first, and the virus will not be built again.

3. summary

In fact, this virus is an old one, and the reason why it still interferes with people for a long time is precisely because it is highly covert and seemingly harmless.Especially in places like schools, except for students and teachers of relevant majors, other computer users have little knowledge of the virus, so that they infected other computers with the virus without knowing it.Although this virus is relatively simple to solve, it is also necessary for us to speak specifically as above, so that the majority of computer users can pay attention to it.If there are very important files in the USB flash drive and we happen to be infected with this virus, we should not rush to format the USB flash drive. We might as well try the above methods to avoid or minimize the loss.