McAfee Labs Threat Advisory
VBS/Autorun.worm

October 4, 2013

McAfee Labs periodically publishes Threat Advisories to provide customers with a detailed analysis of prevalent malware. This Threat Advisory contains behavioral information, characteristics and symptoms that may be used to mitigate or discover this threat, and suggestions for mitigation in addition to the coverage provided by the DATs.

To receive a notification when a Threat Advisory is published by McAfee Labs, select to receive “Malware and Threat Reports” at the following URL**:** https://sns.snssecure.mcafee.com/content/signup_login.

Summary

VBS/Autorun.worm has the ability to infect removable media devices. Infection starts either with manual execution of the infected file or by invoking the corresponding .LNK files that could cause automatic execution of the worm. After infection it may also download other malware or updates to itself directed by the C&C server.

Detailed information about the worm, its propagation, and mitigation are in the following sections:

McAfee Labs Threat Intelligence descriptions for this malware are available in the following locations:

http://www.mcafee.com/threat-intelligence/malware/default.aspx?id=3320377
http://www.mcafee.com/threat-intelligence/malware/default.aspx?id=3922462
http://www.mcafee.com/threat-intelligence/malware/default.aspx?id=3828819
http://www.mcafee.com/threat-intelligence/malware/default.aspx?id=3839940
http://www.mcafee.com/threat-intelligence/malware/default.aspx?id=3933216
http://www.mcafee.com/threat-intelligence/malware/default.aspx?id=3933217
http://www.mcafee.com/threat-intelligence/malware/default.aspx?id=3401935
http://www.mcafee.com/threat-intelligence/malware/default.aspx?id=3514120
http://www.mcafee.com/threat-intelligence/malware/default.aspx?id=142697

The minimum DAT versions required for detection are:

Detection Name	DAT Version	Date
VBS/Autorun.worm.aadd	7112	06/20/2013
VBS/Autorun.worm.aadd!lnk	7189	09/05/2013
VBS/Autorun.worm.aapa	7181	08/28/2013
VBS/Autorun.worm.aapb	7182	08/29/2013
VBS/Autorun.worm.aapc	7190	09/06/2013
VBS/Autorun.worm.aapd	7190	09/06/2013
VBS/Autorun.worm.aafs	7140	07/18/2013
VBS/Autorun.worm.aafv	7148	07/26/2013
VBS/Autorun.worm.k	5074	07/13/2007

The Threat Intelligence Library contains the date that the above signatures were most recently updated.

Please review the Threat Library for the most up to date coverage information.

Infection and Propagation Vectors

VBS/Autorun.worm is detection for malicious Visual Basic script (VBS) files encrypted with a commercial encryptor that uses base64 encoding to obfuscate the files.

The following variants of VBS/Autorun.worm were seen in the wild:

- VBS/Autorun.worm.aadd
- VBS/Autorun.worm.aadd!lnk
- VBS/Autorun.worm.aapa
- VBS/Autorun.worm.aapb
- VBS/Autorun.worm.aapc
- VBS/Autorun.worm.aapd
- VBS/Autorun.worm.aafs
- VBS/Autorun.worm.aafv
- VBS/Autorun.worm.k

All of them perform the same activity by connecting to the site and port number mentioned in the de-obfuscated code and copies itself to the removable drives. Although they perform similar activities they appear in different types.

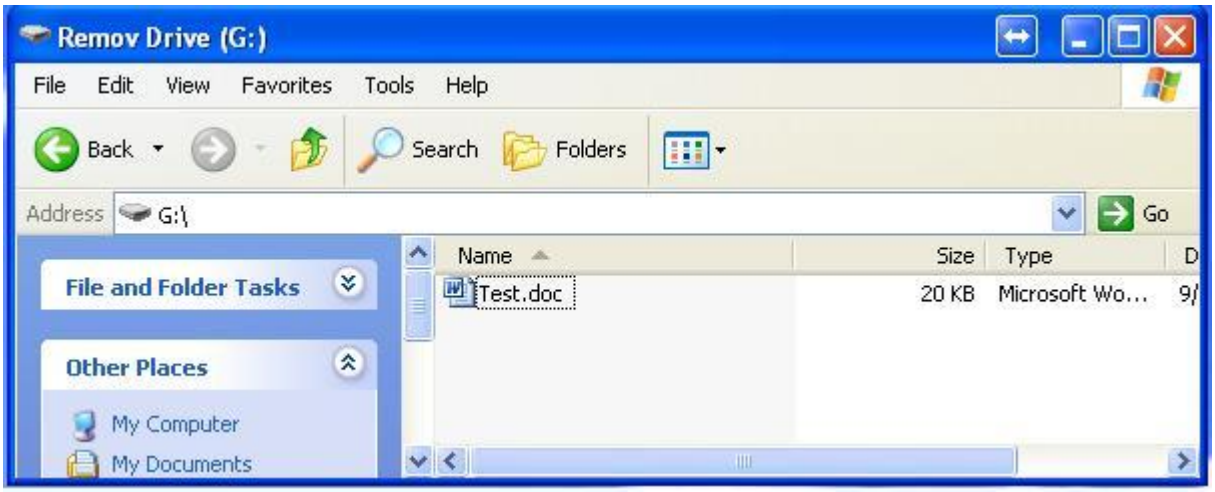
- Type 1: Comes in as a plain un-obfuscated VB scripts.
- Type 2. Base64 encrypted scripts.
- Type 3. Encrypted strings and decoded with char(charcode), charW(charcode) method type scripts.

This VBScript worm spreads via removable storage devices, such as floppy disk drives or a USB flash drives.

It checks the user computer for removable drives. Upon finding the removable drive is the worm copies itself into it. It creates several link (.lnk) files that run the VBScript worm.

The .lnk file is named using the file names already available on the removable drive, and hides the original clean file.

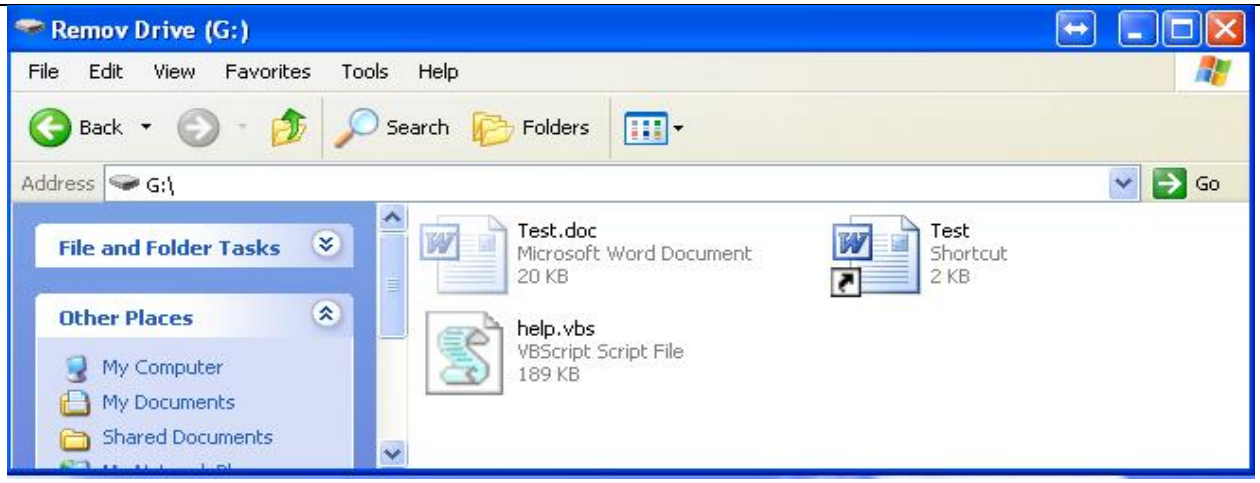
The following diagram illustrates the same:



If there is a file called **Test.doc** on the removable device, the worm creates a file called **Test.lnk.** This .lnk file redirects to a VBScript file that installs another copy of itself on the removable drive. The worm then changes the attributes of the **Test.doc** file to "hidden" and "system" to hide the legitimate file. It does this to encourage user to click on the .lnk file and run the worm.

In this example the removable drive would look like this before infection:

After infection:



The Test.lnk file would contain the following commands:

```
C:\WINDOWS\system32\cmd.exe /c start help.vbs&start Test.docx & exit
```

Characteristics and Symptoms

Description
VBS/Autorun.worm is a worm that spreads through removable drives. It allows backdoor access and control of user computer by a remote attacker.

Upon execution, this VBScript worm creates a copy of itself in either %TEMP% or %APPDATA% folder with a random file name as shown below:

- %Temp%\Servieca.vbs
- %AppData%\oguscovbpx.vbs

The worm also copies itself in the startup folder

- %UserProfile%\Start Menu\Programs\Startup\Servieca.vbs

It creates the following registry key as an infection marker

- HKEY_LOCAL_MACHINE\software\Filename

The following one of the registry value has been added to the system

- HKEY_CURRENT_USER\S-1-[varies]\
  njq8 = "n"

- HKEY_LOCAL_MACHINE \SOFTWARE\FileName\
  = "false – Date of Execution"

This worm connects a C&C server using a HTTP POST command.

It sends the following information about user computer to the server:

- Disk volume serial number
- Computer name
- User name
- Operating system information, Example, the name and version
- Installed Antivirus software details

Once it receives information about user computer the C&C server replies to the worm with instructions on what to do next. The commands may be any of the following:

- Run a command in the system
- Download and run a file, including other malware
- Update the worm
- Remove the worm after an update or after other malware is run

It can run the following commands from the attacker:

- exec - Download and run additional code
- uns - Uninstall itself

The following are some of the C&C servers observed after infection:

- man222.no-ip.biz
- sytes.net
- bifrost-jordan.zapto.org
- msgbox.zapto.org
- sidisalim.myvnc.com
- ouhiba.zapto.org
- pato2007.no-ip.biz
- khdt1.zapto.org
- adolf2013.sytes.net
- daddy.sytes.net
- mda.no-ip.org
- games.servecounterstrike.com
- hackk-hackk.zapto.org
- bagdad.no-ip.info
- boffon.no-ip.biz
- gerssy.zapto.org
- jamawaranti.no-ip.biz
- moussaab.no-ip.biz

The following are the observed C&C server TCP ports where the worm connected to:

- Port 846
- Port 55
- Port 555
- Port 5246
- Port 1888
- Port 288
- Port 2222
- Port 1184
- Port 81
- Port 88
- Port 1515

Notes

- %UserProfile% - C:\Documents and Settings\[UserName]
- %Temp% - C:\Documents and Settings\[UserName]\Local Settings\Temp
- %AppData% - C:\Documents and Settings\[UserName]\Application Data

Static reversing

The commercial encryptor used in this script is **Safa Crypter**.

Latest variants come with multiple level of obfuscation, with fully encrypted top level as shown in Fig 1.

Encrypted file:

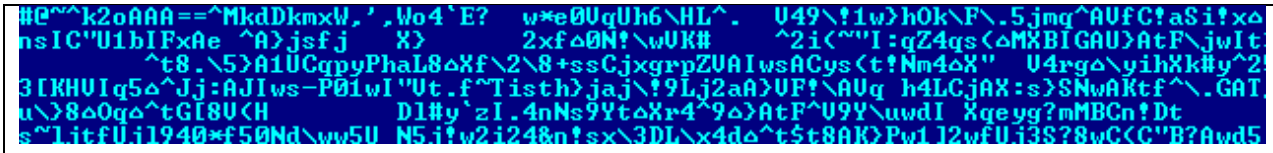
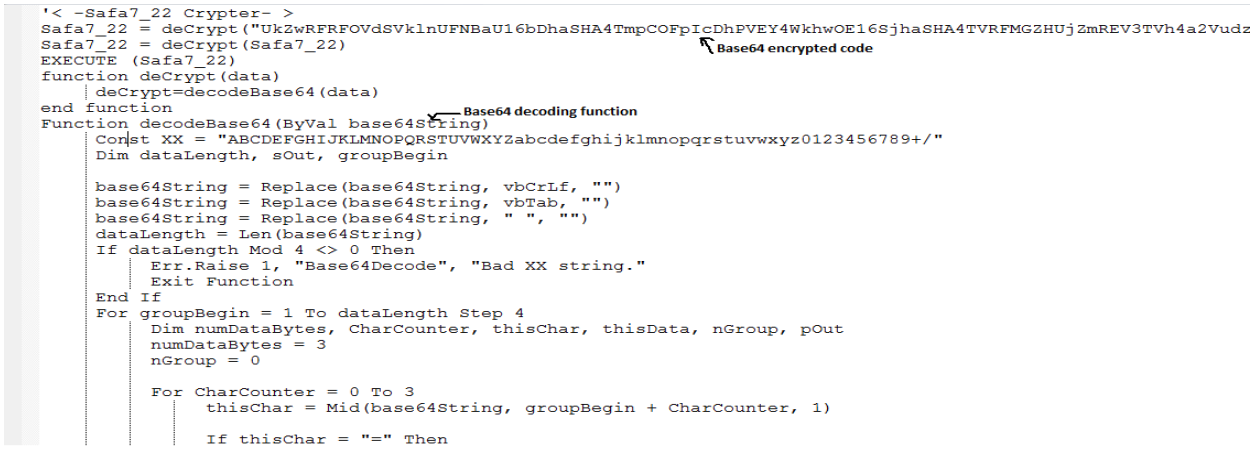


Fig 1.

On unpacking the sample we can see base64 encrypted strings as shown in fig 2. It is encrypted using Safa Crypter. It contains a Base64 decrypted function to decrypt base64 encrypted string. This sample has 2 levels of base64 encryption.




```
'< -Safa7_22 Crypter- >
Safa7_22 = deCrypt("UkZwRFRFOVdSVklnUFNBaU16bDhaSHA4TmpCOFpIcDhPVEY4WkhwOE16SjhaSHA4TVRFMGZHUjZmREV3TVh4a2Vudz
Safa7_22 = deCrypt(Safa7_22)
EXECUTE (Safa7_22)
function deCrypt(data)
    deCrypt=decodeBase64(data)
end function
Function decodeBase64(ByVal base64String)
    Const XX = "ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/"
    Dim dataLength, sOut, groupBegin

    base64String = Replace(base64String, vbCrLf, "")
    base64String = Replace(base64String, vbTab, "")
    base64String = Replace(base64String, " ", "")
    dataLength = Len(base64String)
    If dataLength Mod 4 <> 0 Then
        Err.Raise 1, "Base64Decode", "Bad XX string."
        Exit Function
    End If
    For groupBegin = 1 To dataLength Step 4
        Dim numDataBytes, CharCounter, thisChar, thisData, nGroup, pOut
        numDataBytes = 3
        nGroup = 0

        For CharCounter = 0 To 3
            thisChar = Mid(base64String, groupBegin + CharCounter, 1)

            If thisChar = "=" Then
```

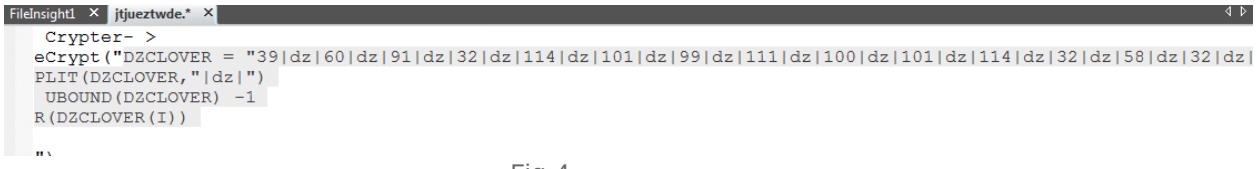
Fig2.

On decoding the base64 string we get the following output in fig 3. This is only the completion of first level.

```
'< -Safa7_22 Crypter- >
Safa7_22 = deCrypt("RFpDTE9WRVIgPSAiMzl8ZHp8NjB8ZHp8OTF8ZHp8MzJ8ZHp8MTE0fGR6fDEwMXxkenw5OXxkenwxMTF8ZHp8MTAwfG
Safa7_22 = deCrypt(Safa7_22)
EXECUTE (Safa7_22)
function deCrypt(data)
    deCrypt=decodeBase64(data)
end function
```

Fig 3.

ase64 decoding is repeated again to decrypt second level encryption .The result is as shown below in fig 4.



```
FileInsight1 ×  jtjueztwde.* ×
 Crypter- >
eCrypt("DZCLOVER = "39|dz|60|dz|91|dz|32|dz|114|dz|101|dz|99|dz|111|dz|100|dz|101|dz|114|dz|32|dz|58|dz|32|dz|
PLIT(DZCLOVER,"|dz|")
 UBOUND(DZCLOVER) -1
R(DZCLOVER(I))

"
```

Fig 4.

The decrypted code has a function to convert the decimal to ASCII characters. Using decimal to ASCII convertor actual malicious code of VBS/Autorun.worm can be obtained as seen in fig 5.

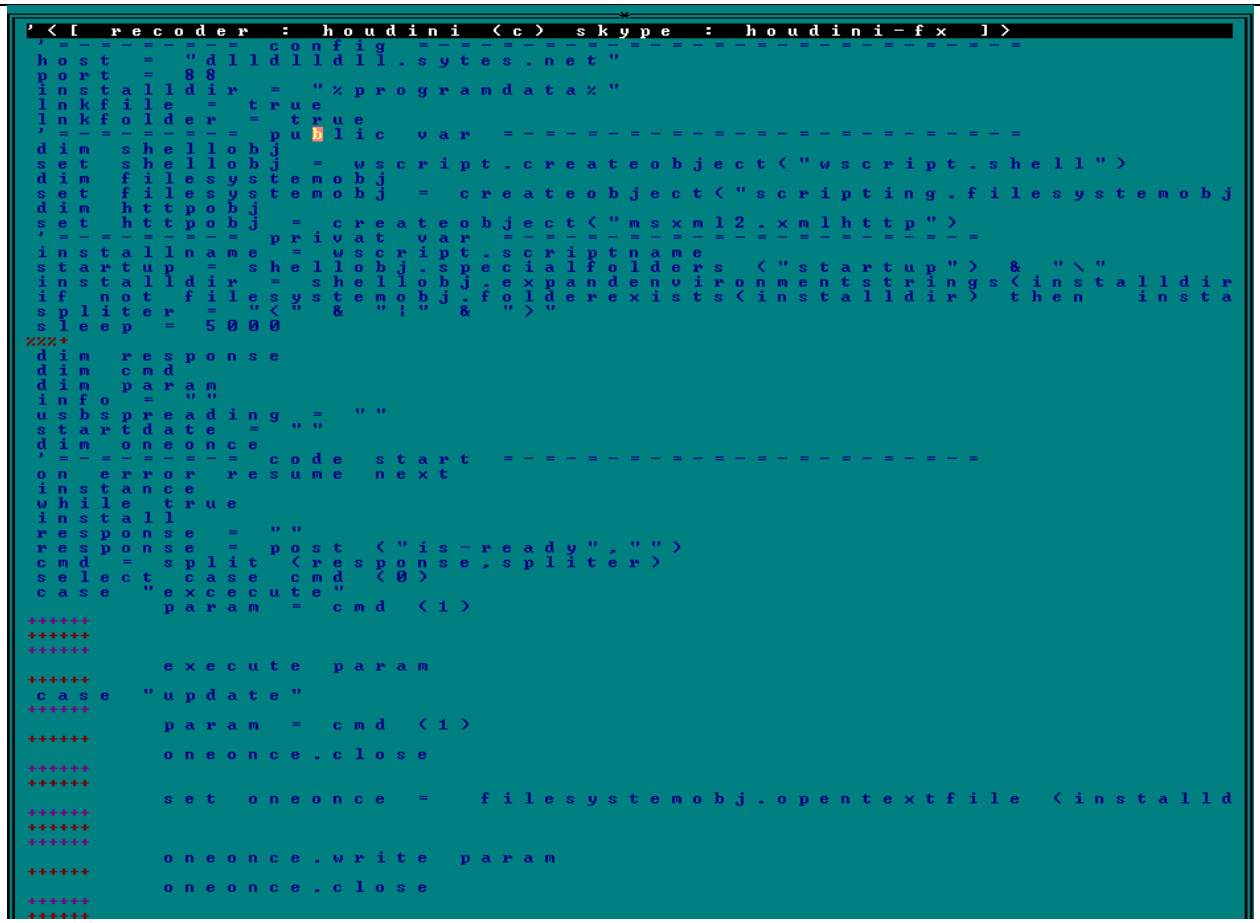


Fig 5.

Restart Mechanism

Description

The following registry entries would enable the worm to execute every time when Windows starts:

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\
  Servieca.vbs = "wscript.exe //B “%Temp%\Servieca.vbs""

- HKEY_CURRENT_USER\S-1-[varies]\Software\Microsoft\Windows\CurrentVersion\Run\
  Servieca.vbs = “wscript.exe //B "%Temp%\Servieca.vbs""

Mitigation

- Disable the Autorun feature on Windows. You can do this remotely using Windows Group Policies (http://support.microsoft.com/kb/967715).
- Restrict the use of USB drives in mission-critical and server machines.
- Implement and test Access Protection Rules through McAfee product to prevent writing of *.LNK files in removable media.
- Restrict access to the ports and monitor and block the above mentioned URLs.

Getting Help from the McAfee Foundstone Services team

This document is intended to provide a summary of current intelligence and best practices to ensure the highest level of protection from your McAfee security solution. The McAfee Foundstone Services team offers a full range of strategic and technical consulting services that can further help to ensure you identify security

risk and build effective solutions to remediate security vulnerabilities.

You can reach them here: https://secure.mcafee.com/apps/services/services-contact.aspx