WEBROOT

This solution addresses Webroot SecureAnywhere

Malware Prevention Guide

Use Reputable, Proven, Multi-Tenant Endpoint Security

We are often asked this leading question: "which endpoint security solution will offer 100% prevention and protection from malware?" The simple answer is none. Even the best endpoint security (which we pride ourselves on innovating and striving towards) will only be 100% effective most of the time.

For instance, real-time anti-phishing to stop email links to phishing sites, web browser protection to stop browser threats, and web reputation to block risky sites that might only occasionally be unsafe. Other changes can be made to the computer and environment to secure things further.

Cybercriminals are in the business of finding ways around endpoint security protection and their methods of attack will evolve in order to succeed. Each day, different malware campaigns create new variants of an infection. It is then repackaged or delivered in a way to remain undetectable by antivirus.

Back up your data.

If something like ransomware unfortunately succeeds and your data is affected, the most reliable protection is being able to restore that data and minimize business downtime. Backups that are tested and known to be working will always be vital to protecting an environment.

Please bear in mind: when planning your backup strategy, ransomware will also try to encrypt files on drives that are mapped, and some modern variants will look for unmapped drives too. Ransomware will look for external USB drives, as well as any network file stores that you have assigned a drive letter to.

Using a comprehensive, automatic backup solution, such as Carbonite Endpoint 360, for all your endpoint devices and the data that resides on them, including data in Microsoft O365 protects against accidental deletions, overwriting, ransomware and other threats.

You need to set up a regular backup regimen that, at a minimum, backs up data to an external drive, or backup service, that is completely disconnected when it is not performing the backup.

The recommended best practice is that your data and systems are backed up in at least three different places.

» Your main storage area (file server)
» Local disk backup
» Mirrors in a cloud business continuity service

In the event of a ransomware disaster, this set-up will give you the ability to mitigate any takeover of your data and almost immediately regain the full functionality of your critical IT systems.

User Education.

The "human firewall" – yours and other computer users – are often the weakest security link. A lot of lip service is paid to User Security Education, and with the advent of online self-paced courses there is no excuse not to look at using those tools to help educate your users of the risks they face in the office and from using the Internet at home.

We offer Webroot Security Awareness Training. This training helps educate users to recognize emails that are meant to steal info or cause harm.

If a user receives an invoice, receipt, or any other form of attachment from someone they are unfamiliar with, chances are it is bad. For word document emails, it is also advised to warn users to not click on "enable content" for emails and attachments from unfamiliar sources.

Webroot and Ransomware Payloads

As the impact and severity of crypto-ransomware threats and attacks has grown, we have published many blogs and articles on how best to defend against these modern day extortionists. We do not believe that our business or consumer customers should have to choose between extortion and losing precious, irreplaceable data.

When it comes to endpoint security, there are many choices out there. While published detection tests help when it comes to crypto-ransomware, most detection testing is flawed – with many programs achieving 100% detection results that can't be reproduced in the real world.

Webroot has built a strong reputation for stopping crypto-ransomware. Our goal, first and foremost, is to be 100% effective. Webroot was the first antivirus and antimalware vendor to move completely away from the standard, signature-based file detection method. By harnessing the power of cloud computing, Webroot replaced traditional, reactive antivirus with proactive, real-time endpoint monitoring and threat intelligence, defending each endpoint individually, while gathering, analyzing, and propagating threat data collectively. This predictive infection prevention model enables Webroot solutions to accurately categorize existing, modified, and new executable files and processes, at the point of execution, to determine their status.

Using this approach, Webroot rapidly identifies and blocks many more infections than signature-based approaches, and we are highly proficient at detecting and stopping crypto-ransomware.

The Webroot approach to preventing infection has continuously proven its efficacy at stopping crypto-malware in real time by addressing threats the moment they attempt to infect a device, stopping the encryption process before it starts.

Regardless of which endpoint security solution you choose, make sure that offers a multi-tenant and multi-layered approach against malware to ensure it quickly recognizes external threats and any suspicious behaviors. A next-generation endpoint security solution with protection beyond file-based threats is essential.

Restrict Remote Desktop access, secure weak usernames and passwords.

Cybercriminals constantly scan the internet for systems with commonly used remote desktop ports, then brute force them with weak usernames and passwords combinations to gain access. Once access has been gained, the intruder can disable protections, deploy variants of ransomware, create user accounts, and download other unwanted malicious software.

We recommend applying the steps below to help secure RDP and prevent this type of attack:

Preventing scanning for an open port:

- Restrict RDP to a whitelisted IP
- Require two-factor authentication, i.e. smartcards
- Use protection software to prevent RDP brute force
- Create a GPO to enforce strong password requirements: https://technet.microsoft.com/en-us/library/cc786468(v=ws.10).aspx
- Change the default RDP port from 3389 to another unused port

  To change the default port, execute the following in an elevated command prompt:

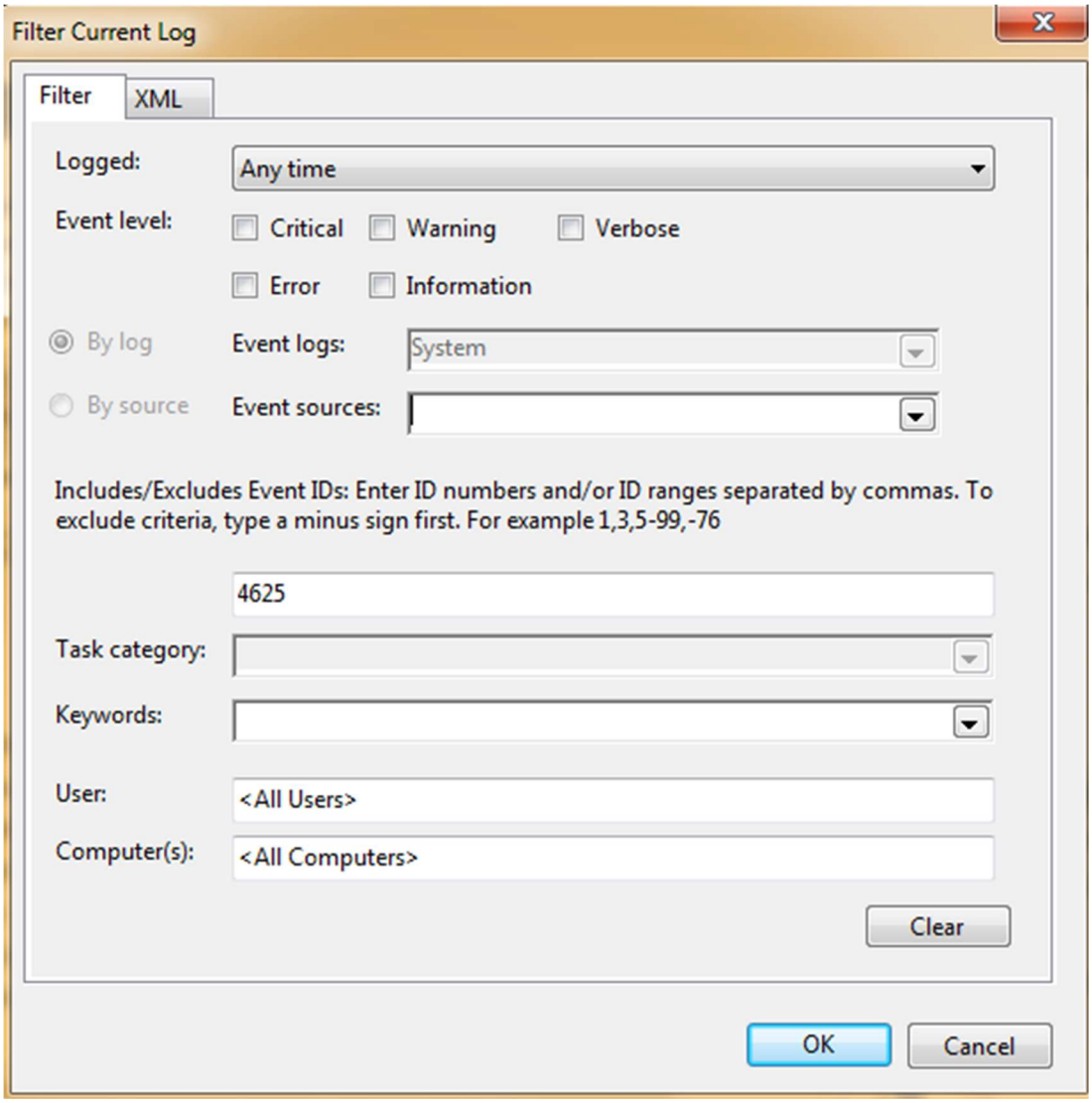
  ```
  REG ADD
  "HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\T
  erminal Server\WinStations\RDP-Tcp" /t REG_DWORD /v
  PortNumber /d XXXX /f
  ```

  The parameter “XXXX” is the port number you would like to move RDP to. It is recommended to choose a random port number that is not in use and outside of the 33XX port range.

- Block RDP entirely (port 3389) via firewall
- Restrict RDP to a whitelisted IP range

It is also important to monitor possible intrusions with Windows Event Viewer. This will show you what cybercriminals may be doing to try and get in, and help you adjust and use different security measures in your environment. Here’s an example to filter event logs for the event ID

“4625” (An account failed to log on):



Patch and keep software up to date.

Unpatched software is another common vulnerability. For example, ransomware like older exploits, such as, CryptXXX, Locky, and the newer exploit, Sodinokibi, were distributed via exploit kits. Exploit kits target software vulnerabilities of Adobe Flash Player, Oracle Java, Internet Explorer, Microsoft Silverlight and other vulnerable applications.

If unpatched software is exploited, an exploit kit landing page can execute arbitrary code and initiate a silent drive by download. It is critical for system administrators to keep this type of software up to date as most infections dropped by Exploit Kits are known as "zero days". Zero-

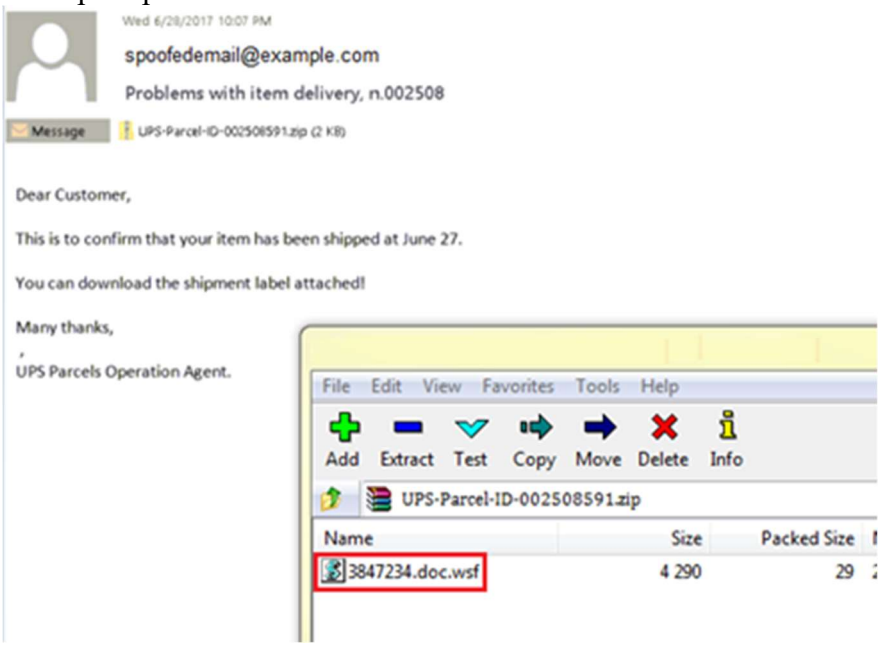
day threats are brand new and fully undetected by all antivirus until the threat is researched. If outdated software must be present in your environment, we recommend you download and install Microsoft's EMET to mitigate attacks. Download EMET

Disable execution of script files.

Webroot has discovered ransomware variants delivered through email attachments as well. These malicious attachments are often a zip archive that contain a script, which serves the purpose of downloading/executing a ransomware/malware payload.

Webroot recommends preventing the execution of script file types to avoid this type of attack.

Example Spam Email:



In order to prevent these types of documents and scripts from running, we recommend choosing the most appropriate solution for your environment from the section below.

Block WSF, VBS, WSH, HTA, VBS and JS files:

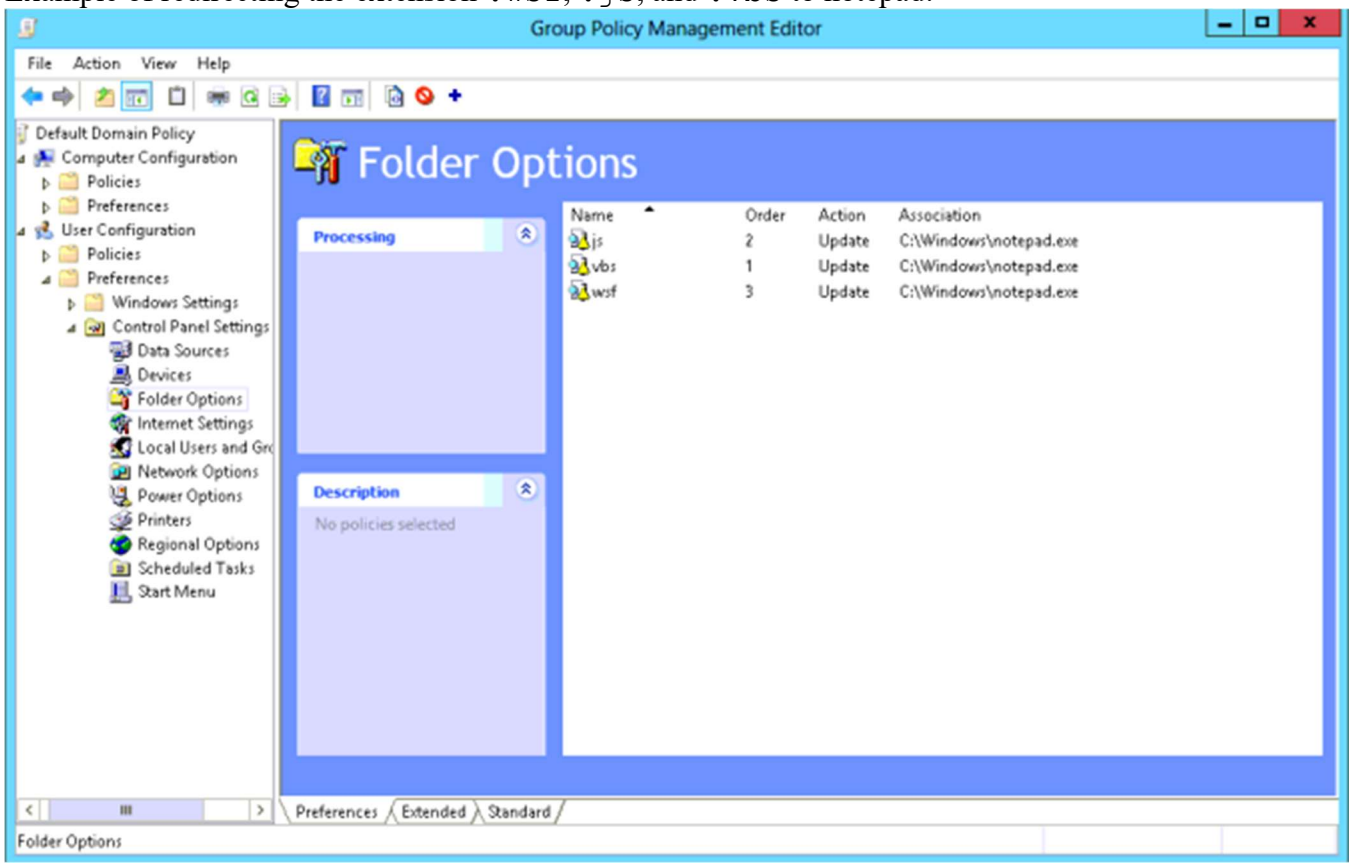
There are three options to prevent script files from running on a system.

Option 1: REDIRECT SCRIPT FILE EXTENSIONS VIA GPO

> To enable this policy setting, access the system set up for policy control and navigate to the following setting:
>
> **User Configuration - Preferences - Control Panel - Settings**
> Right-click on **Folder Options** and navigate to **New** > **Open With** .

Type in the each unwanted extension, i.e. `wsf, js, vbs` into the "File extension" box, then input the path of a program you want to have as default to open the file.
Tick **Set as default** and press **OK**.

Example of redirecting the extension `.wsf`, `.js`, and `.vbs` to notepad:



We recommend redirecting the file types: `.hta, .jse, .js, .vbs, .vbe, .wsf, .wsh, and .ps1.`

If a system administrator needs to run a `WSF`, `VBS`, `JS`, or any other script file, this can still be achieved by starting the WScript program with the script file as an argument.

For example:

```
:C:\Windows\System32\WSCRIPT.exe C:\example.vbs
```

Option 2: REDIRECT SCRIPT FILE EXTENSIONS VIA WEBROOT CONSOLE

If there is not a policy controller available, as an alternative, you can redirect file extensions with the utility below. By downloading the utility, you acknowledge that you agree to the https://download.webroot.com/UtilityEula.html

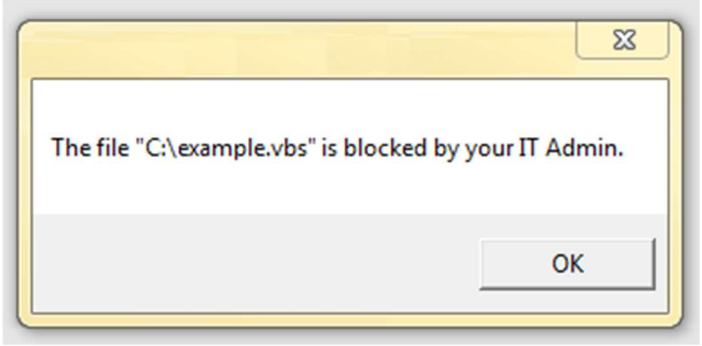
If you have an existing agreement with Webroot governing your use of this utility software, then such agreement will supersede the above terms and conditions in the event of any conflicting terms between the agreement and such terms and conditions.

1. Sign into the Webroot Enterprise Console and click **Group Management**.
2. Select the hostnames which you would like to have this applied to, and then navigate to **Agent Commands** > **Advanced** > **Customer Support Diagnostics**.
3. Input the following link into the URL field:

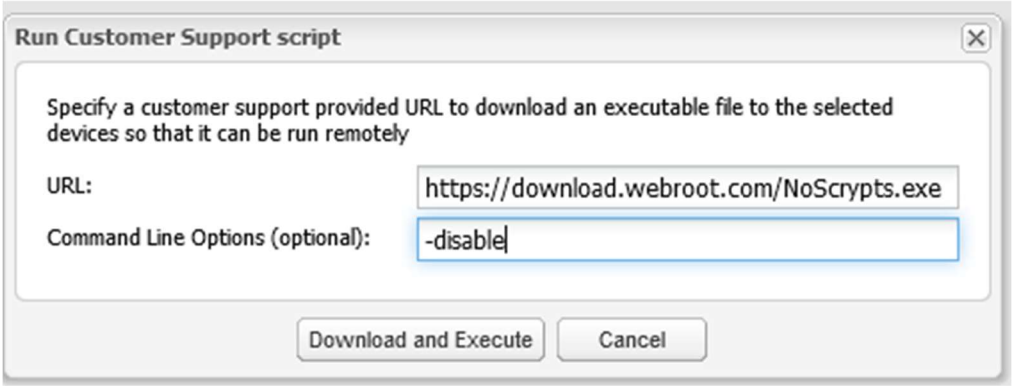
https://download.webroot.com/NoScrypts.exe

For the **Command Line Options** field, the following commands can be used:

`-disable` - This command will redirect the default action for the following file types: .hta, .jse, .js, .vbs, .vbe, .wsf, .wsh, to instead show a message box like so:

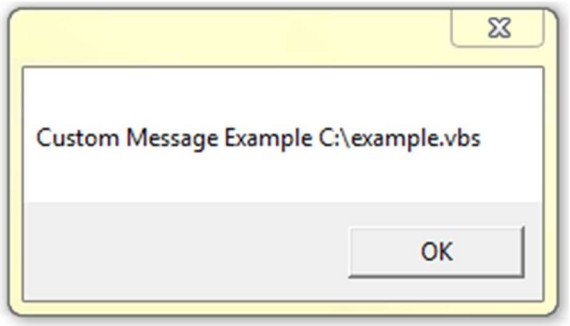


To apply this from the Webroot Endpoint Console, refer to the screenshot below:

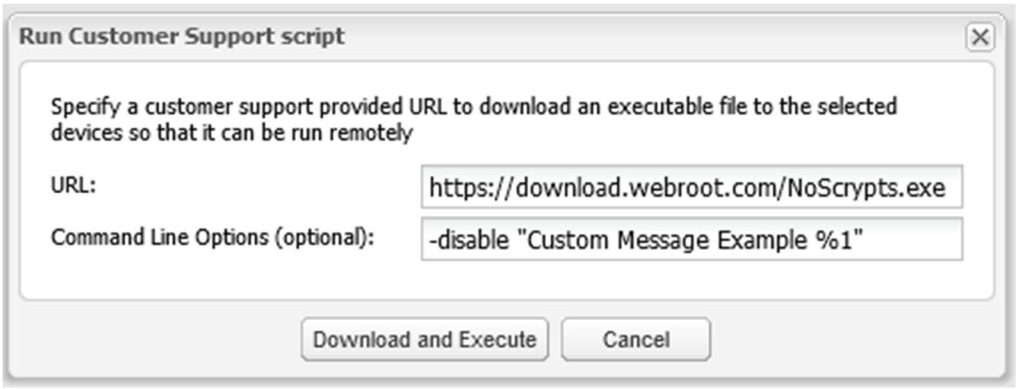


-disable “Custom Message” – This command will allow you to redirect the default action for the same file types, however it also allows you to

specify the message you would like the user to see. Where “”Custom Message”” is the message you would like to display to a user that opens a script file. Quotes are required around this text. Optionally you may include %1 in your custom message. This will show the file that was blocked like so:

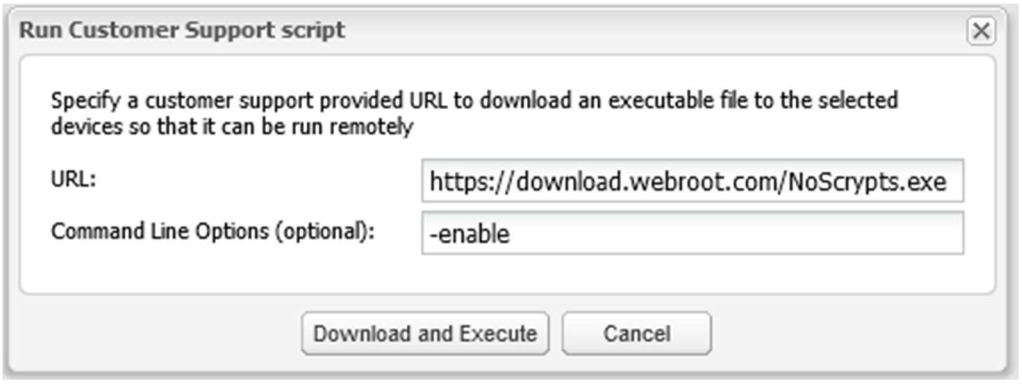


To apply this from the Webroot Endpoint Console, refer to the screenshot below:



`-enable` - This command restores the default execution program for the file types mentioned above.

To apply this from the Webroot Endpoint Console, refer to the screenshot below:



4. Click “Download and Execute” to send the command to the system.

Note: You may view the status of sent commands by choosing the “View commands for selected endpoints” option in the “Agent Commands” menu. Depending on poll interval, it may take up to 24 hours for the endpoint(s) to receive this command. You may force a poll check or configuration update to receive this command immediately by locating the Webroot icon in the system tray, right clicking it, and selecting “Refresh Configuration”.

5. Ensure script files are blocked by attempting to open a file with a blocked file type.

Option 3: DISABLE WSCRIPT HOST

WScript Host `(C:\Windows\System32\WSCRIPT.exe)` is an application within Windows that interprets `.vbs, .vbe, .js, .jse, .wsf` and other types of script files. When a script is run, it will execute the script through this program. Because of this, you may want to disable WScript Host entirely. To do so, use one of the following procedures. By downloading the utility, you acknowledge that you agree to the https://download.webroot.com/UtilityEula.html . If you have an existing agreement with Webroot governing your use of this utility software, then such agreement will supersede the above terms and conditions in the event of any conflicting terms between the agreement and such terms and conditions.

From the Webroot Console:

1. Sign into the Webroot Enterprise Console and click **Group Management**.
2. Select the hostnames that you would like to have this applied to, and then navigate to **Agent Commands > Advanced > Customer Support Diagnostics.**
3. Enter the following link into the URL field:
   https://download.webroot.com/DisableWSCRYPT.exe
4. For the **Command Line Options** field, the following commands can be used:

`-disable`
This command will disable WScript and disallow execution of script files.

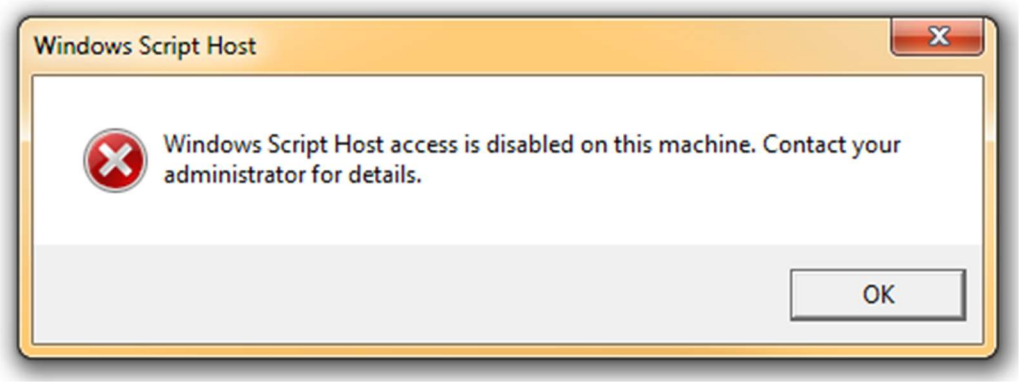
`-enable`
This command will enable WScript and allow execution of script files.

5. Click “Download and Execute” to send the command to the system.

Note: You may view the status of sent commands by choosing the “View commands for selected endpoints” option in the “Agent Commands” menu. Depending on poll interval, it may take up to 24 hours for the endpoint(s) to

receive this command. You may force a poll check or configuration update to receive this command immediately by locating the Webroot icon in the system tray, right clicking it, and selecting “Refresh Configuration”.

6. Ensure WScript is blocked by opening a command prompt, typing “WScript”, and pressing enter. You should be presented with the following message:



Manually - 64 BIT:

To disable Windows Script Host, execute the following in an elevated command prompt:

```
REG ADD "HKLM\Software\Microsoft\Windows Script
Host\Settings" /v Enabled /t REG_DWORD /d 0 /f
/reg:32

REG ADD "HKLM\Software\Microsoft\Windows Script
Host\Settings" /v Enabled /t REG_DWORD /d 0 /f
/reg:64
```

To re-enable Windows Script Host, execute the following:

```
REG ADD "HKLM\Software\Microsoft\Windows Script
Host\Settings" /v Enabled /t REG_DWORD /d 1 /f
/reg:32

REG ADD "HKLM\Software\Microsoft\Windows Script
Host\Settings" /v Enabled /t REG_DWORD /d 1 /f
/reg:64
```

Manually - 32 BIT:

To disable Windows Script Host, execute the following in an elevated command prompt:

```
REG ADD "HKLM\Software\Microsoft\Windows Script
Host\Settings" /v Enabled /t REG_DWORD /d 0 /f
```

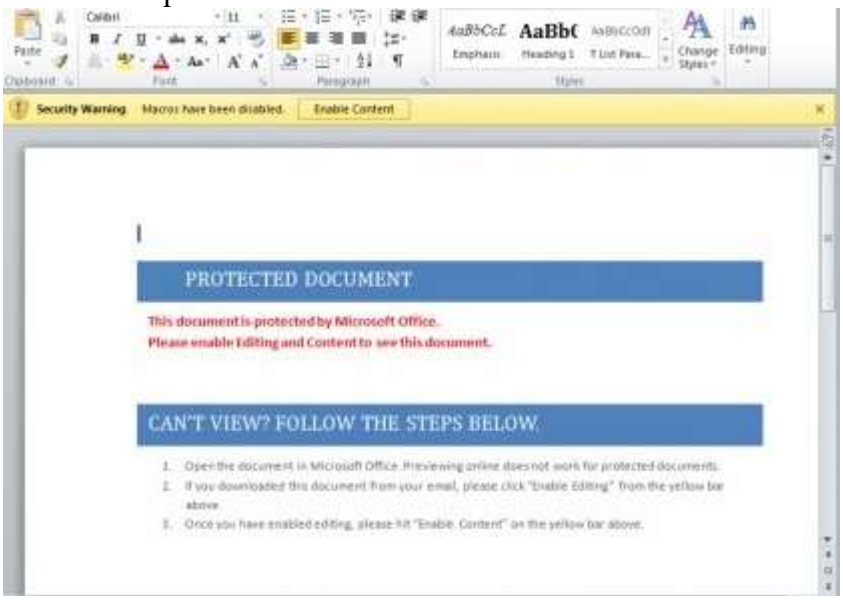
To re-enable Windows Script Host, execute the following:

```
REG ADD "HKLM\Software\Microsoft\Windows Script
Host\Settings" /v Enabled /t REG_DWORD /d 1 /f
```

Disable Macro execution.

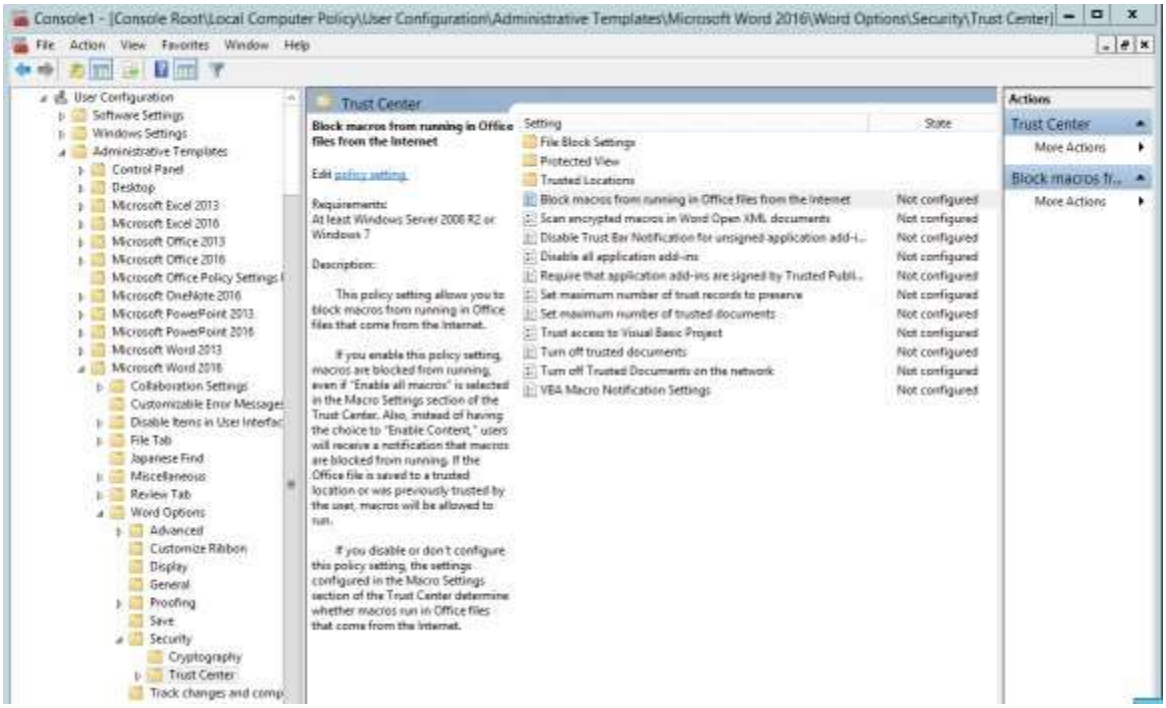
Office Macros can be beneficial to some work environments, however in most cases they are not necessary to have enabled and are only a security risk. Some ransomware may attempt to utilize macro scripts within documents as a vector for a malicious payload delivery.

Macro example:



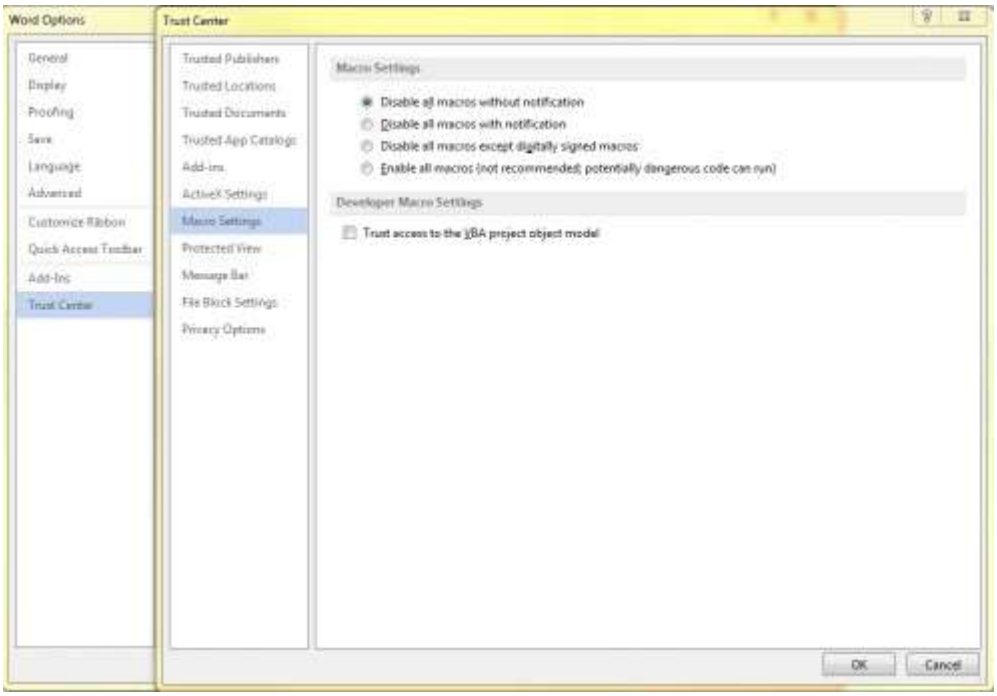
To enable this policy setting, Run gpedit.msc and navigate to the following setting:

User configuration > **Administrative templates** > **Microsoft Word 2016** > **Word options** > **Security** > **Trust Center**.
Double-click on **Block macros from running in Office files from the Internet setting** and **Enable** it.



Office 2013: https://technet.microsoft.com/en-us/library/ee857085.aspx

Note: If there is not a policy controller available, as an alternative you can disable macros without notification manually:



Prevent Users from running Powershell via GPO.

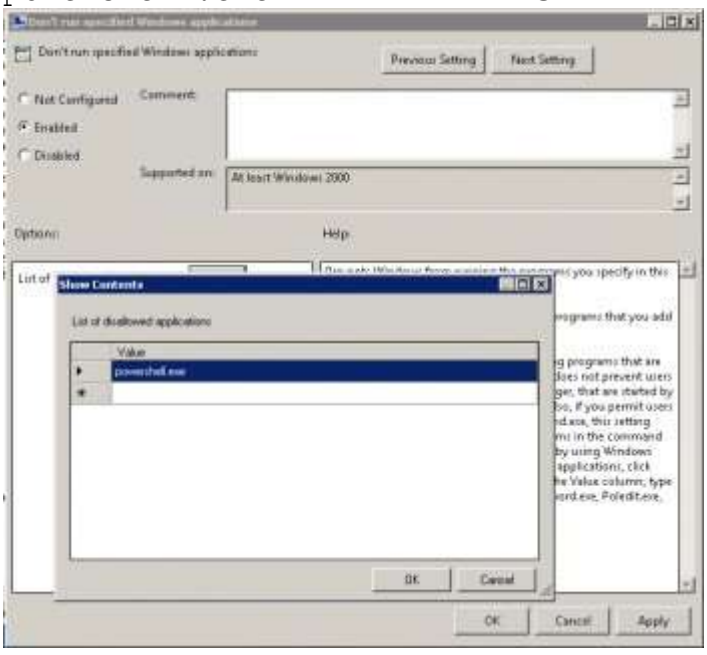
To enable this policy setting, Run gpedit.msc and navigate to the following setting:

User configuration > **Administrative templates** > **System**

1. Double-click on **Don't run specified Windows applications**.

2. Click the radio button **Enabled** to enable the policy.

3. Click the **Show** button next to **List of disallowed applications** and add `powershell.exe` to the list and click **OK**.



4. Test by attempting to run Powershell.