WEBROOT®
Smarter Cybersecurity™

MSP Guide: Stopping Crypto Ransomware Infections in SMBs

16 Easy Actions for MSPs

Introduction and Background

As the impact and severity of crypto ransomware threats and attacks has grown over the past 2½ years, Webroot has published many blogs and articles on how best to defend against these modern day extortionists. Webroot does not believe that businesses or consumers should have to choose between extortion and losing precious, irreplaceable data.

A question often asked: which endpoint security solution will offer 100% prevention and protection from crypto ransomware? The simple answer is none. Even the best endpoint security will only be 100% effective most of the time. At other times, cybercriminals will have found a way to circumvent endpoint security defenses and the attacks will succeed.

As an endpoint security provider, Webroot cannot stand on the sidelines when, even with Webroot's highly effective endpoint security, users could still get infected, especially when other key mitigation strategies like protected backups will help users be really secure.

Webroot has hosted many webinars on crypto ransomware. These webinars regularly generate a large volume of questions, so this guide has been issued to help prevent partners and other organizations from becoming crypto ransomware victims.

This paper explores over 15 ways to secure SMBs from crypto ransomware attacks to more completely secure IT environments from crypto ransomware and its consequences. Regardless of business size, and even with a modest outlay, highly damaging threats can be mitigated.

This guide intends to point out some practical approaches to protecting SMBs from crypto ransomware. Some of these recommendations may not be suitable to certain IT environments. Take this guide with the small warning that some recommendations will cause certain programs not to install or function as expected.

On behalf of Webroot, we hope MSPs and other service providers will find this guide educational, useful, and valuable in protecting businesses from extortion.

Crypto Ransomware Mitigation Guide

This guide examines a number of mitigation strategies that help protect organizations' data from crypto ransomware attacks.

Crypto ransomware writers have developed more sophisticated ways to infect endpoints, infections that go on to encrypt local, mapped, and unmapped drives in businesses networks. Crypto ransomware is no longer an annoyance. It's a highly persistent and organized criminal activity in full deployment with Ransomware as a Service (RaaS) at its core.

The damage from becoming a victim of crypto ransomware and not having adequate safeguards and mitigation strategies in place is considerable – life-threatening in the case of a recent LA hospital breach. For smaller businesses, such an attack could put them out of business.

1. Use Reputable, Proven, Multi-Vector Endpoint Security

There are a huge number of options when it comes to endpoint security. While published detection tests can indicate whether a solution can stop crypto ransomware, most detection testing is flawed – with many programs achieving 100% detection results that can't be reproduced in the wild.

Webroot has built a strong reputation for stopping crypto ransomware. The 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 is highly proficient at detecting and stopping crypto ransomware.

SMBs need protection that covers multiple threat vectors. For instance, organizations need 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.

Over the past four years, the Webroot approach to infection prevention has continuously proven its efficacy at stopping ransomware in real time by addressing threats the moment they attempt to infect a device, stopping the encryption process before it starts. Today, Webroot is probably the only endpoint security vendor that delivers proven endpoint malware prevention at scale. Because of this, it is fast becoming the solution of choice to conventional endpoint antivirus solutions.

Regardless of the solution, it's essential the security offers multi-dimensional protection and prevention 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.

2. Put Strong Backup Practices in Place

Even service providers and administrators running next-generation endpoint security can still fall victim to crypto ransomware infections. When infections do get through, organizations need a strong backup and business continuity plan to be able to restore data and minimize business downtime.

What some organizations fail to recognize in their backup strategy is that some crypto ransomware like CryptoLocker will encrypt not only local drives, but also encrypt files on any mapped drives. Some modern variants will look for unmapped drives, external drives such as a USB thumb drives, and any network or cloud file stores that have been assigned a drive letter. Organizations 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 not performing the backup.

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

- Main storage area (file server)
- Local disk backup
- Mirrors in a cloud business continuity service

In the event of a ransomware disaster, this setup will give administrators the ability to mitigate any takeover of data and almost immediately regain the full functionality of critical IT systems. With all of the disastrous outcomes of not having a mature business continuity and disaster recovery plan in place, it is wise for MSPs and business owners to take a deep look into their systems and invest in available solutions.

Crypto ransomware especially punishes businesses that don't regularly back up their data, which is something that should be at the core of any IT infrastructure. Since backup and recovery services have become so affordable, there's no reason for a business not to have a robust plan in place

3. General Protection Tips

These tips are used to protect IT environments and thwart crypto ransomware threats and attacks.

3.1. Make sure that endpoint security is installed and set up correctly.

It is worth checking that the appropriate protection policies are active and applied to the correct user groups or however policies are allocated.

3.2. Check regularly that backups are working.

It's vital to check that backups are working and that data integrity is maintained and data is easily restored to the host.

3.3. Ensure the latest Windows updates are applied.

A number of infections are instantly ruled out if Windows is up to date. Reduce workload by putting in place a patching routine. This is a security fundamental.

3.4. Keep all plugins up to date.

Keeping all third party plug-ins updated to their latest build is an important counter to exploits. Make this part of the patch management regime.

3.5. Use a modern browser with an ad blocking plugin.

Modern browsers like Chrome and Firefox are constantly being updated to remove vulnerabilities. They also give the option to add BHOs or plug-ins that will make users more secure. At the most basic level, simply having a pop-up blocker installed and running can save a lot of users from getting infected.

3.6. Disable autorun.

Autorun is a useful feature, but it is used by malware to propagate itself around a corporate environment. With the growth of USB sticks, malware increasingly uses autorun as a means of proliferation. Commonly used by Visual Basic Script (VBS) malware and worms, it is best to disable it as a Policy.

3.7. Disable Windows Scripting Host.

VBS are Microsoft scripts used by malware authors to either cause disruption in an environment or to run a process that will download more advanced malware. Disable them completely by disabling the Windows Scripting Host engine that VBS files use to run.

3.8. Have users run as limited users and NOT admins.

This is highly desirable from a security perspective but not always possible for power users. This tip is important because some current ransomware threats are capable of browsing and encrypting data on any mapped drives that the end user has access to. Restricting the user permissions for the share or the underlying file system of a mapped drive will provide limits to what the threat has the ability to encrypt.

3.9. Show hidden file extensions.

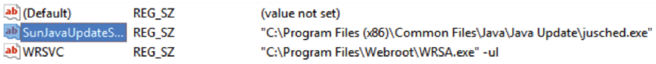
One way ransomware like CryptoLocker and others frequently arrive is in a file named with the extension ".PDF.EXE" or something similar. The malware writer counts on the default Windows behavior of hiding known file extensions. If full file extensions are visible, it is easier to spot suspicious files.

4. Creating Windows Policies to Defend Against Ransomware

When it comes to crypto ransomware, some Windows Policies need to be created to block certain paths and file extensions from running.

Java is generally the most popular way to exploit software, but these rules apply to nearly all commonly used plugins. Generally speaking, if users do not intend on using certain plugins, it is better not to have them installed.

If plugins are being used, then make sure they are up to date, i.e. do not disable the run keys for the Java updaters, etc.



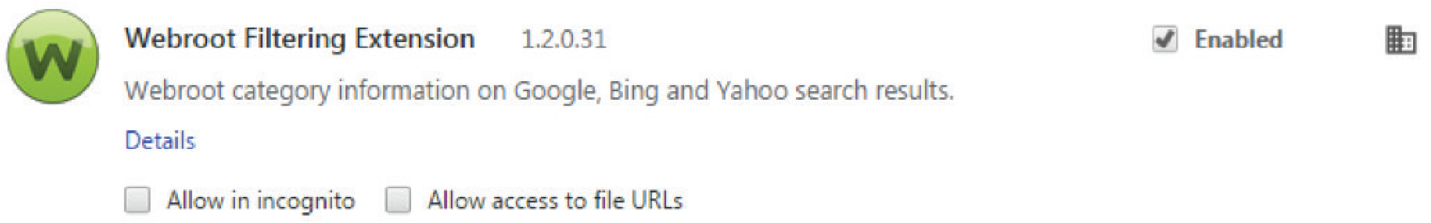
```
(Default)          REG_SZ          (value not set)
SunJavaUpdateS...  REG_SZ          "C:\Program Files (x86)\Common Files\Java\Java Update\jusched.exe"
WRSVC              REG_SZ          "C:\Program Files\Webroot\WRSA.exe" -ul
```

Example of a Java Updater Service

Common Paths

This guide talks about paths and file types, so here is a brief introduction. Malware generally drops into a few common paths. Once there, it is free to move around within the PC (and network paths).

- Common paths for malware to drop into are:
- User temp folders (often called %localusertemp%)
- Appdata and its sub folders (roaming, local app data)
- User profiles
- Temp folder (%temp% or C:\Windows\temp)
- Browser cache folders (%cache path depends on browser used see below for an example)
- c:\users\admin\appdata\local\microsoft\windows\temporary internet files\content.ie5\
- Desktop folder



Webroot Filtering Extension 1.2.0.31 ☑ Enabled

Webroot category information on Google, Bing and Yahoo search results.

Details

☐ Allow in incognito ☐ Allow access to file URLs

Webroot Filtering Extension in Chrome

To go to any of the paths with the % sign, just type the full phrase into a run window or windows start search. For instance, typing "%temp%" will go directly to "C:\Users\admin\AppData\Local\Temp"

Once any infection is on a PC and actively running, it can move itself around and become more difficult to find, or move to a location that will help it spread. More sophisticated malware can spread to network paths. It can use a registry entry to "autostart" or other methods like "scheduled task service," etc.

» C:\program data\ (this is a hidden folder by default)

» C:\Windows

» C:\Windows\System32

» C:\Recylcer\ (hidden folder, recycle bin)

» Root of the c:\

» C:\Program files\ (both 32,64bit paths, common location for PUA's)

Malware will often use well-known names or Windows system names to try to throw off the user. For example, Winlogon.exe is a core component of Windows and is located at: c:\windows\system32\winlogon.exe and is around 450 kb in size.

If administrators see a WinLogon.exe file in a user's temp folder that is twice that size, it should be a red flag and the file should be examined! Antimalware usually takes care of this, however administrators should take action beyond simply deploying antimalware. The following sections show administrators how to use policies to restrict access to certain file types and paths.

The more restrictive the policies are, the better. However, these changes can lead to certain programs not functioning.

5. Choosing a Second Browser

It's advisable to have a second browser installed on endpoints for a number of reasons:

5.1. If the only browser gets damaged it can make connecting remotely difficult. Not everybody uses RDP. In fact, Webroot recommends disabling it.

5.2. PUAs or malware can reduce the speed of browsers until they become unstable and unusable.

5.3. Some sites may not render correctly on old versions of IE. Firefox and Chrome can be used to test if this is the case.

5.4. Older versions of Windows do not have the ability to install newer versions of IE.

5.5. Newer browsers can use plugins.

There are dozens of browsers available, but Chrome and Firefox are the two most popular browsers on the market at the moment. Another useful function of both Chrome and Firefox is the ability to use plugins.

Useful Browser Plug-in Types:

» Ad blockers

» Script blockers

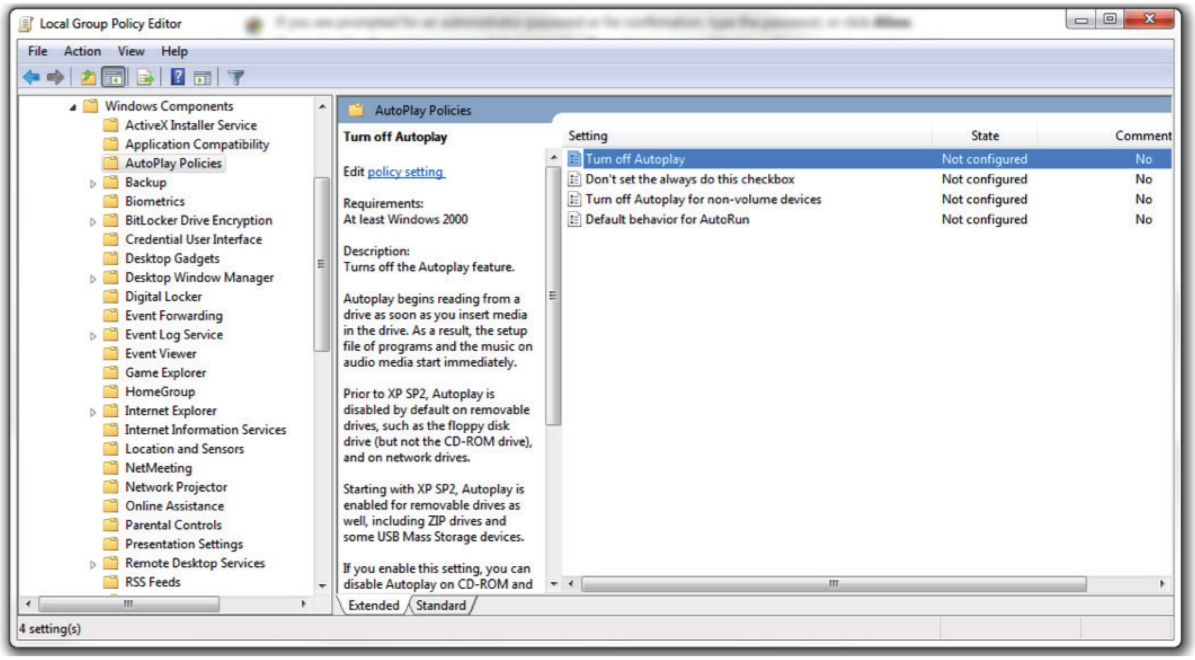
» Web filters

While many websites need advertisements to stay online, more and more popular websites (i.e. millions of visitors a year) infect users due to 3rd party hosted advertisements on their websites – malvertising. Just recently (March 2016) some very reputable news sites with US hosting were hijacked and served malvertising to visitors for almost all of a Sunday. Ad blocker plugins can be installed and left without any user input and are very useful for protecting more naïve users.

Script blockers stop Java scripts from running on websites unless they have specifically been allowed. These require a bit more knowledge and aren't recommended for less technical users. Many websites use Flash and Java plugins, and administrators that disable Java can expect additional support tickets and calls.

Web filters are very commonly installed by antivirus products and can act as a first line of defense against threats. They can scan websites before the user gets a chance to see them, stopping threats from executing.

The Webroot filter checks website reputations and will alert the user if they are visiting a site that is unsafe.



Turn off Autoplay

Edit policy setting

Requirements:
At least Windows 2000

Description:
Turns off the Autoplay feature.

Autoplay begins reading from a drive as soon as you insert media in the drive. As a result, the setup file of programs and the music on audio media start immediately.

Prior to XP SP2, Autoplay is disabled by default on removable drives, such as the floppy disk drive (but not the CD-ROM drive), and on network drives.

Starting with XP SP2, Autoplay is enabled for removable drives as well, including ZIP drives and some USB Mass Storage devices.

If you enable this setting, you can disable Autoplay on CD-ROM and

Setting	State	Comment
Turn off Autoplay	Not configured	No
Don't set the always do this checkbox	Not configured	No
Turn off Autoplay for non-volume devices	Not configured	No
Default behavior for AutoRun	Not configured	No

Turning off Autoplay

6. Disabling Autorun

While autorun is a useful feature, malware uses it to spread around corporate environments. Autorun can be disabled by using the Local Group Policy Editor.

(**Note** – this doesn't affect the functionality of USB drives.)

1. Click the **Start** and type **gpedit.msc** and then hit **Enter**.

2. Under **Computer Configuration**, expand **Administrative Templates**, expand **Windows Components**, and then click **Autoplay Policies**.

3. In the **Details** pane, double-click Turn off Autoplay.

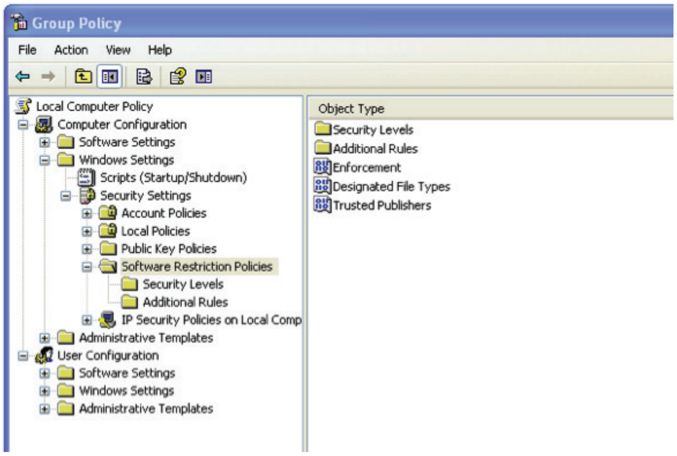
4. Click **Enabled**, and then select **all drives** in the **Turn off Autoplay** box to disable autorun on all drives.

7. Using the Policy Editor to Block Paths

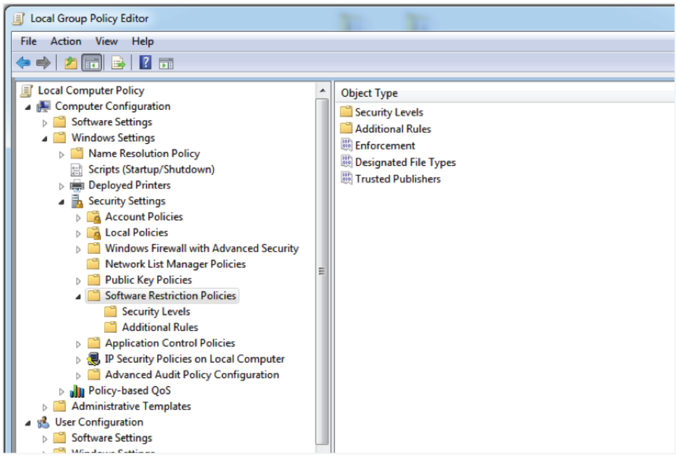
Policies are a powerful tool that have a multitude of purposes. They commonly stop users from opening or installing certain software, but they can be creatively used as well. The example below uses local policies, but the same principles apply to network group polices. This guide is only a very brief introduction, so explore this link from Microsoft for more information: https://technet.microsoft.com/en-us/library/bb457006.aspx

Policies can be set up in groups so there are more or less strict policies for certain groups. This can be useful for administrators who serve clients with varying levels of expertise.

Please note: It is advised that any policies be tested on a test PC that is not mission-critical!



Accessing Group Policy



Local Group Policy Editor

Examples of useful policies:

- Block the opening of executables in temp
- Block the modification of the VSS service
- Block the opening of executables in temp+appdata
- Block the creation of startup entries

The following file types shouldn't be run in the following directories:

- .SCR,.PIF,CPL in the users temp, program data, or desktop

The previously stated policy would be reasonably safe. Crypto ransomware does sometimes use the .SCR file format, which is a portable executable (PE) that is sometimes forgotten. A further step could be taken by creating a policy that blocks PE file formats from common paths where malware droppers are commonly located.

- .EXE, .DLL, .SYS, .FON, .EFI, .OCX, and .SCR
- Temp, Appdata, ProgramData, etc.

The Local Group Policy Editor can be opened by running the following process. To open the Local Group Policy Editor from the command line:

Click **Start**, type msc in the **Start Search** box, and then press Enter.

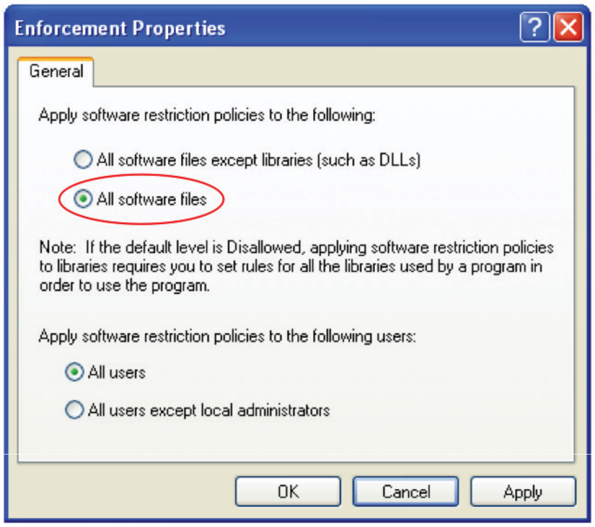
To open the Local Group Policy Editor as an MMC snap-in:

1. Click **Start**, click in the **Start Search box**, type mmc, and then press **Enter**.
2. On the **File** menu, click **Add/Remove Snap-in**.
3. In the **Add or Remove Snap-ins** dialog box, click **Group Policy Object Editor**, and then click **Add**.
4. In the **Select Group Policy Object** dialog box, click **Browse**.
5. Click **This Computer** to edit the Local Group Policy Object, or click **Users** to edit Administrator, Non-Administrator, or per-user Local Group Policy objects.
6. Click **Finish**.

8. Testing Out a Policy

To create a policy, expand the tree to get to the following:

- Computer Configuration > Windows Settings > Security Settings > Software Restriction Policies



Enforcement Properties

General

Apply software restriction policies to the following:

○ All software files except libraries (such as DLLs)

● All software files

Note: If the default level is Disallowed, applying software restriction policies to libraries requires you to set rules for all the libraries used by a program in order to use the program.

Apply software restriction policies to the following users:

● All users

○ All users except local administrators

Modifying a Setting in Enforcement Properties

First modify a setting in Enforcement Properties. Change it from "All software files except libraries" to "All software files."

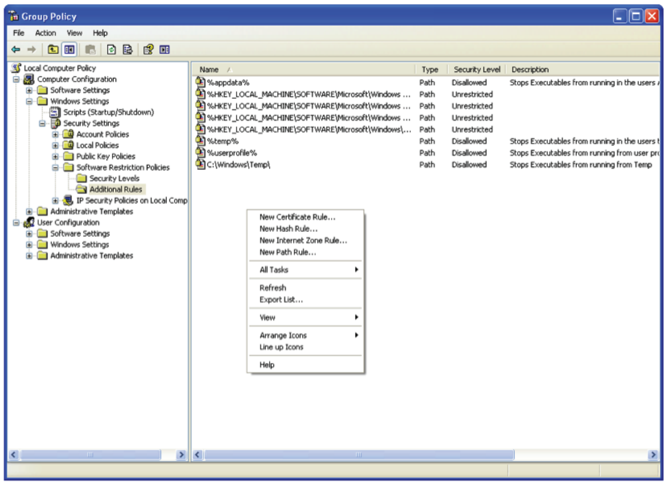
9. Creating a Policy

To create a policy, right click on the right hand side of the Policy window and select "New Path Rule."

Creating a Policy

This window can be used to browse to specific folders, or common Windows wildcard paths can be used. In the case below, a Policy has been created that will block executable files from launching from the following path:

C:\Windows\Temp



Group Policy

Name	Type	Security Level	Description
%appdata%	Path	Disallowed	Stops Executables from running in the users a
%HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows ...	Path	Unrestricted	
%HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows ...	Path	Unrestricted	
%HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows ...	Path	Unrestricted	
%HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\...	Path	Unrestricted	
%temp%	Path	Disallowed	Stops Executables from running in the users t
%userprofile%	Path	Disallowed	Stops Executables from running from user pr
C:\Windows\Temp\	Path	Disallowed	Stops Executables from running from Temp

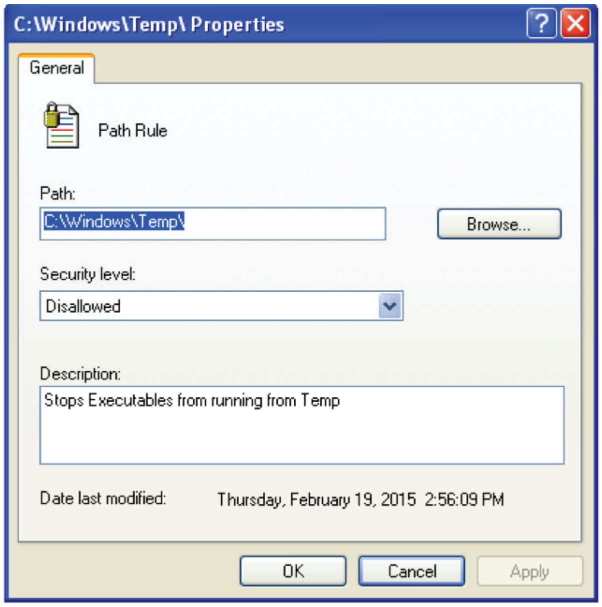
Creating a Policy

This is the Windows temp folder (used by a number of programs and installers) so it will probably cause some issues if implemented, but it's useful to demonstrate what can be done. Get creative with the paths defined (see screenshot 'Creating a Policy').

Please note: In the case above the user will not be able to run anything from their desktop!

1. %appdata%
2. %temp%
3. %userprofile%
4. %localappdata%
5. %programdata%
6. C:\Windows\Temp

It is worth noting that a number of legitimate programs and updaters also run from user appdata. If there is legitimate software that is set to run not from the usual Program Files area but from appdata, it will need to be excluded from the rules or it will NOT run.



C:\Windows\Temp\ Properties

General

Path Rule

Path: C:\Windows\Temp\

Security level: Disallowed

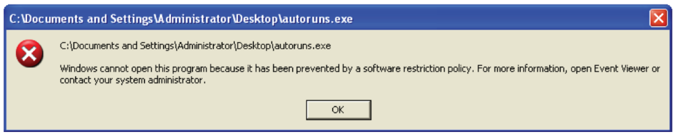
Description: Stops Executables from running from Temp

Date last modified: Thursday, February 19, 2015 2:56:09 PM

Stopping an Executable in Temp

The example below shows a few policies created to block executables from running within the following name/paths:

The screen shot below shows where an executable attempted to run on the local desktop. In this case, Windows automatically pop-ups an alert and the program doesn't run. If the file is moved to another path that doesn't have a restricted policy, the program will open without any issues.



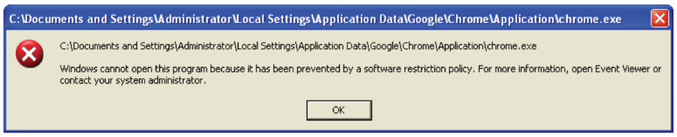
C:\Documents and Settings\Administrator\Desktop\autoruns.exe

C:\Documents and Settings\Administrator\Desktop\autoruns.exe

Windows cannot open this program because it has been prevented by a software restriction policy. For more information, open Event Viewer or contact your system administrator.

Executable Block Notice

10. Fixing Issues with Blocked Programs



C:\Documents and Settings\Administrator\Local Settings\Application Data\Google\Chrome\Application\chrome.exe

C:\Documents and Settings\Administrator\Local Settings\Application Data\Google\Chrome\Application\chrome.exe

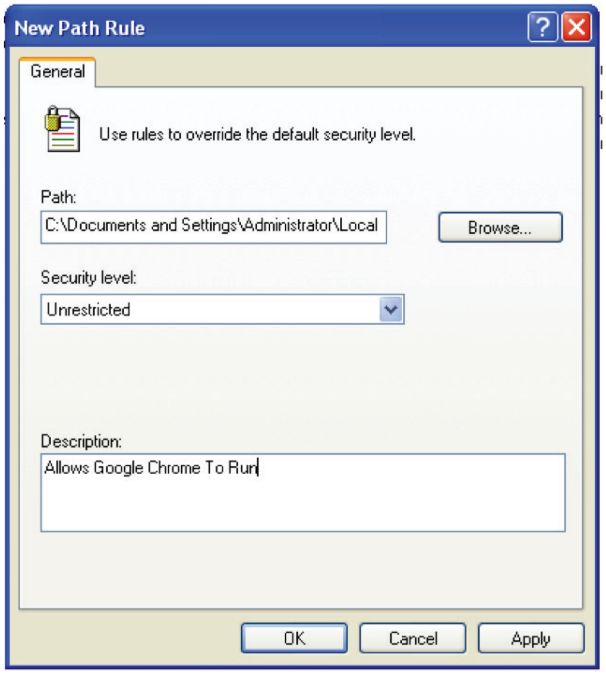
Windows cannot open this program because it has been prevented by a software restriction policy. For more information, open Event Viewer or contact your system administrator.

An Example of an Overly Strict Policy

A number of programs will stop working if policies are applied to the local appdata and temp folders.

For example, the popular browser Chrome will no longer run on the PC. This is due to the policy blocking all executables from the user's profile folder. However, Firefox will still open because its installs in C:\Program Files\Mozilla. Internet Explorer will also run as it's located in the program files path.

This policy is too strict! In the next example, a policy was disabled and a more focused, individual path and file policy was created.



New Path Rule

General

Use rules to override the default security level.

Path: C:\Documents and Settings\Administrator\Local

Security level: Unrestricted

Description: Allows Google Chrome To Run

Path and File Policy Rule

11. Blocking Access to the Volume Shadow Copy Service

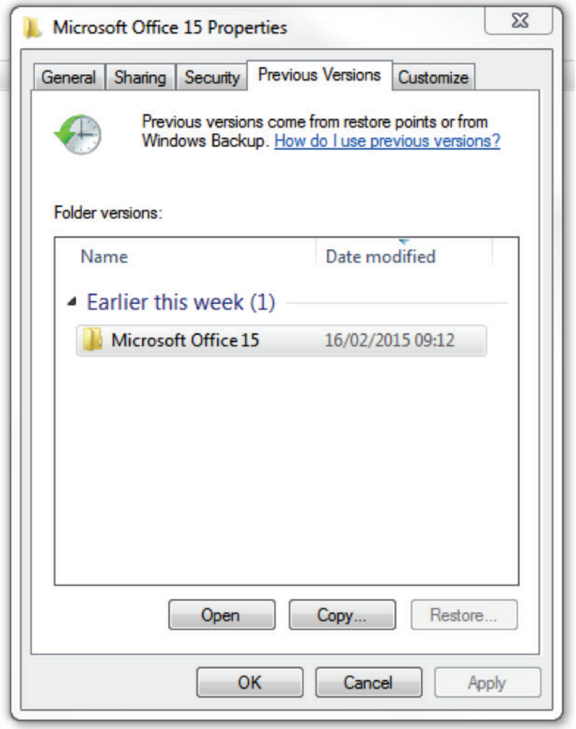
On Windows XP and more recent versions, Windows will create local copies of files using the VSS copy service.

It is located in the following path:
C:\Windows\System32\VSSAdmin.exe

The earlier versions of CryptoLocker didn't stop and remove VSS copies. Because of this oversight, data could be recovered. One of the most popular tools for this is Shadow Explorer, although the Windows function can also be used to roll the data back. It's worth noting that VSS copies are only for the local drive (normally the C:\ drive).

The VSS service is realistically only useful in Vista and above, and it's a last ditch option for encrypted files.

Please note: VSS should never be considered a substitute for backup. It protects only the local drive!



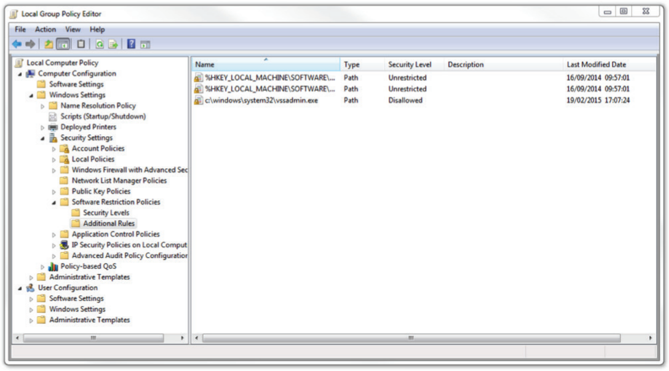
Previous versions come from restore points or from Windows Backup. How do I use previous versions?

Folder versions:

Name	Date modified
Earlier this week (1)	
Microsoft Office 15	16/02/2015 09:12

Path and File Policy Rule

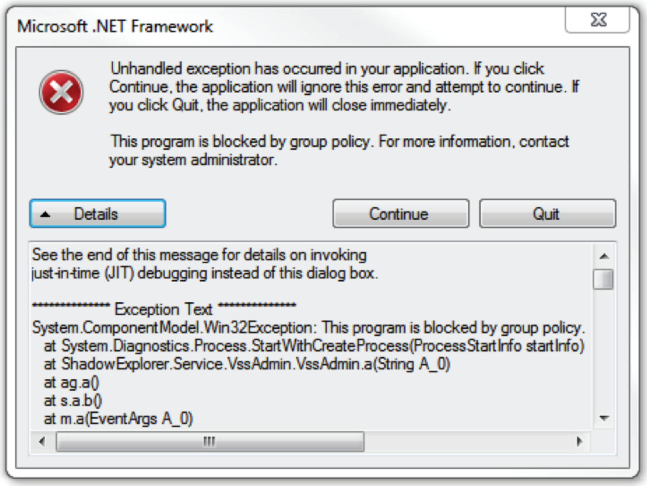
Administrators can lock access to the service and stop ransomware like CryptoLocker from trying to erase file backups. Just create a policy but point to the VSSAdmin executable. Any attempt to access/stop the service will result in a block.



Name	Type	Security Level	Description	Last Modified Date
%HKEY_LOCAL_MACHINE\SOFTWARE\...	Path	Unrestricted		16/09/2014 09:57:01
%HKEY_LOCAL_MACHINE\SOFTWARE\...	Path	Unrestricted		16/09/2014 09:57:01
c:\windows\system32\vssadmin.exe	Path	Disallowed		19/02/2015 17:07:24

Blocking VSSadmin in Local Group Policy Editor

If a program tries to access the VSSAdmin service, it will either be blocked or it won't open.



Unhandled exception has occurred in your application. If you click Continue, the application will ignore this error and attempt to continue. If you click Quit, the application will close immediately.

This program is blocked by group policy. For more information, contact your system administrator.

```
See the end of this message for details on invoking
just-in-time (JIT) debugging instead of this dialog box.

************** Exception Text **************
System.ComponentModel.Win32Exception: This program is blocked by group policy.
   at System.Diagnostics.Process.StartWithCreateProcess(ProcessStartInfo startInfo)
   at ShadowExplorer.Service.VssAdmin.VssAdmin.a(String A_0)
   at ag.a()
   at s.a.b()
   at m.a(EventArgs A_0)
```

Policy Notification on Blocking VSSAdmin

12. Blocking VBS Scripts

VBS scripts are used by malware authors either to cause disruption in an environment or to run a process that will download more advanced malware. The ILOVEYOU VBS-based attack caused a huge amount of damage back in the early 2000s. Nowadays, most VBS scripts cause irritation by hiding folders, moving files, etc. These can be disabled completely by disabling the Windows Script Host engine, which is what .VBS files use to run.

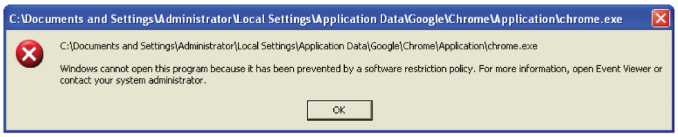
Warning: If any login scripts are used they will not be able to run.

The following registry entries are used to block the Windows Script Hosting Engine Executable from running (Wcscript.exe)

» HKEY _ CURRENT _ USER\Software\Microsoft\Windows Script Host\Settings\Enabled

» HKEY _ LOCAL _ MACHINE\Software\Microsoft\Windows Script Host\Settings\Enabled

When a VBS file attempts to run with the above registry key enabled users will see the following error message:



C:\Documents and Settings\Administrator\Local Settings\Application Data\Google\Chrome\Application\chrome.exe

C:\Documents and Settings\Administrator\Local Settings\Application Data\Google\Chrome\Application\chrome.exe

Windows cannot open this program because it has been prevented by a software restriction policy. For more information, open Event Viewer or contact your system administrator.

Notice of Blocking Windows Script Hosting

The following two registry keys provide a simple method to blocking scripts. The policy editor can be used to create a customized versions scripts need to run:

http://download.webroot.com/VBSDisable.zip

http://download.webroot.com/VBSEnable.zip

13. Filtering .EXE Files in Email Servers

If the email gateway can filter files by extension, administrators can deny emails sent with .EXE attachments or emails with obfuscated extensions. This is a common attack vector for crypto ransomware.

14. Disabling RDP

CryptoLocker/Filecoder malware often accesses target machines using Remote Desktop Protocol (RDP), a Windows utility that allows others to access your desktop remotely. If your endpoints don't need to use RDP, we recommend disabling RDP to protect machines from Filecoder and other RDP exploits. Keep in mind that Windows 7 and later OS versions disable RDP by default, but it is worth double checking on any OS. Where RDP is essential, we urge you to restrict RDP to only the users who need it, as well as imposing two factor authentication for access and a password policy that locks accounts after 5 failed login attempts. Ensuring that any Microsoft RDP vulnerability patches are applied immediately will also increase protection. Finally, to protect against remote password guessing attacks, we advise changing the listening port from the default (3389) to another to add a further barrier against breaches.

15. User Education

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 really is no excuse for not having users educated on the risks of using the network at work and at home.

Here are some simple tips to help keep users more secure:

15.1 Use two-factor authentication whenever possible.

Use it for access to the network and when users work remotely in combination with a VPN. Look at two-factor for password resets and access to web-based business tools.

15.2 Enforce the use of secure passwords.

The enforcement of strong password rules and a little basic training on strong passwords is a very important prerequisite for a more secure network.

15.3 Increase junk filtering and avoid clicking through on emails.

Phishing and spear phishing are two of the most common ways that users are duped into getting infected in the first place. Educating users about links and quarantining emails with links might be the only way to stop determined spear phishing attacks.

16. Handling Infections

If an organization is hit with an infection, the following course of action is strongly recommended:

16.1 Isolate the PC(s) immediately to stop any further incursions.

16.2 Do not re-image the PC until the infection is categorized.

16.3 Start cleaning up the infection by contacting the endpoint security vendor's support staff, who will be able to assist with any clean-up activities and ensure the infection is completely removed.

16.4 Check if user data was encrypted. The earlier this is done the better.

16.5 Alert other employees if this was a targeted attack, or about the threat vector, if appropriate.

Conclusion

This guide is not intended to be exhaustive – just to provide Webroot experience and advice on some of the best ways to protect against crypto ransomware.

A few simple steps can mean protecting against an attack and not relying on the goodwill of a criminal to restore a business' data and productivity.

Further Information

» A lot of very useful information about crypto ransomware was released by the ICIT in its ICIT ransomware report: "2016 Will Be The Year Ransomware Holds America Hostage." The PDF for this document can be found at this URL: http://icitech.org/wp-content/uploads/2016/03/ICIT-Brief-The-Ransomware-Report.pdf

» This document benefits from content taken from Webroot blogs and articles written by Webroot Threat Research and Support teams.

Links to recent and relevant blogs may be found below:

» KeRanger:
- http://www.webroot.com/blog/2016/03/07/18611/

» Locky:
- http://www.webroot.com/blog/2016/02/22/locky-ransomware/

» Padcrypt:
- http://www.webroot.com/blog/2016/02/18/new-ransomware-padcrypt-first-live-chat-support/

» RaaS Ransomware as a Service:
- http://www.webroot.com/blog/2015/07/28/encryptor-raas-ransomware-as-a-service/

» TeslaCrypt:
- http://www.webroot.com/blog/2015/03/12/teslacrypt-encrypting-ransomware-that-now-grabs-your-games/

» Critroni:
- http://www.webroot.com/blog/2014/07/25/critroni-new-encrypting-ransomware/

» A Typical Macro Infection:
- http://www.webroot.com/blog/2016/01/14/a-look-at-a-typical-macro-infection/

» Best practices for securing your environment against CryptoLocker and ransomware:
- https://community.webroot.com/t5/Webroot-Education/Best-practices-for-securing-your-environment-against/ta-p/191172

About Webroot

Webroot delivers next-generation network and endpoint security and threat intelligence services to protect businesses and individuals around the globe. Our smarter approach harnesses the power of cloud-based collective threat intelligence derived from millions of real-world devices to stop threats in real time and help secure the connected world. Our award-winning SecureAnywhere® endpoint solutions, BrightCloud® Threat Intelligence Services, and FlowScape® solution protect millions of devices across businesses, home users, and the Internet of Things. Trusted and integrated by market-leading companies, including Cisco, Citrix, F5 Networks, Aruba, Palo Alto Networks, A10 Networks, and more, Webroot is headquartered in Colorado and operates globally across North America, Europe, and Asia. Discover Smarter Cybersecurity™ solutions at webroot.com.

World Headquarters
385 Interlocken Crescent
Suite 800
Broomfield, Colorado 80021 USA
+1 800 772 9383

Webroot EMEA
6th floor, Block A
1 George's Quay Plaza
George's Quay, Dublin 2, Ireland
+44 (0) 870 1417 070

Webroot APAC
Suite 1402, Level 14, Tower A
821 Pacific Highway
Chatswood, NSW 2067, Australia
+61 (0) 2 8071 1900