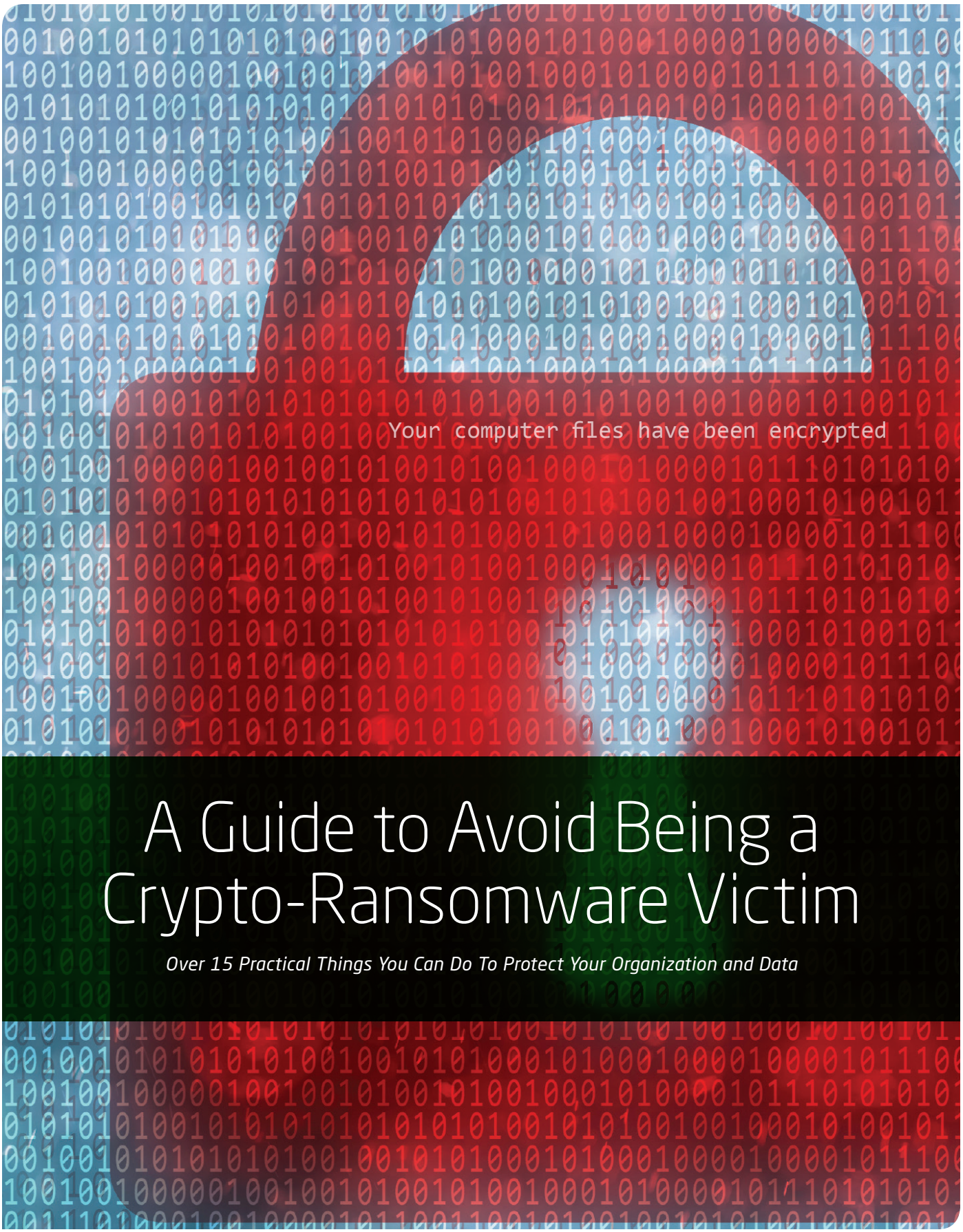
WHITE PAPER

WEBROOT
Smarter Cybersecurity™



A Guide to Avoid Being a Crypto-Ransomware Victim

Over 15 Practical Things You Can Do To Protect Your Organization and Data

CONTENTS

INTRODUCTION AND BACKGROUND

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

We often get asked the leading question: "which endpoint security solution will offer 100% prevention and protection from crypto-ransomware?" 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. At other times the cybercriminals will have found ways to circumvent endpoint security defenses and their attack will likely succeed.

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

As a result of the many webinars we've held on crypto-ransomware, and all the questions received, we have decided to issue this guide to help our customers and other organizations from becoming crypto-ransomware victims. It's consciously titled 'A Guide to Avoid Being a Crypto-Ransomware Victim!' and explores over 15 key ways to more completely secure your IT environment from crypto-ransomware, while demonstrating that with even a modest outlay you can mitigate this growing and highly damaging criminal threat.

Please bear in mind that this guide is only intended to point out some of the more practical approaches you can take. Some of these recommendations may not be suitable to your particular IT environment. Take this guide with the small warning that some of these recommendations will cause certain programs not to install or function as expected.

CRYPTO-RANSOMWARE MITIGATION GUIDE

This guide will examine a number of mitigation strategies that will help protect your organizations' data from crypto-ransomware attacks.

The truth is that we have seen crypto-ransomware writers develop ever more sophisticated ways to infect endpoints, infections that even 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 recent LA hospital breach. For smaller businesses, such an attack could put them out of business.

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

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.

Of course, you need protection that covers multiple threat vectors. 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.

Over the past four years, the Webroot approach to infection prevention 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. Today, Webroot is probably the only endpoint security vendor that delivers proven endpoint malware prevention at scale. Because of this, we are fast becoming the alternative of choice to conventional endpoint antivirus solutions.

Regardless of which endpoint security solution you choose, it's essential it 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. Critical Data Backup

If you have failed to stop ransomware from successfully encrypting your data, then the next best protection is being able to restore your data and minimize business downtime.

Bear in mind when you are setting up your backup strategy that crypto-ransomware like CryptoLocker will also encrypt files on drives that are mapped, and some modern variants will look for unmapped drives too. Crypto-ransomware will look for external drives such as a USB thumb drives, as well as any network or cloud file stores that you have assigned a drive letter to. 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. 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 the solutions available to protect them.

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 by businesses like yours to protect their IT environments and thwart crypto-ransomware threats and attacks.

3.1. Make sure your chosen 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 you allocate policy.

3.2. Check regularly that your backups are working.
It's vital to check that your 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 your workload by applying them and putting in place a patching routine. Like backups, many organizations suffer damaging infections simply because they are not up to date with their patching. This is a security fundamental, and there is no good excuse for not having a good patch management regime in place.

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 Ad Blocking plugin.
Modern browsers like Chrome and Firefox are constantly being updated to reduce their vulnerabilities. They also give you the option to add BHO's 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. You can 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. It is important however as 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.

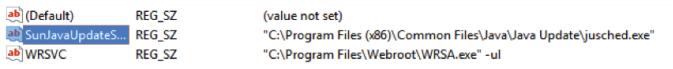
3.9. Show hidden file extensions.
One way ransomware like CryptoLocker and others frequently arrive is in a file named with the extension ".PDF.EXE" or something similar. The malware writer counts on Window's default behavior of hiding known file-extensions being active so that users' suspicions are not raised by this corrupt extension. If you enable the ability to see full file extensions, it is easier for you and your users to easily spot suspicious files.

4. Creating Windows Policies to Defend against Ransomware

When it comes to crypto-ransomware, you will need to create some Windows Policies to block certain paths and file extensions from running.

Java generally gets the most coverage when it comes to exploited software, but it applies to nearly all commonly used plugins. Generally speaking, if you do not intend on using certain plugins it is better not to have them installed.

If you do make use of them, then make sure they are up to date, i.e. do not disable the run keys for the Java updaters, etc.



Example of a Java Updater Service

Common Paths

In this guide, we talk about paths and file types, so a brief introduction might be useful. Malware generally drops into a few common paths. Once there, it is free to move around within 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

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 you see a WinLogon.exe file in the user's temp folder that is twice that size, it should be a red flag and the file should be looked at! In fact, this is taken care of by antimalware, but it does give you an idea of what we are trying to achieve in this guide. In the following sections we are going to show you how to use policies to restrict access to certain file types and paths.

The more restrictive we 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 your endpoints for a number of reasons:

5.1. If your only browser gets damaged it can make connecting remotely difficult. Not everybody uses RDP. In fact, we recommend 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.

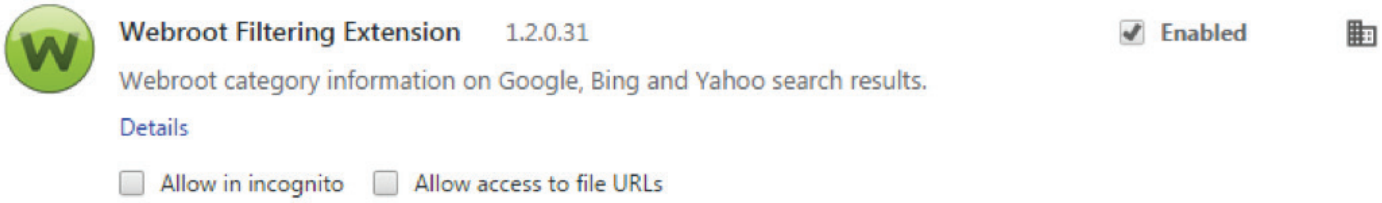
5.4. Older versions of Windows do not have the ability to install newer versions of IE.

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 very useful ability within both Chrome and Firefox is the ability to use plugins. As we've mentioned, these are be quite helpful at stopping some issues entirely.

Useful Browser Plug-in Types:

- Ad blockers
- Script blockers
- Web filters



Webroot Filtering Extension Installed in Chrome

While many websites need advertisements to stay online, we have seen more and more popular websites (i.e. millions of visitors a year) infecting customers due to 3rd party hosted adverts 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 stopping less technical users from being infected.

Script blockers stop Java scripts from running on websites unless you specifically ask for them to be allowed. These require a bit more technical knowledge on the user's behalf and thus aren't recommended for less technical users. Many websites use Flash and Java plugins, and if a user isn't able to figure this out, it can lead to support tickets/calls.

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

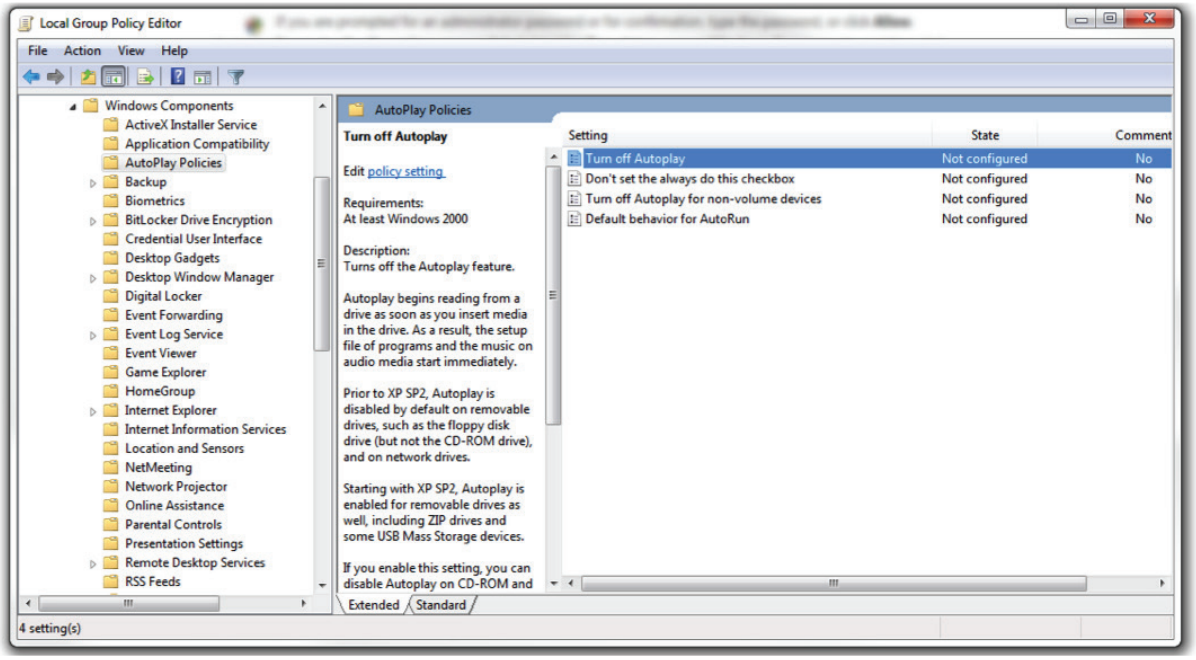
The Webroot filter checks website reputations and will alert the user if they are visiting a site that is unsafe.

6. Disabling Autorun

While autorun is a useful feature, it is used by malware to spread around a corporate environment. You can disable autorun 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.



Turning off Autoplay

7. Using the Policy Editor to Block Paths

Policies are a powerful tool that you can use for a multitude of purposes. They commonly stop users from opening or installing certain software, however you can get very creative with them too. The example below uses local policies, but the same principles apply to network group polices. This guide can only be a very brief introduction, but should you need more information we would advise looking at this link from Microsoft: https://technet.microsoft.com/en-us/library/bb457006.aspx

Policies can be set up in groups so you can have more or less strict policies for certain groups. This can be useful if you have a group of users that need more access, or are more tech savvy.

Please note that we advise you test any policies on a test PC that is not mission-critical!

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
- Blocking creation of startup entries

Realistically, the following files types shouldn't be run in the following directories:

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

A policy on the above would be a reasonably safe. Crypto-ransomware does sometimes use the .SCR file format, which is a portable executable (PE) that is sometimes forgotten. You could go another step and create a policy blocking PE file formats from common paths where malware droppers are commonly located.

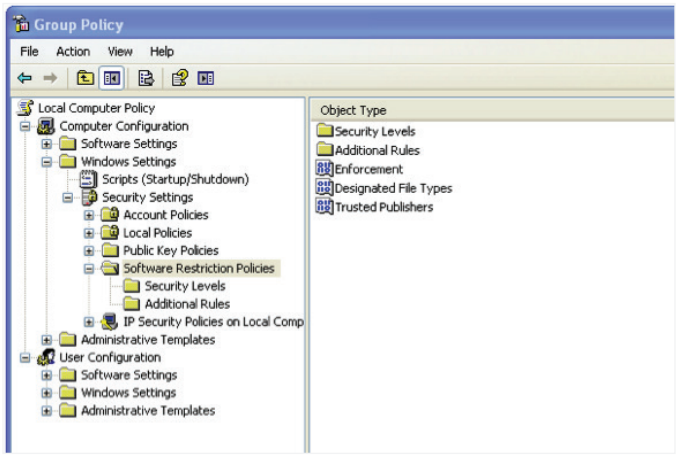
- .EXE, .DLL, .SYS, .FON, .EFI, .OCX, and .SCR
- Temp, Appdata, ProgramData, etc.

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

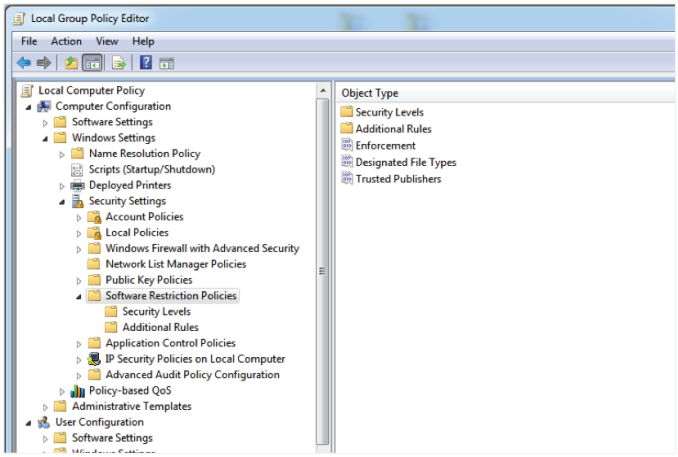
- Click **Start**, type msc in the **Start Search** box, and then press **Enter**.

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**.



Accessing Group Policy

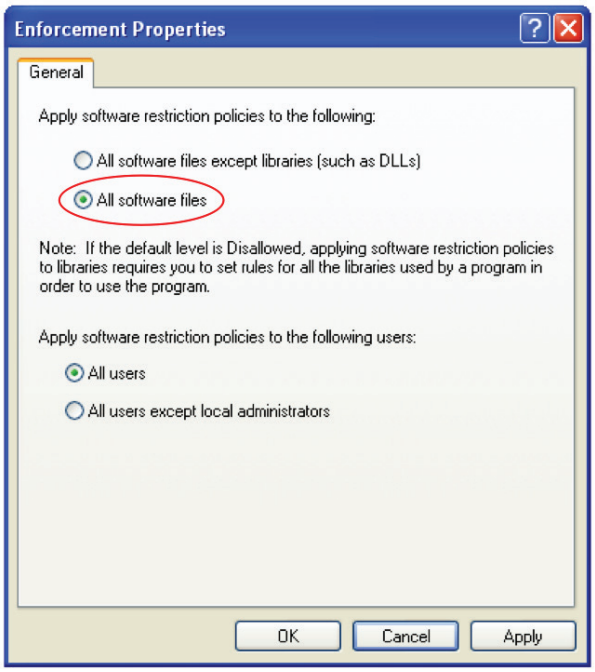


Local Group Policy Editor

8. Testing Out a Policy

To create a policy you need to expand out the tree to get to the following:

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



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."

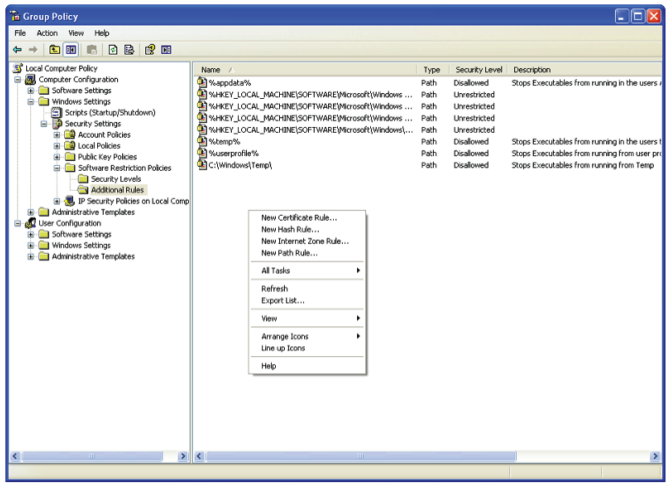
Creating a Policy

Then we get a small window in which we can create our rules. In this window, we can browse to specific folders or we can use common Windows wildcard paths. In the case below, we have created a Policy that will block executable files from running from the following path:

C:\Windows\Temp

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 you can do. You can get creative with the paths you define (see in screenshot below).

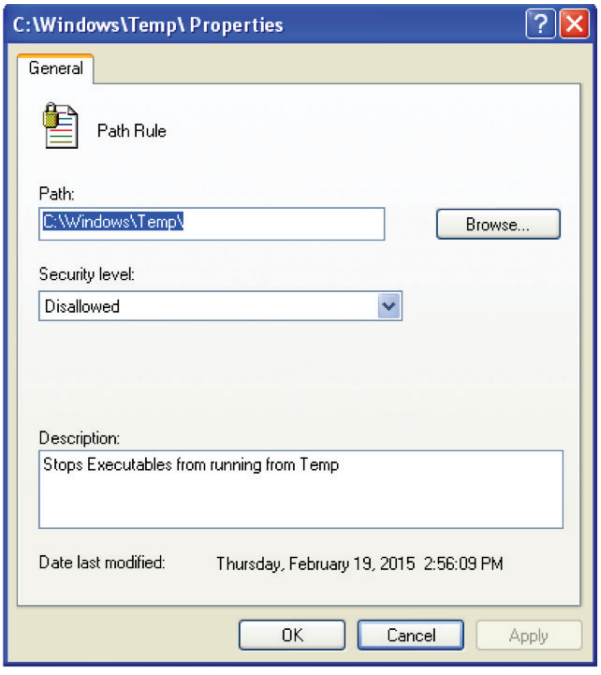
Please Note that in the case above the user will not be able to run anything from their desktop!



Creating a Policy

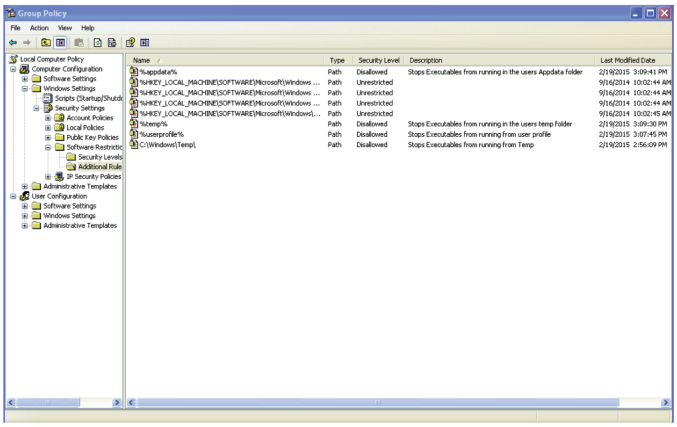
1. %appdata%
2. %temp%
3. %userprofile%
4. %localappdata%
5. %programdata%
6. C:\Windows\Temp

It is worth noting that a number of legitimate programs and updaters also run from the user's appdata. If for some reason you have legitimate software that you know is set to run not from the usual Program Files area but the appdata area you will need to exclude it from your rules or it will NOT run.



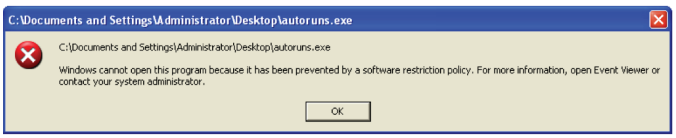
Stopping an Executable in Temp

In the example below, we have created a few policies to block executables from running within the following Name/Paths:



Stopping Executables by Path

In the screen shot below we have attempted to run an executable that is located on the local admins desktop. As you can see, Windows automatically pop-ups an alert and the program doesn't run. If we moved the file to another path that doesn't have a restricted policy, the program will open without any issues.

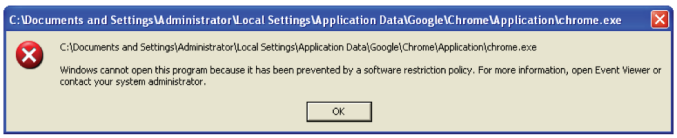


Executable Block Notice

10. Fixing Issues with Blocked Programs

A number of programs will stop working if you apply policies to the local user's appdata and temp folders.

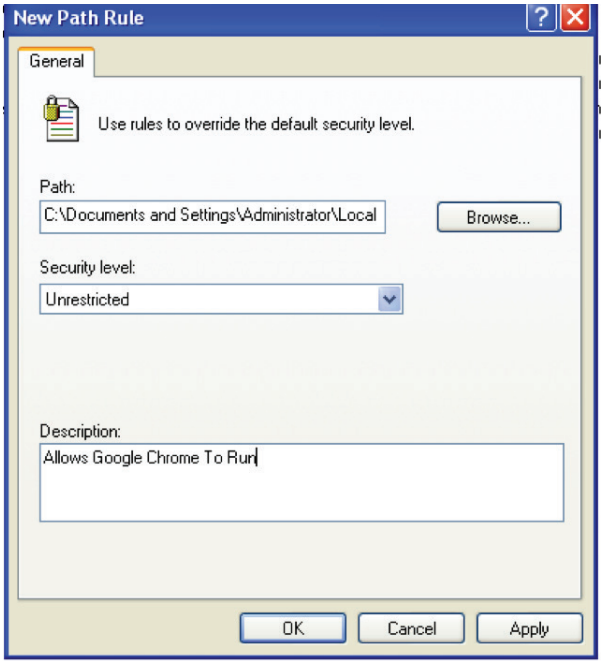
For example, the popular browser Chrome will no longer run on the PC. This is due to the policy of blocking all executables from the user's profile folder. However, Mozilla Firefox will still open because its installs in C:\Program Files\Mozilla\. Internet Explorer will also run as it's located in the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



An Example of an Overly Strict Policy

This policy is too strict! In the next example we have disabled that policy and started creating more focused path and file polices.

We can create an individual path and file policy rule as seen below.



Path and File Policy Rule

11. Blocking Access to the Volume Shadow Copy Service

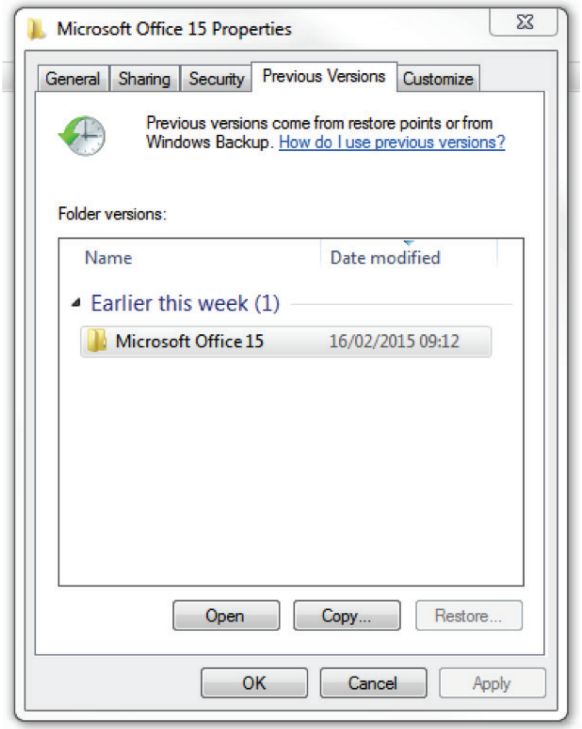
On Windows XP and above, Windows will create local copies of files using the VSS copy service.

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 you can use the Windows function to roll the data back. It's worth noting that VSS copies are only for the local drive (normally the C:\ drive).

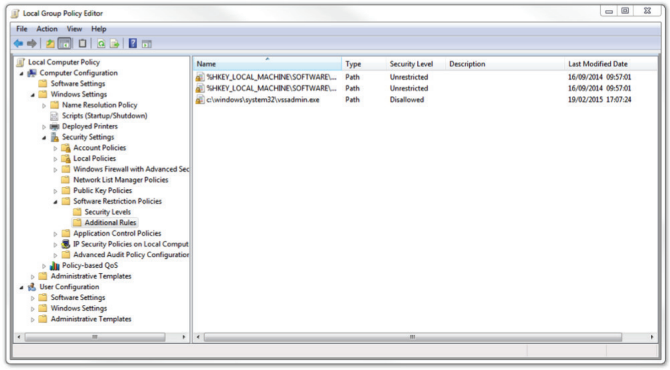
The VSS service is realistically only useful in Vista and above, and it's a last ditch option for encrypted files.

Important Note – VSS should never be considered a substitute for backup. It protects only the local drive!



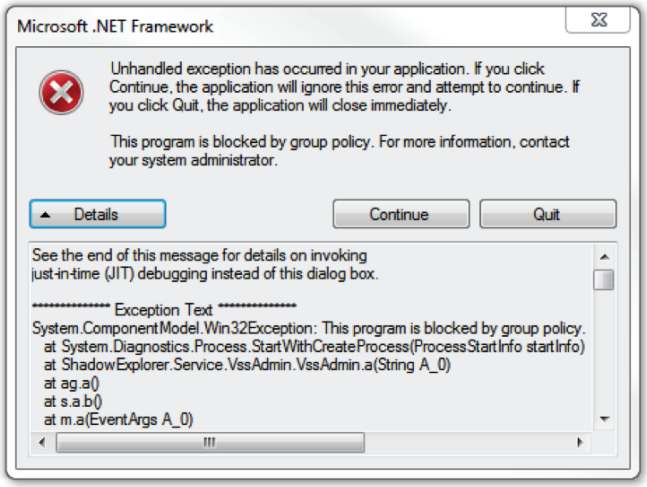
Path and File Policy Rule

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



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.



Policy Notification on Blocking VSSAdmin

12. Disabling Windows Script Hosting – 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 malware caused a huge amount of damage back in the early 2000s. Nowadays, most VBS scripts cause irritation by hiding folders, moving files, etc. You can disable them completely by disabling the Windows Script Host engine, which is what .VBS files use to run.

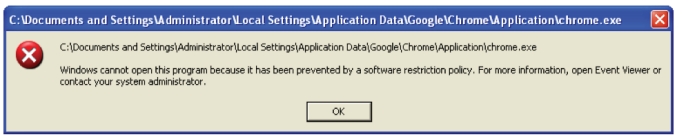
Warning: if your company uses any login scripts they will not be able to run.

Note that you can use a policy to also disable the use of VBS files (see the link posted earlier in item 7).

The following two registry entries are the two entries that 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 you will see the following error message:



Blocking Notice Windows Script Hosting

This is a simple method to block these, the following two registry keys are located below if you wish to use them. You can use the policy editor to create more custom versions if you do need to run scripts:

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

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

13. Filtering .EXE Files in Email Servers

If your email gateway has the ability to filter files by extension, you may wish to deny email sent with .EXE files, or to deny mail sent with files that have two file extensions, the last one being executable ("*.*.EXE" files). This is a common threat vector for crypto-ransomware

14. Disabling RDP

The CryptoLocker/Filecoder malware often accesses target machines using Remote Desktop Protocol (RDP), a Windows utility that allows others to access your desktop remotely. If you do not require the use of RDP, you can disable RDP to protect your machine from Filecoder and other RDP exploits. In Windows 7 and later versions, RDP is disabled by default, but it is worth checking regardless of the OS you protect.

15. User Education

The "human firewall" – your 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 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.

Here are some simple things you can do to help keep your users more secure:

15.1 Use two-factor authentication whenever possible.
Use it for access into the network and when users work remotely from the office in combination with a VPN connection. Look at two-factor for password resets and access to web-based business tools.

15.2 Enforce the use of secure passwords.
We still rely on password authentication for sign-on to our desktops and other applications. The enforcement of strong password rules and a little basic training of users on how to create strong but easily remembered passwords, is a very important prerequisite for a more secure work environment.

15.3 Increase junk filtering and avoid clicking through on e-mails.
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, even those that appear to come from someone they know and trust is going to help. And quarantining email with links or disabling links might be the only way to stop determined spear-phishing attacks.

16. Handling Infections

If your organization is unfortunate enough to be hit with an infection, we strongly recommend the following courses of action.

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

16.2 Do not re-image the PC until it is determined what the infection was.

16.3 Start cleaning-up the infection by contacting your 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 Determine the nature of that particular infection with your vendor's support staff.

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

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

17. Conclusion

This guide is not intended to be exhaustive – just to give you the benefit of our experience on some of the best ways to ensure you do not become a crypto-ransomware victim. Extortion is an ugly crime and paying up only fuels further crime and misery.

Just taking a few simple steps can mean protecting your organization from the impact of suffering such an attack and not relying on the goodwill of a criminal to get your data restored and business productive.

18. Further Information

18.1 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

18.2 This document benefits from content taken from Webroot Blogs and articles written by our Threat Research and Support teams. A particular thanks goes to those contributors for the contents of this Guide.

Links to the most recent and relevant WebrootBlogs 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

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