

Your computer files have been encrypted

MSP Guide: Stopping Crypto Ransomware Infections in SMBs

16 Easy Actions for MSPs



CONTENTS

An MSP Guide to Protecting SMBs from Crypto Ransomware 1

Introduction and Background3

Crypto Ransomware Mitigation Guide.....3

 1. Use Reputable, Proven, Multi-Vector Endpoint Security3

 2. Data Backup; Datto Business Continuity4

 3. General Protection Tips.....6

 4. Creating Windows Policies to Defend Against Ransomware7

 5. Common Paths7

 6. Choosing a Second Browser.....7

 7. Disabling Autorun8

 8. Using the Policy Editor to Block Paths9

 9. Testing Out a Policy.....10

 10. Creating a Policy10

 11. Fixing Issues with Blocked Programs11

 12. Blocking Access to the Volume Shadow Copy Service.....11

 13. Blocking VBS Scripts.....12

 14. Filtering .EXE Files in Email Servers13

 15. Disabling RDP13

 16. User Education13

 17. Handling Infections.....13

 18. Conclusion.....15

 19. Further Information.....15

INTRODUCTION AND BACKGROUND

As the impact and severity of crypto ransomware have grown over the past 2½ years, we have published many blogs and articles on how best to defend against these modern day extortionists. Neither Webroot nor Datto believe that businesses should have to choose between extortion and losing precious, irreplaceable business data, which ultimately might put a customer out of business.

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 striving toward) will only be 100% effective some of the time. At other times, cybercriminals will have found ways to circumvent endpoint security and their attacks will succeed.

As an endpoint security provider, we cannot stand on the sidelines when we know that even with Webroot® endpoint security organizations could still get infected — especially when other key mitigation strategies, like protected backups, will help keep business on its feet.

CRYPTO RANSOMWARE MITIGATION GUIDE

This guide will examine a number of mitigation strategies that will help protect organization's data from crypto ransomware attacks.

We have seen crypto ransomware writers develop ever 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 SMBs, such an attack could put them out of business permanently. We are no longer talking about a few PCs being compromised but entire networks, including servers. Recent discoveries in the wild point to a new age of self-propagating crypto worms and ransomware evolving from indiscriminate attacks to targeted attacks on enterprise networks. Crypto worms are not yet self-sufficient but they do have some of the characteristics of successful worms, including rapid propagation, payload delivery, and crippling recovery efforts.

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.

Datto and Webroot have co-hosted many webinars on crypto ransomware. These webinars regularly generate a large volume of questions, so we have decided to issue this guide to help prevent our partners and other organizations from becoming crypto ransomware victims.

This paper explores over 15 ways to secure SMBs from crypto ransomware attacks — including using Datto backup, disaster recovery and business continuity solutions — 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 is only intended to point out some of the more practical approaches to take. 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 and Datto, we hope you find this guide educational, useful, and valuable in protecting businesses from extortion.

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.

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 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 is chosen, 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. Data Backup; Datto Business Continuity

There are a growing number of ransomware families proliferating today – and each type has many variants, with new family variants surfacing frequently. Ransomware is constantly evolving as cybercriminals adapt code and use new obfuscation techniques to avoid detection by security software. While strong endpoint security is an absolute necessity, it's not enough to secure an organization from ransomware.

A complementary cloud-based technology to Webroot is Datto. Datto provides modern data protection and business continuity technology designed specifically for the needs of SMBs. While businesses of all sizes are at risk, SMBs may be more likely to suffer an attack. Frequently, small business IT teams are stretched thin and in some cases rely on dated technology due to budgetary constraints. This is the perfect storm for ransomware vulnerability.

Modern Backup and Recovery for SMBs

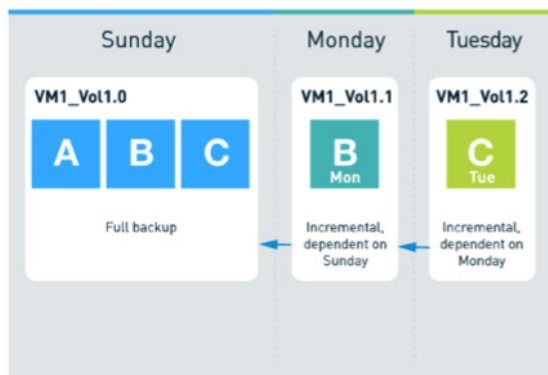
Modern data protection products, like Datto, can take snapshot-based, incremental backups as frequently as every five minutes to create a series of recovery points. Backups are stored in a universal virtual

file format on an on-premise Datto appliance and simultaneously replicated in the Datto cloud for disaster recovery. If a business suffers a ransomware attack, you can quickly restore data and applications to a point in time before the corruption occurred. Datto offers fast restores, typically less than 10 seconds, due to proprietary [Inverse Chain Technology](#).

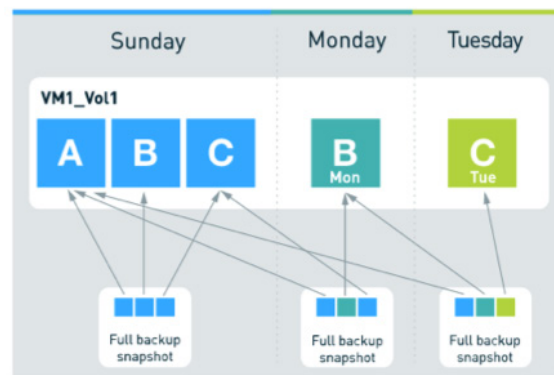
Incremental backup has operated on the same basic principle since tape was the preferred medium. First, a full backup is created. Then, subsequent backups only copy data that has changed since that initial full. In order to recover data, the backup system must rebuild a full backup from a chain of incrementals. If one incremental is corrupt, all of the recovery points that follow become unusable – which means the data is then lost.

Inverse Chain Technology takes the old methodology and turns it on its head. Instead of chains of dependent incrementals, which must be reconstructed, Inverse Chain Technology stores every previous recovery point in an independent, fully constructed state using a ZFS-based “copy on write” capability. So, there is no rebuild process when reverting to a previous point in time.

When it comes to ransomware, the benefits of this technology are threefold. First, businesses don't need to pay the ransom to get their data back. Second, potentially expensive downtime is avoided. And third, since this restores to a point in time before the ransomware infection, it can be certain everything is clean and the infection won't be triggered and re-infect the data again.



TRADITIONAL BACKUPS create multiple backup files for each server. These files are logically dependent upon each other, creating a “dependency chain”. Removing parts of the chain is taxing if not impossible, putting backup data at continuous risk.



DATTO “INVERSE CHAIN TECHNOLOGY” leverages integrated advanced file system versioning to facilitate dependency-free “views” of the backup data. Every recovery point in a fully constructed state and any one can be deleted without resetting a chain.

SMB Business Continuity Today

Many organizations don't fully understand how long it takes to recover using traditional backup technology.

It wasn't long ago that daily incremental and weekly full backups to tape or dedicated disk backup with an off-site copy on tape was the only option for most businesses.

Many companies still use this approach today. Restores from on-site backups are fast and effective. However, if data needs to be restored from off-site tape – say if a business suffered a ransomware attack that impacted primary and backup systems – it can be painfully slow.


The same goes for restoring data from traditional cloud backups. Incremental backups to the cloud are fast because, only small amounts of data are being sent periodically throughout the day. If a few files need to be restored, no big deal. They'll restore over the Internet quickly. But, if a large number of files need to be restored following a ransomware attack, the restore could drag on for days.

This has kept a lot of businesses away from cloud backup in the early days. But today, some data protection products allow users to run applications from image-based backups of virtual machines on-premise or in the cloud.

This capability is commonly referred to as “recovery-in-place” or “instant recovery.” The technology allows users to continue business operations while primary systems are being restored, dramatically reducing downtime. The Datto version of this technology is called Instant Virtualization.

In the event of a ransomware infection, this approach will give the ability to mitigate any takeover of data and almost immediately restore 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 at their IT systems and invest in the solutions available to protect them.

Crypto ransomware punishes businesses that don't back up their data. Since modern cloud services are so affordable, there's really no excuse for a business not to have a robust business continuity plan in place.



RECOVERY TIME CALCULATOR

EVALUATE YOUR RECOVERY TIME AND RECOVERY POINT OBJECTIVES

SET OBJECTIVES	
RECOVERY TIME OBJECTIVE 0 HR 30 MIN	RECOVERY POINT OBJECTIVE 12 HR 0 MIN

RECOVERY PROCESS	
HOW MUCH DATA IS ON YOUR CRITICAL BUSINESS SYSTEMS?	250 GB
HOW OFTEN DO YOU CURRENTLY BACKUP THESE SYSTEMS?	12 HR 0 MIN
HOW LONG DOES IT TAKE TO INITIATE YOUR RECOVERY PROCESS?	1 HR 0 MIN
ARE YOU RECOVERING DATA FROM A LOCAL NETWORK OR THE CLOUD?	<input checked="" type="radio"/> LOCAL <input type="radio"/> CLOUD

DOWNTIME COSTS	
HOW MANY EMPLOYEES WOULD BE AFFECTED IF THE CRITICAL SYSTEMS FAILED?	20 EMPLOYEES
WHAT IS THE AVERAGE WAGE OF AN EMPLOYEE USING THESE SYSTEMS?	20 DOLLARS PER HOUR
WHAT IS THE OVERHEAD COST OF THESE EMPLOYEES?	0 DOLLARS PER HOUR
WHAT IS THE REVENUE GENERATED PER HOUR OF THESE EMPLOYEES?	0 DOLLARS PER HOUR

CALCULATE

Example of Recovery Time Calculator

3. General Protection Tips

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

3.1. Make sure the 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 Windows' default behavior of hiding known file-extensions being active so that users' suspicions are not raised by this corrupt extension. If the ability to see full file extensions is enabled, 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 generally gets the most coverage when it comes to exploited software, but it applies 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\WRSVC.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 %localuser temp%)
- » 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:\Recycler\ (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


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 Installed in Chrome

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.

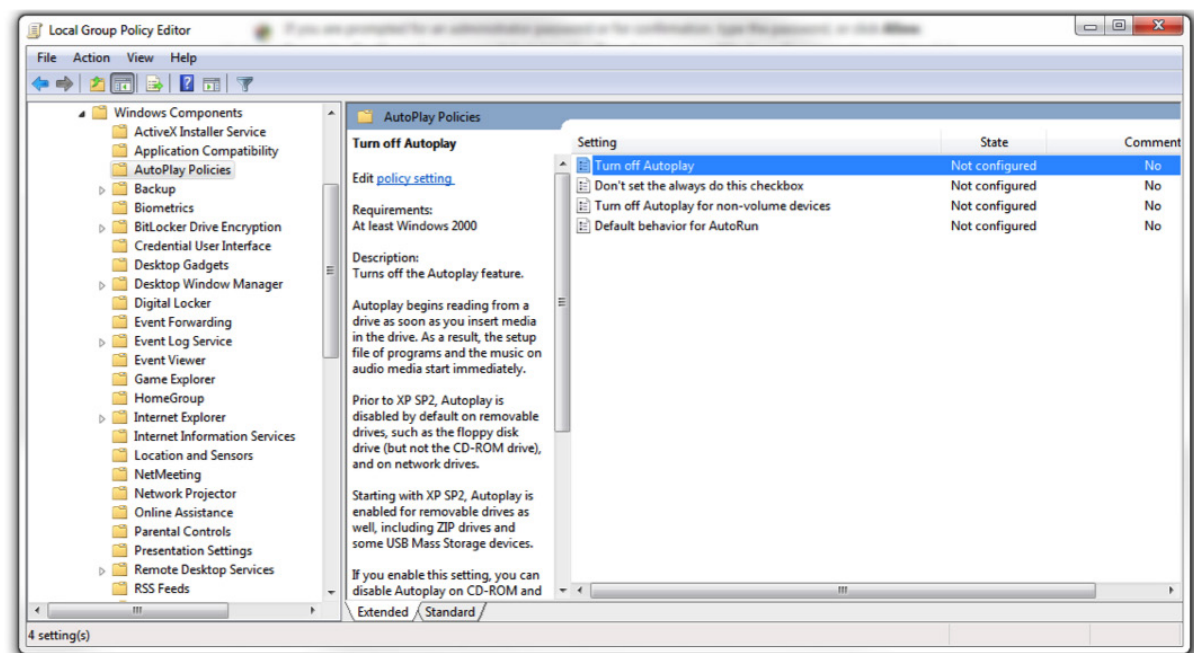
The Webroot filter checks website reputations and will alert the user if they are visiting a site that is unsafe.

6. Disabling Autorun

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



Turning off Autoplay

7. Using the Policy Editor to Block Paths

Policies are a powerful tool that can be used for a multitude of purposes. They commonly stop users from opening or installing certain software, however they can be creatively used as well. The example below uses local policies, but the same principles apply to network group policies. This guide is only a very brief introduction, but should more information be needed, we advise looking at this link from Microsoft: <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!

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.

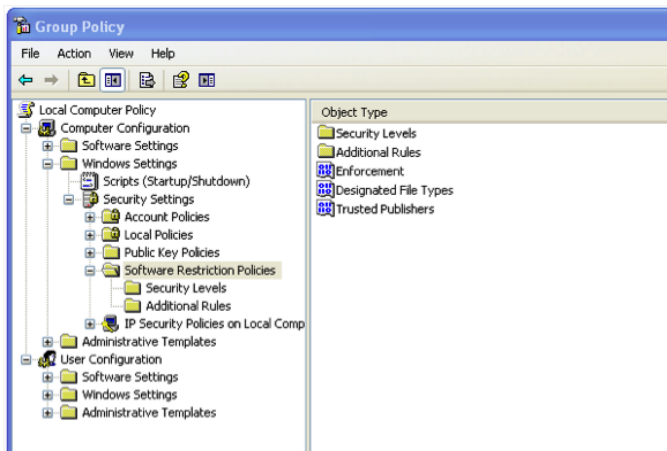
- » .EXE, .DLL, .SYS, .FON, .EFI, .OCX, and .SCR
- » Temp, Appdata, ProgramData, etc.

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

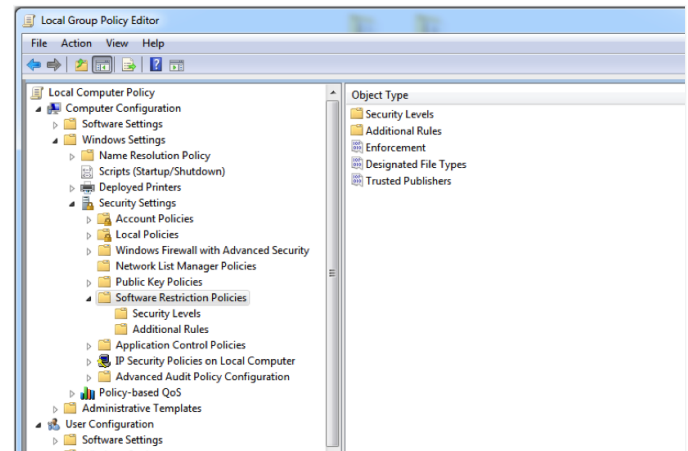
- » Click **Start**, type msc in the **Start Search** box, and then press **Enter**.

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**.



Accessing Group Policy

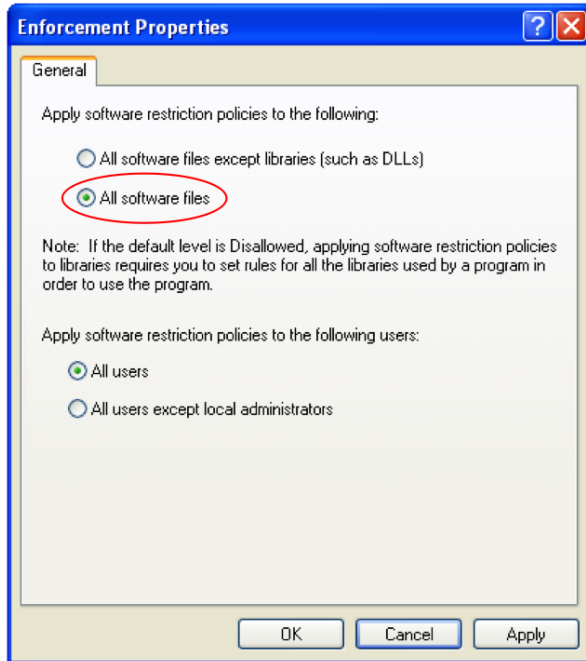


Local Group Policy Editor

8. Testing a Policy

To create a policy, expand 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.”

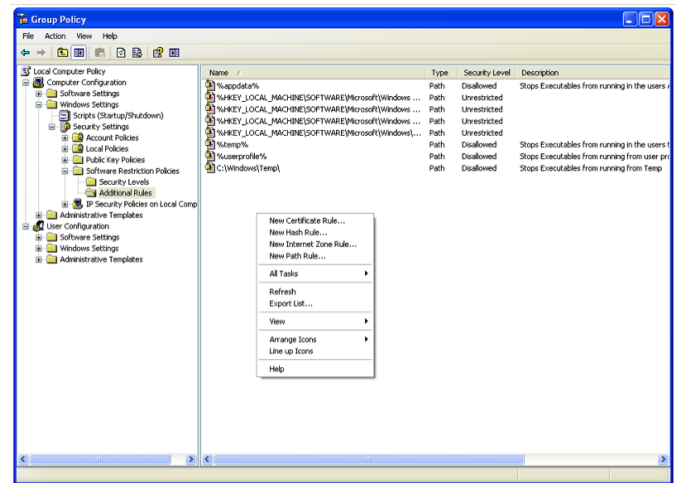
Creating a Policy

Then there is a small window which can be used to create the rules. 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 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 can be done. Get creative with the paths defined (see screenshot 'Creating a Policy').

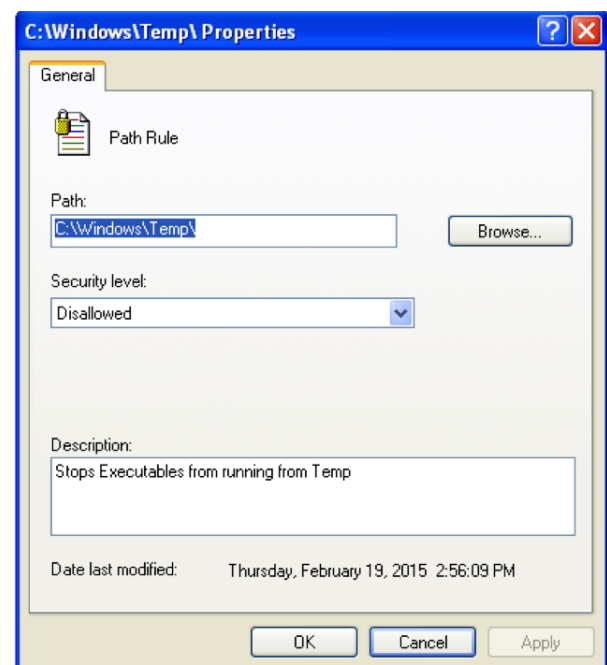
Please note: In the case above the user will not be able to run anything from their desktop!



Creating a Policy

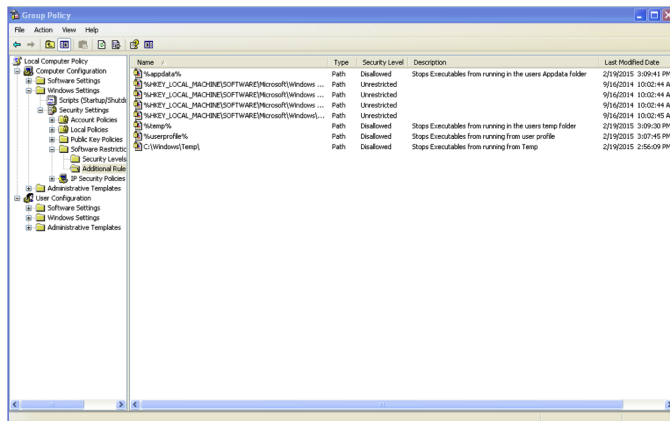
1. %appdata%
2. %temp%
3. %userprofile%
4. %localappdata%
5. %programdata%
6. C:\Windows\Temp

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



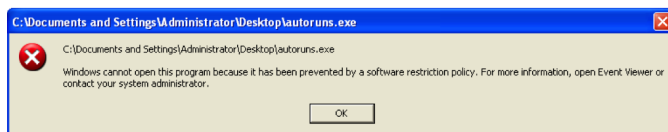
Stopping an Executable in Temp

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



Stopping Executables by Path

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.

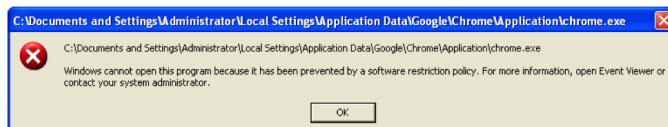


Executable Block Notice

10. Fixing Issues with Blocked Programs

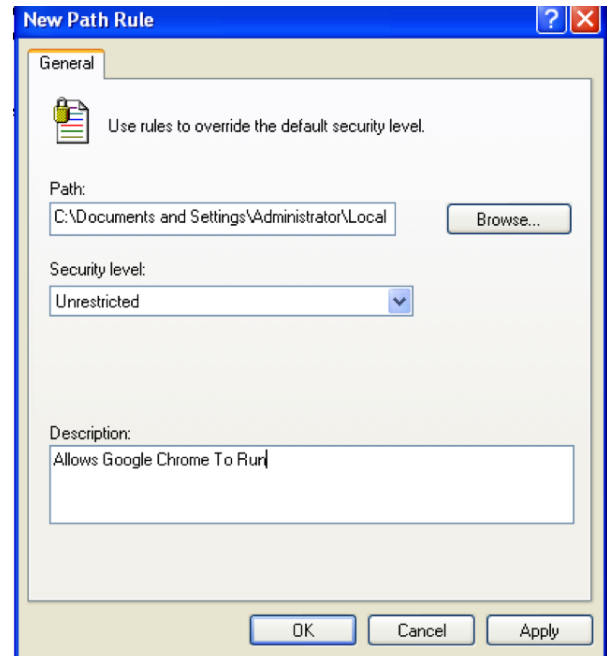
A number of programs will stop working if policies are applied to the local appdata and temp folders.

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.



An Example of an Overly Strict Policy

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



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.

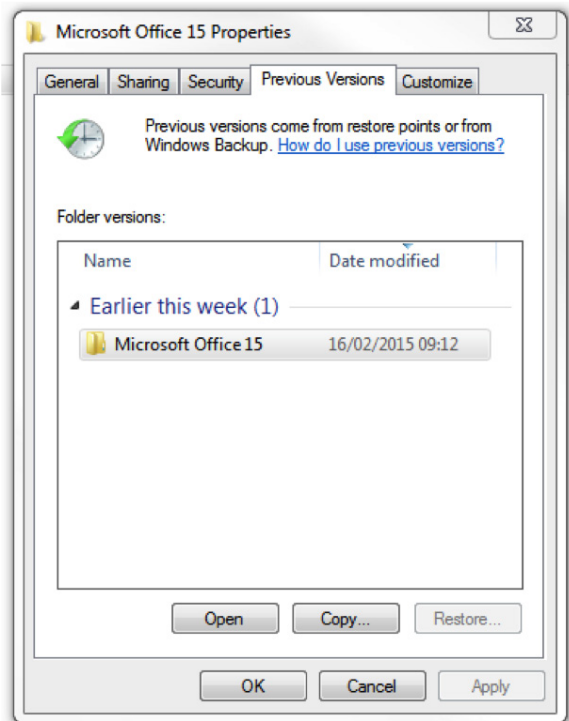
It is located in the following path:

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).

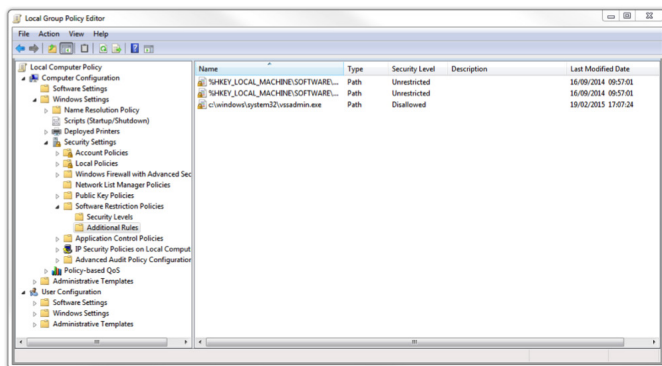
The VSS service is realistically only useful in Vista and above, and it's a last ditch option for encrypted files.

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



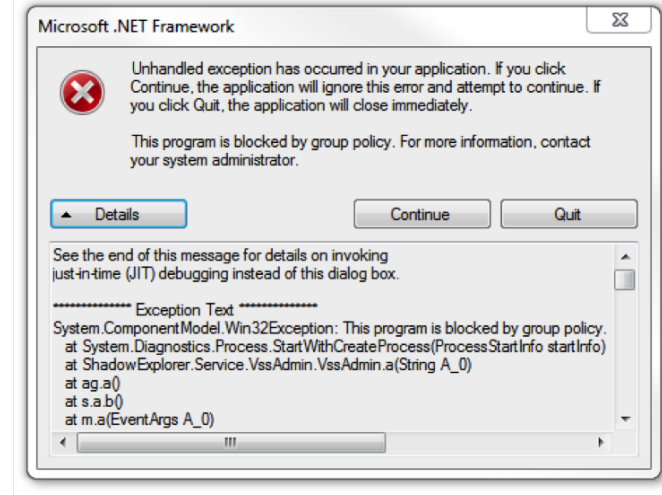
Path and File Policy Rule

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.



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. Blocking VBS Scripts

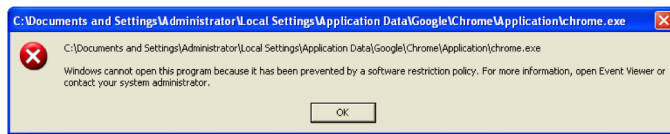
VBS scripts are used by malware authors either to cause disruption in an environment or to run a process that will download more advanced malware. The ILOVEYOU VBS-based attack caused a huge amount of damage back in the early 2000s. Nowadays, most VBS scripts cause irritation by hiding folders, moving 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 (Wscript.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:



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 and Filecoder malware often access target machines using Remote Desktop Protocol (RDP), a Windows utility that allows others to access desktops remotely. If businesses don't need RDP, it should be disabled to protect machines 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.

15. User Education

The "human firewall" — 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 users of the risks they face in the office and from using the Internet at home.

Here are some simple things 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.

17. Conclusion

This guide is not intended to be exhaustive — just to provide the benefit of Webroot's and Datto's experience and advice on some of the best ways to protect against crypto-ransomware. Extortion is an ugly crime and paying up only fuels further crime and misery.

Just taking a few simple steps can mean protecting against an attack and not relying on the goodwill of a criminal to get 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 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>

18.3 In this document are links to the features and functions of Datto's backup disaster recovery and business continuity solutions, here are those links for easy access:

- » **Inverse Chain Technology:**
<http://www.datto.com/technologies/inverse-chain-technology>
- » **Recovery Time Calculator:**
<http://tools.datto.com/rto/>
- » **Instant Virtualization:**
<http://www.datto.com/technologies/instant-virtualization>

About Webroot

Webroot delivers next-generation 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 and BrightCloud® Threat Intelligence Services protect tens of millions of devices across businesses, home users, and the Internet of Things. Trusted and integrated by market-leading companies, including Cisco, 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