CRYPTOLOCKER WARNING

Dangerous new virus

There is a dangerous virus/ransomeware that is hitting many small business customers. The virus comes in through users clicking on shipping email attachments that are actual viruses or through attacks that utilize exploiting older vulnerable java. The attack then installs without administrator rights on the system and begin to attack and go after its real payload: Your key files. ***It will look for any Office or database file and encrypt it. It will also search out across a network for any file across the network that is also an Office or Database file and encrypt it as well.*** It will then throw up a message on the screen asking for payment to decrypt the files.

Figure 1 - Encryption warning on screen

Currently it is difficult to prevent this with mere antivirus and post infection; it cannot be cleaned up with the normal tools such as malwarebytes or your normal antivirus tools.

Be proactive

Included in this document is a proactive setting to help protect your clients from infection. It uses group policy and software restriction policy (in a domain) and using local policy on a non-domain computer.

Be aware that antivirus may not protect your clients, nor the use of non-administrator on the personal computer. If your client is impacted your only remedy may be a backup. If you have no backup, you may need to use a Shadow File copy explorer tool to dig out copies of files.

Here's a copy of a blurb that Amy Babinchak's clients got from a LOB vendor as a warning/prevention guidance

> "We have been notified that two of our existing customers have been infected by a specific breed of Ransomware known as CryptoLocker that has been making the rounds this month.
>
> The malware uses social media or email as attack vectors, and users will see a message purported to be from FedEx, UPS, etc. with a tracking notice. The enticement for a user (especially a business who ships things using these carriers) is that it is legit and they open it. Boom. They are now infected.
>
> This malware will look at the local and network drives and shares, and will ENCRYPT files matching a set of extensions for common business applications. This includes office applications (Excel, Word, WordPerfect) and databases like access and Foxpro.
>
> Therefore (LOB app name) is directly affected and (LOB app2 name) is indirectly affected.
>
> For (bizapp name) the damage is fatal to the indexes. The software ceases to function and no recovery short of a file restore is possible. The underlying images stored in tiff are unaffected.
>
> For (bizapp2 name) the internal data files are safe, however word based documents, RTF files, Excel spreadsheets will all get corrupted. The virus operates on file extensions, so typical WordPerfect non-extension files are probably safe but WordPerfect forms with the .wpd extension will be corrupted/encrypted.
>
> Corrective actions involve: (1) Removal of the malware from all infected computers, and (2) restoration from a prior backup of all the files listed in the extension group listed here: *.odt, *.ods,

*.odp, *.odm, *.odc, *.odb, *.doc, *.docx, *.docm, *.wps, *.xls, *.xlsx, *.xlsm, *.xlsb, *.xlk, *.ppt, *.pptx, *.pptm, *.mdb, *.accdb, *.pst, *.dwg, *.dxf, *.dxg, *.wpd, *.rtf, *.wb2, *.mdf, *.dbf, *.psd, *.pdd, *.eps, *.ai, *.indd, *.cdr, ????????.jpg, ????????.jpe, img_*.jpg, *.dng, *.3fr, *.arw, *.srf, *.sr2, *.bay, *.crw, *.cr2, *.dcr, *.kdc, *.erf, *.mef, *.mrw, *.nef, *.nrw, *.orf, *.raf, *.raw, *.rwl, *.rw2, *.r3d, *.ptx, *.pef, *.srw, *.x3f, *.der, *.cer, *.crt, *.pem, *.pfx, *.p12, *.p7b, *.p7c

Here are two useful links that describe the malware in detail and provide IT departments with technical background for removal:

Emsis CryptoLocker Blog

http://blog.emsisoft.com/#sthash.yfNGRXbO.dpuf

and Bleeping Computer CryptoLocker

http://www.bleepingcomputer.com/virus-removal/cryptolocker-ransomware-information and

http://www.bleepingcomputer.com/forums/t/506924/cryptolocker-hijack-program/page-26#entry3165383

It is also worth noting that this malware is sophisticated enough to understand and bypass current anti-virus and anti-malware software. So even if the user is using strong protection, that will not be enough."

Actions if you have NOT been impacted

Communication: I highly recommend that you warn your clients of this attack. Begin first by sending a proactive email explaining the threat and warning people to be careful on opening up attachments.

> *Just a heads up – we're seeing at least one small business a week being impacted by the CryptoLocker virus. It is a virus that encrypts Office documents on your local computer as well as files on the network. The only recovery is to restore from backup.*
>
> *Be very careful in opening up any attachment as most report that it was an attachment to a FedEx or UPS shipping notice or a Banking email.*
>
> *Once infected, you will get a popup saying your files are encrypted and demanding a ransom to get them back.*

While we have filters on the email, it's still extremely important to be careful. Additionally we will be putting in place a measure to prevent this virus from launching from a workstation should it make its way into your systems.

Preventative Workstation protection: This virus launches from a specific location on the workstation, thus it's recommended to add a group policy setting to block it from Windows Vista/7/8 and from XP. Use software restriction policies as follows:

Windows 7:

You can use Software Restriction Policies to block executables from running when they are located in the %AppData% folder, or any other folder.

File paths of the infection are:

C:\Users\User\AppData\Roaming\{213D7F33-4942-1C20-3D56=8-1A0B31CDFFF3}.exe (Vista/7/8)

C:\Documents and Settings\User\Application Data\{213D7F33-4942-1C20-3D56=8-1A0B31CDFFF3}.exe

So the path rule you want to basically setup is:

Path: %AppData%*.exe
Security Level: Disallowed
Description: Don't allow executables from AppData.

In addition there is a further subfolders that should be set for Windows Vista and higher:

Group policy for Windows XP

Start by setting up a group policy object for Windows XP.

Click on start, administrative tools, Group policy management:

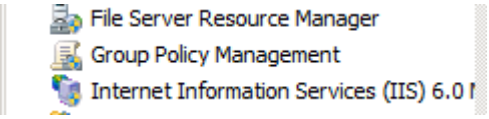
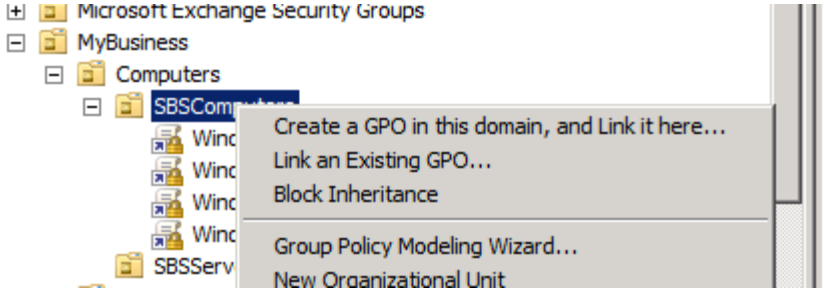


Figure 2 - Launch group policy management

For SBS 2008 and SBS 2011 there are preset up GPOs and WMI filters. You want to build a new GPO in order to track the specific deployment. Expand the domain name until you see the policies. Go underneath the MyBusiness OU, then Computers, then SBSComputers and right mouse click and click on "Create a GPO in this



domain and link it here

First we will set up XP policies:

Call your new policy, CryptoLocker XP or something as descriptive and click okay.

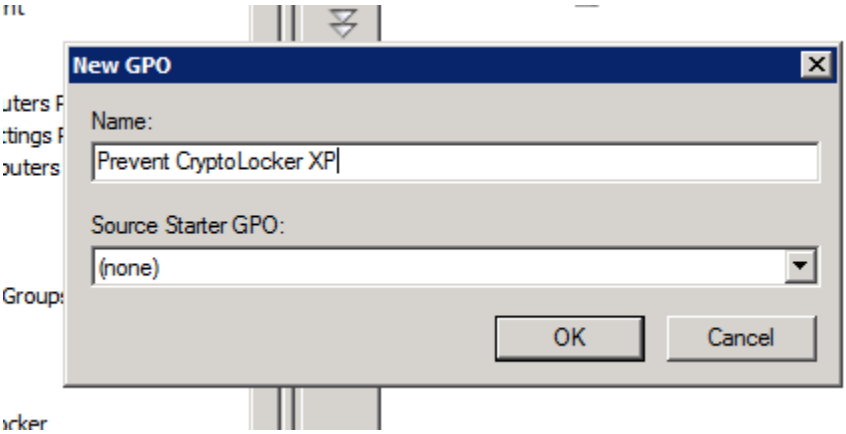


Figure 4 Name your GPO

In the group policy object you just created, right mouse click and click on edit

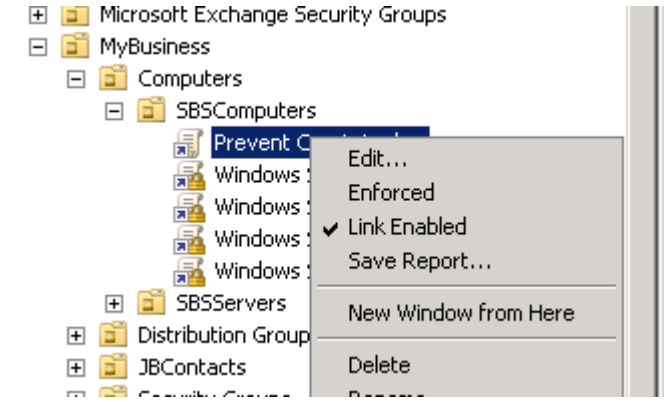


Figure 5 Edit the GPO

Navigate to Computer Configuration >Policies>Windows Settings>Security Settings >Software Restriction Policies

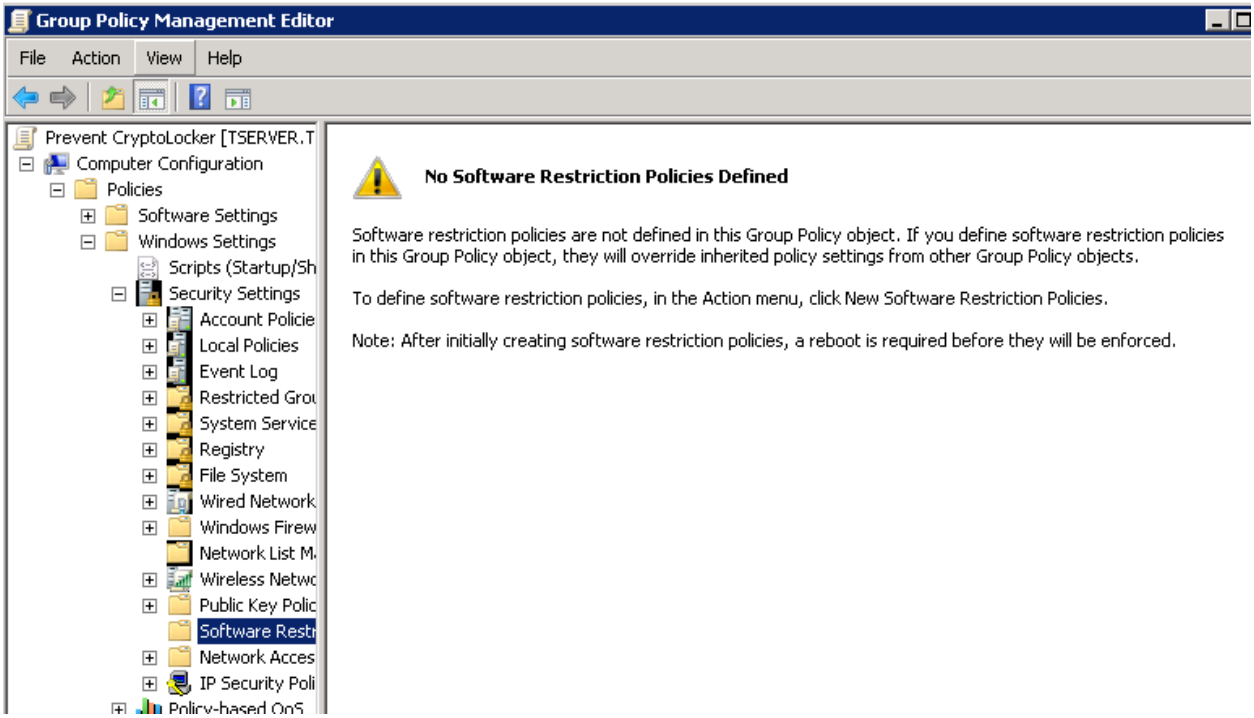


Figure 6 Setting the Software Restriction Setting

Right mouse click and click on “New Software Restriction Policies”

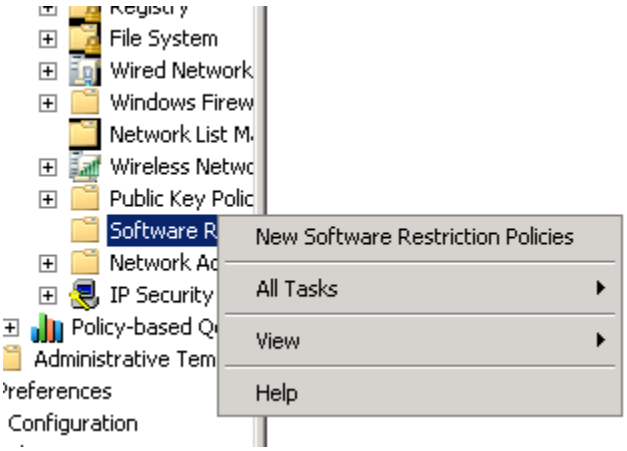


Figure 7 - New Software Restriction Policy

The wizard will open up a new section of Group policy where you will see “Additional rules” as shown below and noted http://technet.microsoft.com/en-us/library/cc781337(v=WS.10).aspx

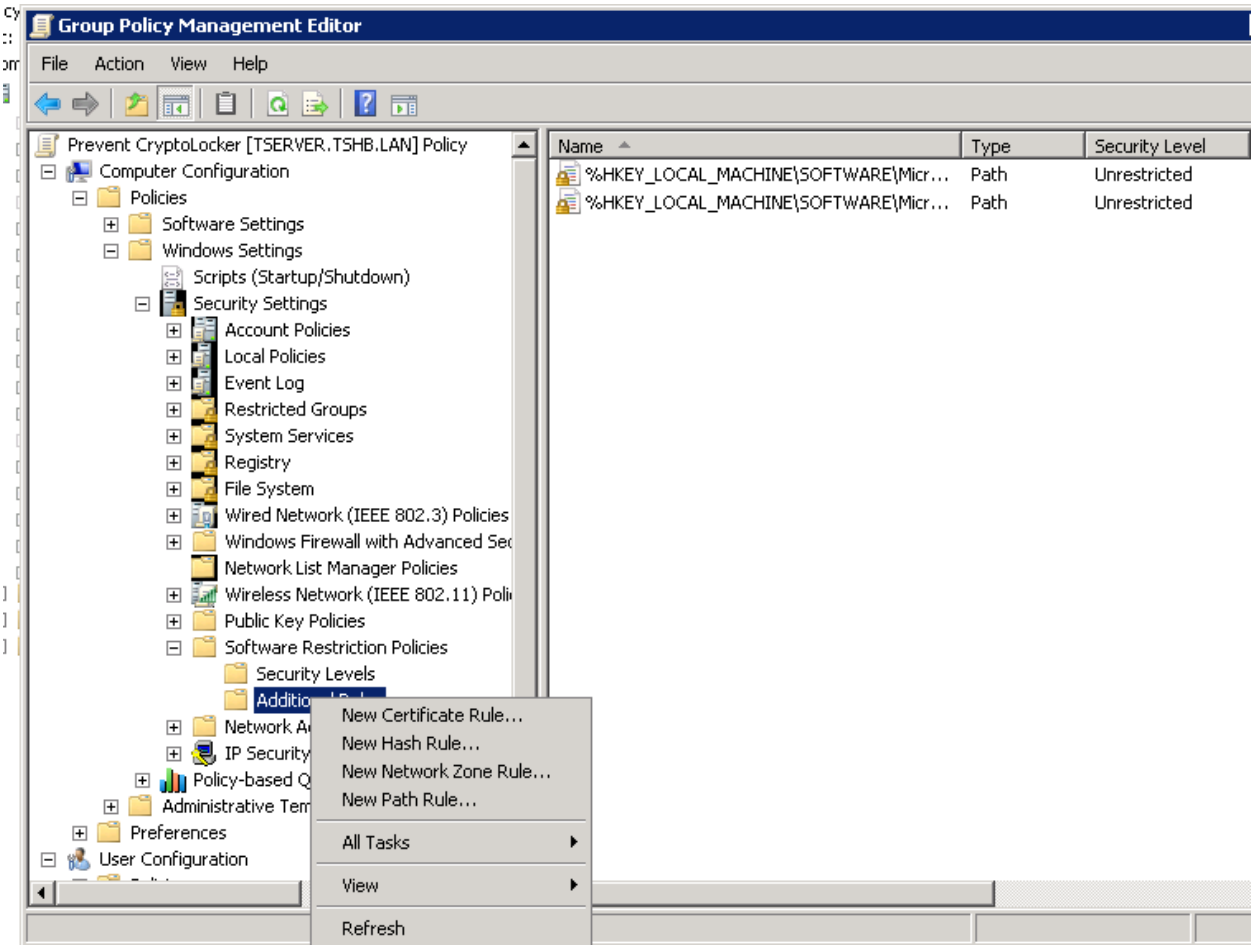


Figure 8 - Set up additional rule

Right mouse click on Additional rules and click on “New Path Rule”

Enter the following information:

Path: %AppData%*.exe

Security Level: Disallowed

Description: Don't allow executables from AppData

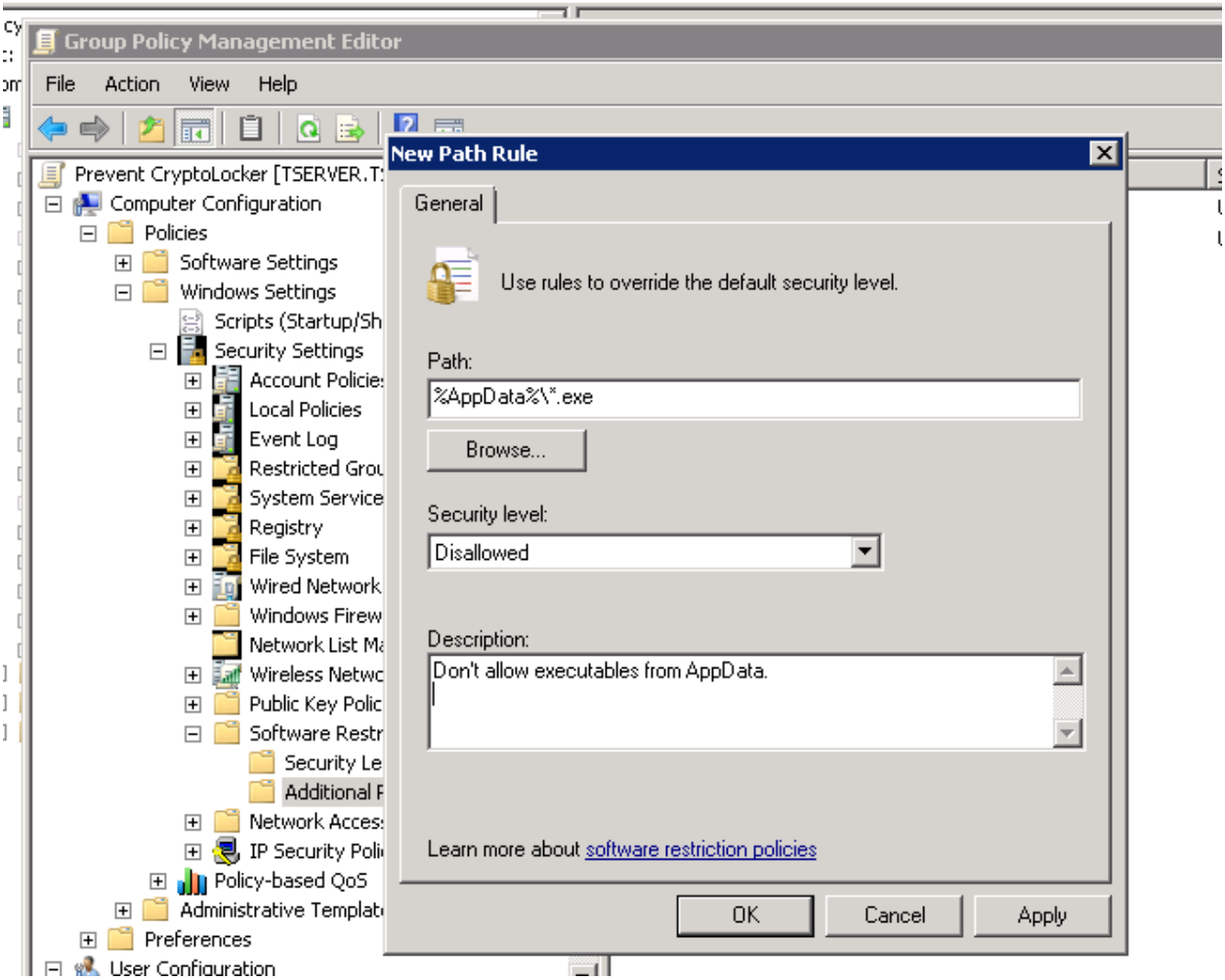


Figure 9 set up rules

Click Okay.

Now do a second one for the subfolders:

Path: %AppData%**.exe
Security Level: Disallowed
Description: Don't allow executables from AppData

It should now look like this:

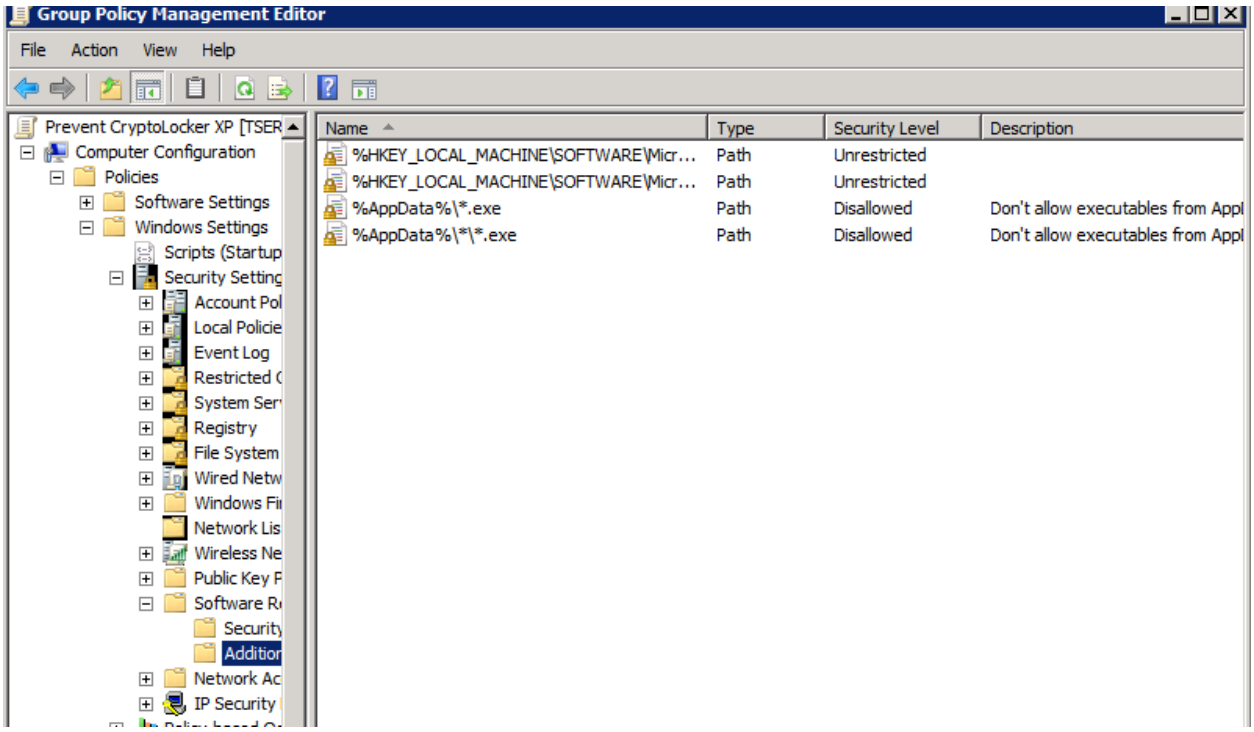


Figure 10 - Path restriction

Let's continue on and do the same for the additional locations to block executable running from zipped attachments (which is how most infections occur)

Block executables run from archive attachments opened with WinRAR:

Path: %Temp%\Rar**.exe
Security Level: Disallowed
Description: Block executables run from archive attachments opened with WinRAR.

Block executables run from archive attachments opened with 7zip:

Path: %Temp%\7z**.exe
Security Level: Disallowed
Description: Block executables run from archive attachments opened with 7zip.

Block executables run from archive attachments opened with WinZip:

Path: %Temp%\wz**.exe
Security Level: Disallowed
Description: Block executables run from archive attachments opened with WinZip.

Block executables run from archive attachments opened using Windows built-in Zip support:

Path: %Temp%*.zip*.exe
Security Level: Disallowed
Description: Block executables run from archive attachments opened using Windows built-in Zip support.

Your final view will look as follows:

Name	Type	Security Level	Description
%AppData%*.exe	Path	Disallowed	Don't allow executables from Appl
%AppData%**.exe	Path	Disallowed	Don't allow executables from Appl
%HKEY_LOCAL_MACHINE\SOFTWARE\Micr...	Path	Unrestricted	
%HKEY_LOCAL_MACHINE\SOFTWARE\Micr...	Path	Unrestricted	
%Temp%\Rar**.exe	Path	Disallowed	Block executables run from archiv
%Temp%\7z**.exe	Path	Disallowed	Block executables run from archiv
%Temp%\wz**.exe	Path	Disallowed	Block executables run from archiv
%Temp%*.zip*.exe	Path	Disallowed	Block executables run from archiv

Figure 11 - Block locations

Now close this policy and set the WMI filter. In the Small business server networks you have preset WMI filters. If you have migrated from a SBS network you should have these as well.

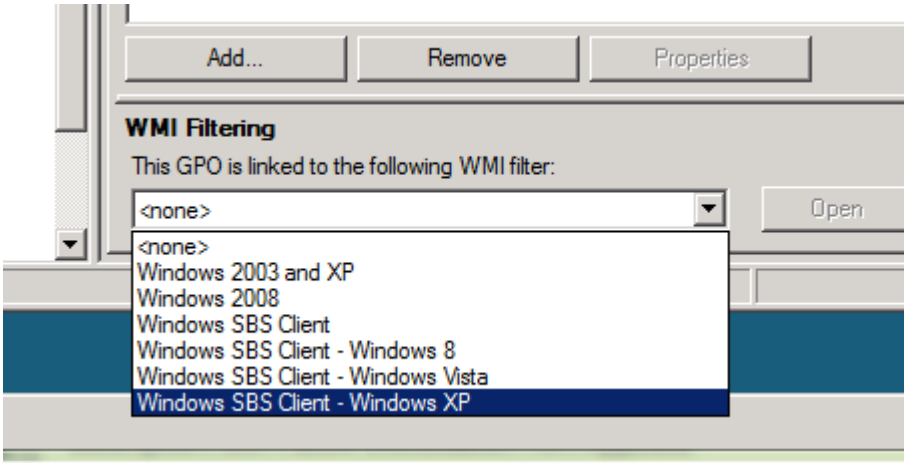


Figure 12 - Choose XP

Choose the Windows XP policy.

If you do not have WMI filters they can be set up as follows:

Go down to the WMI filter section and choose New

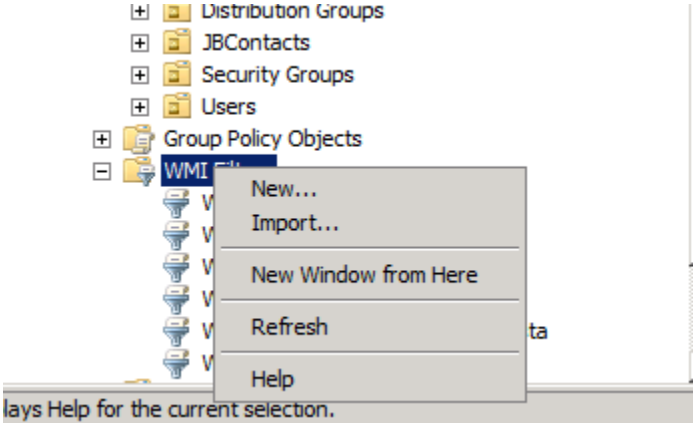


Figure 13 Setting up WMI filter

Name the Filter descriptive and click Add

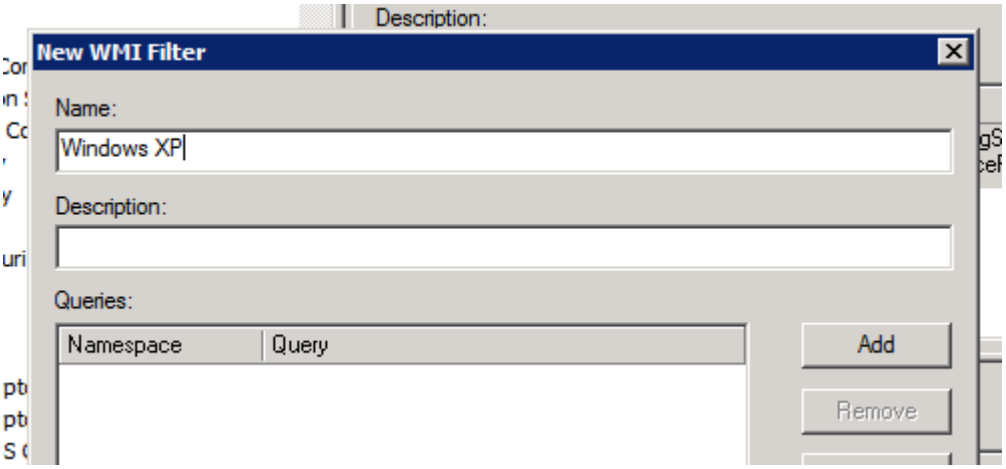


Figure 14 Set up WMI filter

In the query section enter the following value:

> select * from Win32_OperatingSystem Where Version>='5.1.2600' and '6.0.6000'>Version and ServicePackMajorVersion>=2

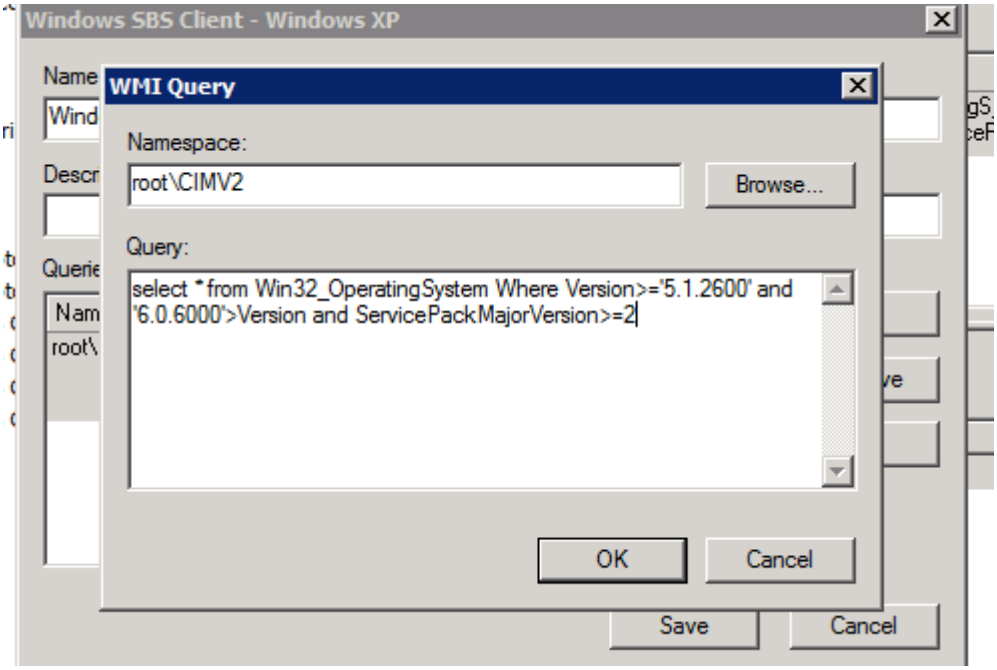


Figure 15 WMI filter

It should look as above.

IF you have an issue with a line of business application not liking this policy – in particular on Windows XP machines, you can set the WMI filter to have this policy only apply on Windows 7 machines. But try setting the policy with no WMI filter initially and alert your clients to report if there are applications that do not like this setting. If they do not, we can go back and add application exclusions on a per app basis.

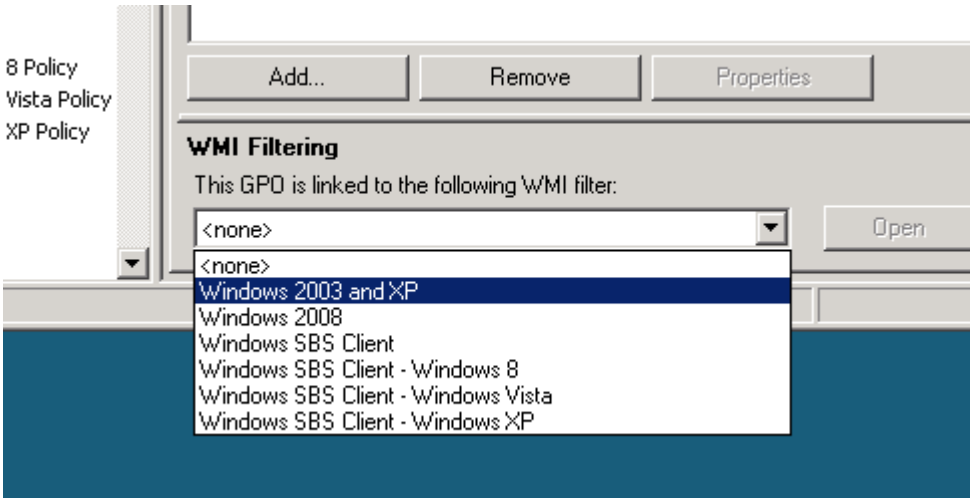


Figure 16 Choose WMI filter if needed

Windows Vista and higher

For Windows 7 do the same sequence of setting up Group policy as shown above.

Path: %AppData%*.exe
Security Level: Disallowed
Description: Don't allow executables from AppData

And

Path: %lAppData%**.exe
Security Level: Disallowed
Description: Don't allow executables from AppData

Block executables run from archive attachments opened with WinRAR:

Path: %Temp%\Rar**.exe
Security Level: Disallowed
Description: Block executables run from archive attachments opened with WinRAR.

Block executables run from archive attachments opened with 7zip:

Path: %Temp%\7z**.exe
Security Level: Disallowed
Description: Block executables run from archive attachments opened with 7zip.

Block executables run from archive attachments opened with WinZip:

Path: %Temp%\wz**.exe
Security Level: Disallowed
Description: Block executables run from archive attachments opened with WinZip.

Block executables run from archive attachments opened using Windows built-in Zip support:

Path: %Temp%*.zip*.exe
Security Level: Disallowed
Description: Block executables run from archive attachments opened using Windows built-in Zip support.

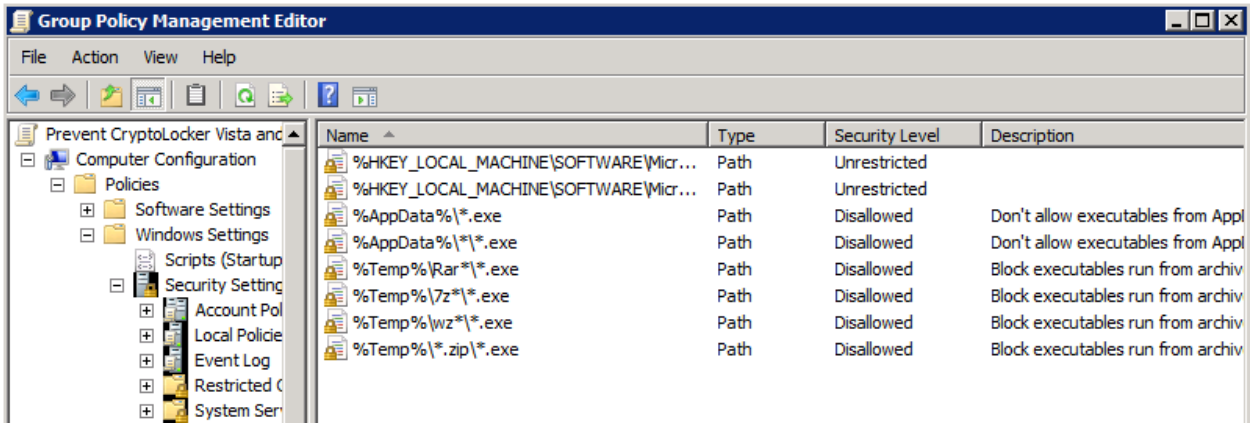


Figure 17 Set the Vista and higher policy

When you are complete it should look as above. Again close the policy you are working on.

This time choose the Windows Vista filter or set a WMI filter as follows:

select * from Win32_OperatingSystem Where Version>='6.0.6000'

So that it looks as follows:

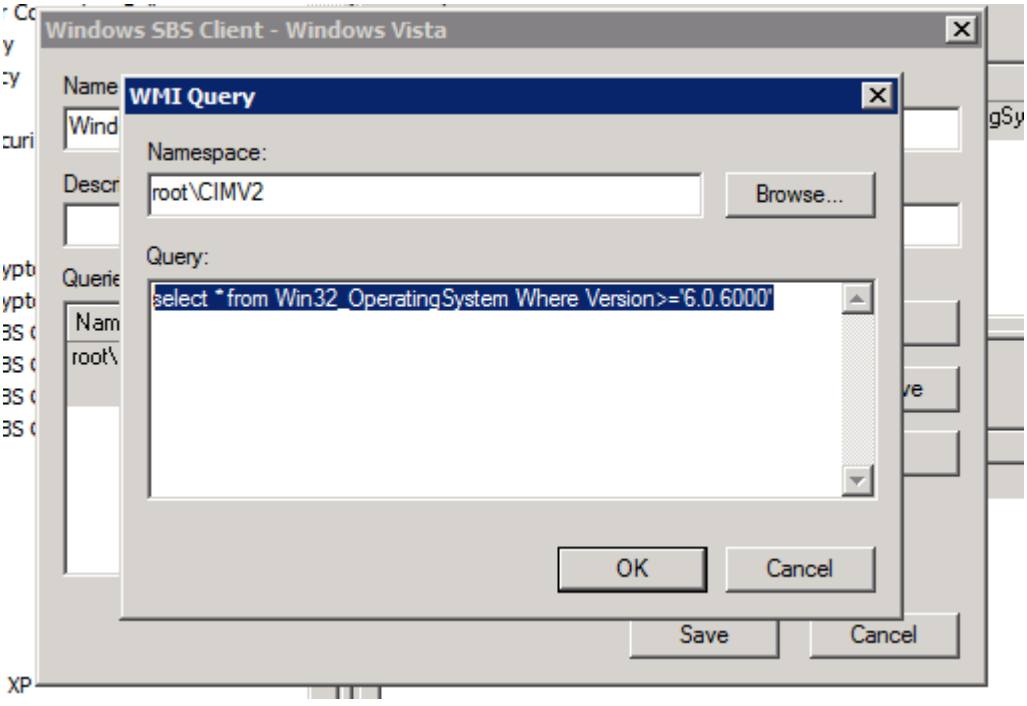


Figure 18 WMI filter

When you are complete you should have two policies, with WMI filtering set up.

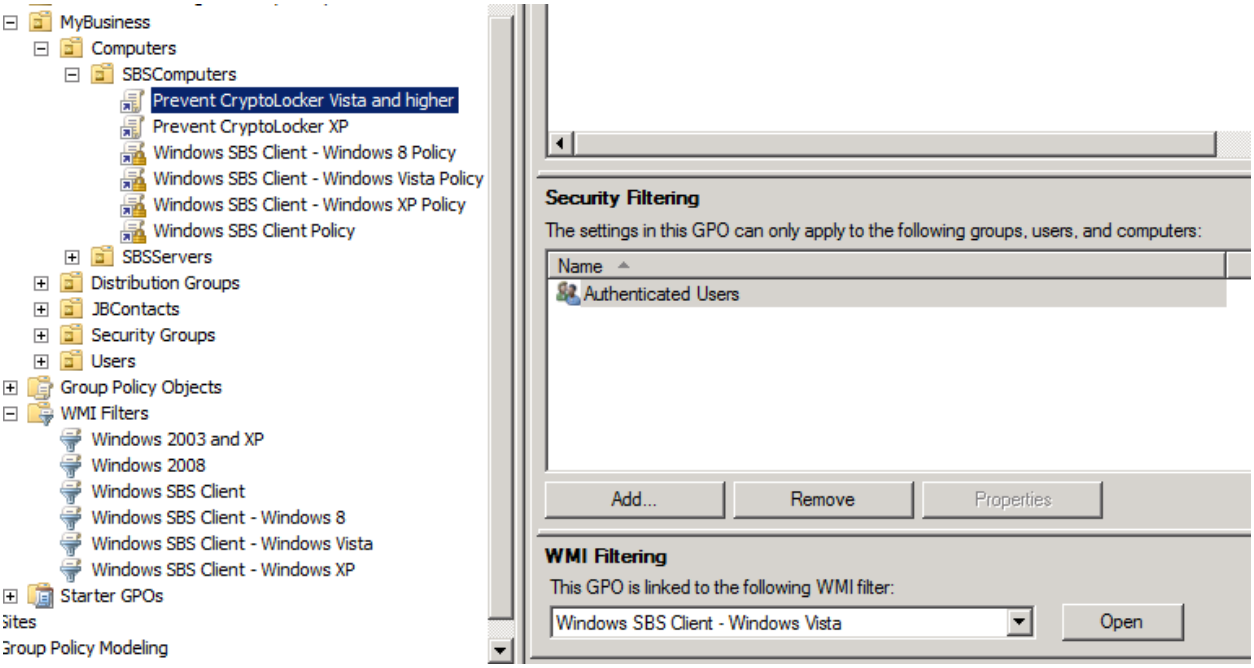


Figure 19 - Final policy

Without a domain

For standalone workstations, you can use the local security policy and set software restrictions as well.

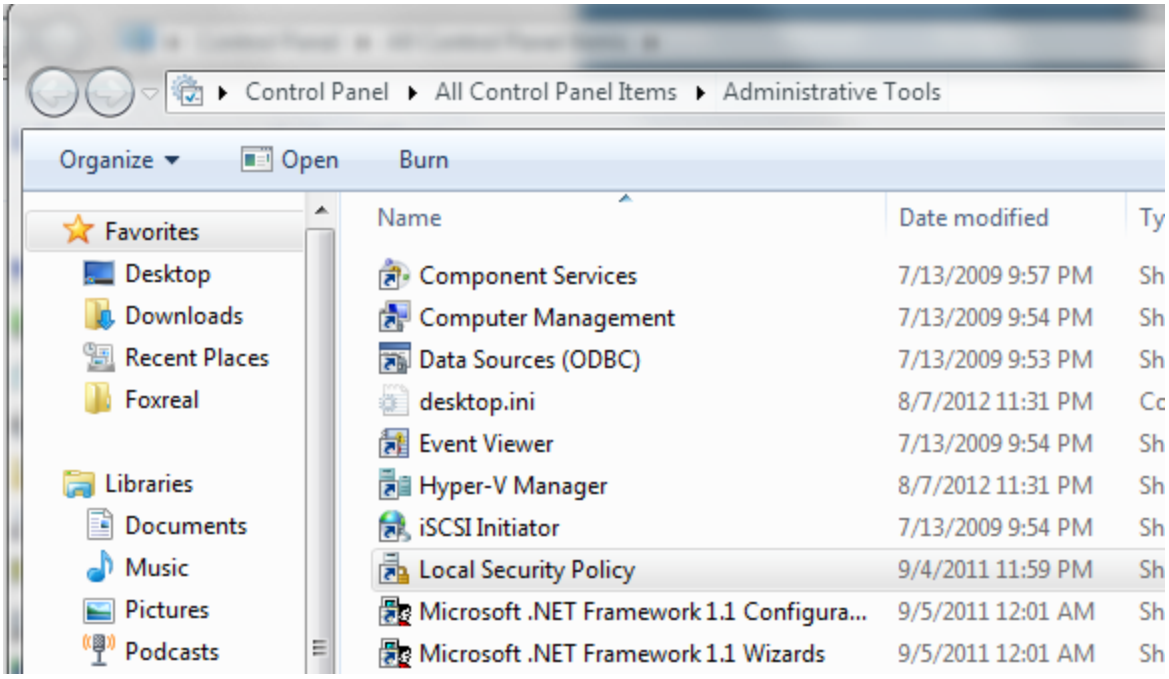


Figure 20 Local security policy

Launch the local security policy in the control panel/administrator tools.

Find the software restriction policy section

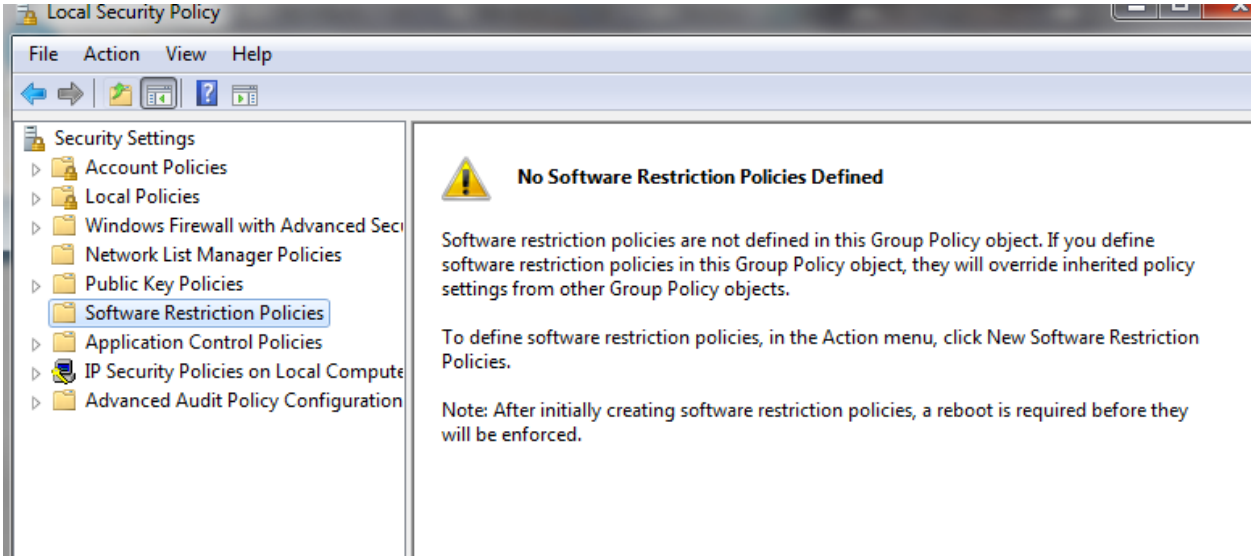


Figure 21 SRP in a standalone workstation

Right mouse click on Software restriction policy and click on add new

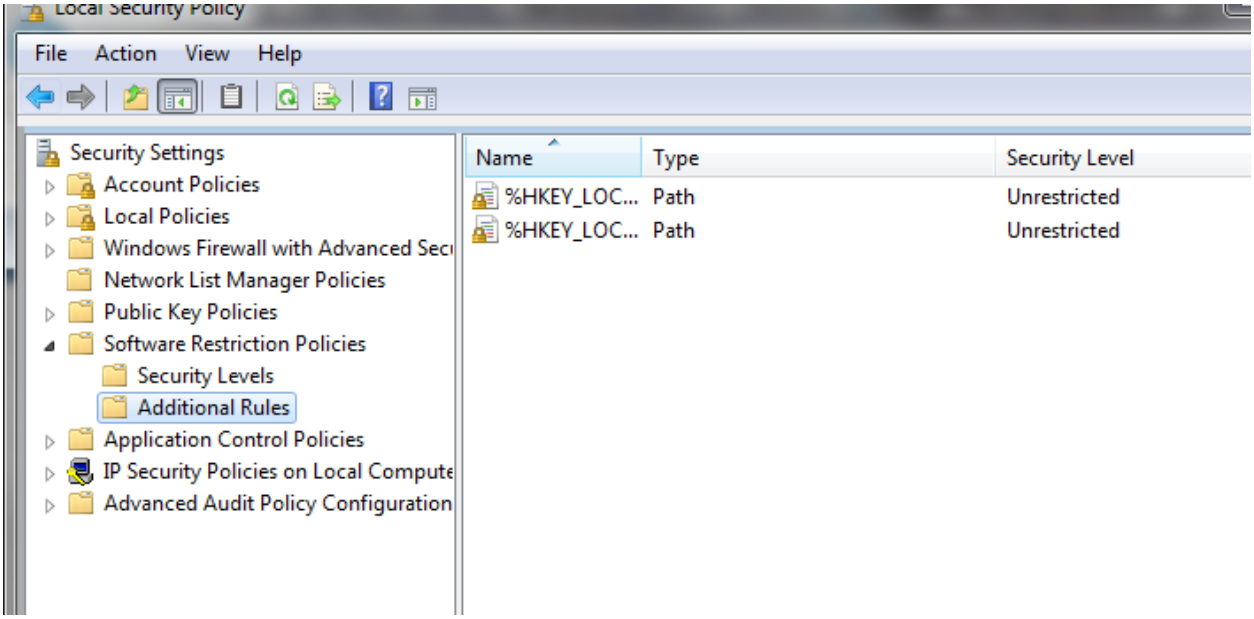


Figure 22 Set up SRP

Now right mouse click on additional rules and click on add new path rule. Just as before place the settings as follows for Windows XP:

Path: %AppData%*.exe
Security Level: Disallowed
Description: Don't allow executables from AppData

And

Path: %AppData%**.exe
Security Level: Disallowed
Description: Don't allow executables from AppData

Block executables run from archive attachments opened with WinRAR:

Path: %Temp%\Rar**.exe
Security Level: Disallowed
Description: Block executables run from archive attachments opened with WinRAR.

Block executables run from archive attachments opened with 7zip:

Path: %Temp%\7z**.exe
Security Level: Disallowed
Description: Block executables run from archive attachments opened with 7zip.

Block executables run from archive attachments opened with WinZip:

Path: %Temp%\wz**.exe
Security Level: Disallowed
Description: Block executables run from archive attachments opened with WinZip.

Block executables run from archive attachments opened using Windows built-in Zip support:

Path: %Temp%*.zip*.exe
Security Level: Disallowed
Description: Block executables run from archive attachments opened using Windows built-in Zip support.

You will need to reboot the computer to have them take effect.

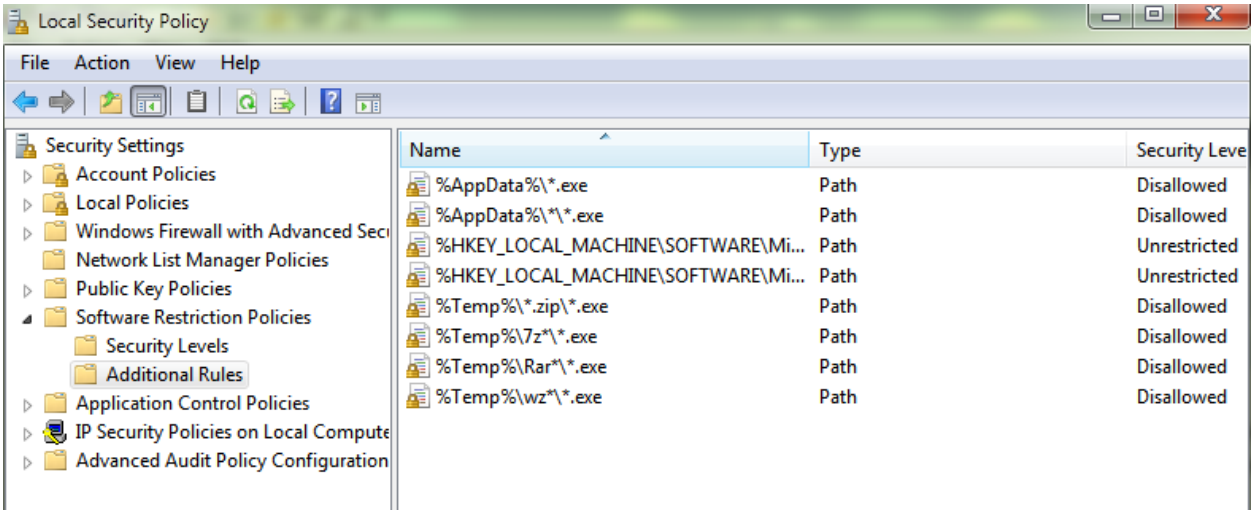


Figure 23 SRP set up

Additional path locations

You can additional path locations such as appdata local, and locallow in Windows Vista and higher to protect those as well, but be aware that there may be impact to line of business apps in these locations. For example remote access tools such as Copilot.com will be blocked in the local file location is blocked.

You may optionally wish to block %localappdata% as an additional location and make it just applicable to the Windows 7 machines.

Additional steps

It's possible that you can prevent encryption of the files by blocking the command and control servers using firewall or web based filtering. But be aware that we will always be one step behind the attackers so this may not work.

As noted from
http://kc.mcafee.com/resources/sites/MCAFEE/content/live/PRODUCT_DOCUMENTATION/24000/PD24786/en_US/McAfee%20Labs%20Threat%20Advisory%20-%20Ransom-Cryptolocker.pdf

As of 10/15/2013 the list of CC servers are:

asrktkfsixcyosb.org
sbfuwsxasjkp.net
emixfepanfsy.co.uk

fkdovmdntspl.info
fqswanunybwt.com
gonnqvibfotg.net
qnkhpddfmtsm.biz
eaffoijeveky.ru
soudpmiyvxmd.org
gbpboroxfiep.co.uk
ofoauksakmgs.info

crjxtpyytwxf.com
qgyvutxttqaj.net
estttyesdbrv.biz
uwuexnaukgiy.ru
vupuoseotond.org
wxfaxwfotkcp.co.uk
xvaqocjidsht.info
soywduppiyvf.com
tmtntatjrhbj.net
upjsdeujrdpv.biz
vnejtjydblua.ru
ynnivqvmcyxxr.org
mxoguylttevli.co.uk
avlpfgiqwdudk.info
ngmneoxxoisqk.com
udsmjlwhfkmeg.net
intkitmowpkrw.biz
vlqtsbjlaojjg.ru
jvrrrjysrthwg.org
hjxywcvnbotlg.co.uk
ifylakjpsgyhf.info
irvggrirvsqqy.com
jnwsjavtnkvmh.net
dyddkwwieairg.biz
euepnfkkvrnnf.ru
ehbktmjmyefwg.org
fdcwwuwoqvkso.co.uk
fxcyhrpfigvcu.info
sidwgwvsyqlxu.com
hdauthcpbwblw.net

unbssmidrhqhn.biz
bnhdumqalrkij.ru
oxibtrwnccaej.org
dsfyhcdkeiprs.co.uk
qdgwghjxusfnj.info
ntmpidpuhvjxm.com
opnclitaxswlu.net
pykluscfamoho.biz

qulxxxgkqjcun.ru
jjrtvxqpkhxem.org
kfsgyduubelru.co.uk
loppindadxdnv.info
mkqclshftuqbu.com
tnfhkwqywydsb.net
hxgfjfggoebgr.biz
uvdotgvjluqgb.ru
igemsolqdaotb.org

But be aware as noted in http://blog.emsisoft.com/2013/09/10/cryptolocker-a-new-ransomware-variant/#sthash.ia2QByWF.E15vKKdG.dpbs "the malware will start generating seemingly random domain names using a domain generation algorithm. This is done by creating a seemingly random string of characters based on the current system time and prepending it to one of the following seven possible top level domains" So this method is probably not viable and probably best left to be attempted by DNS providers and ISP.

As noted by Michael Pope "for those using Kaseya, you can use the Application Blocker feature (Agent > Protection > Application Blocker) to block the file {213D7F33-4942-1C20-3D56=8-1A0B31CDFFF3}.exe from running on machines."

Review for issues

Now that these rules are set up, review the event logs on the client for event 866 Software restriction policies for indicators that the rules are blocking too much and may need to be adjusted or an application needs whitelisting to work.

> Access to C:\Users\Susanb\AppData\Local\Temp\HelperShell.exe has been restricted by your Administrator by location with policy rule {6012feea-fdf2-49ca-a380-d5f9512d7426} placed on path C:\Users\Susanb\AppData\Local**.exe.

Review how your backups are set up

Given that your only remedy may be your backups, Philip Elder recommends reviewing how they are set up:

One of the things we have done from the get-go when it comes to setting up ShadowProtect to stream backups to either a drive set connected to a standalone Hyper-V host or to the standalone DC in a Hyper-V cluster setting is to set the shares to allow the Domain Admin MOD.

Inheritance on the folder's NTFS permission set is removed/copied out then Domain Users/Machine Users group will get removed altogether.

We do this for a number of reasons

Users cannot connect to the ShadowProtect images

They are password protected and are using at least AES128bit

Users cannot delete the images

While we are into our client's servers on a regular basis sometimes the occasional domain admin account password will expire in the interim.

ShadowProtect will start failing to back up to the shared folder as a result of not being able to log on so a small bonus in the mix.

We are seeing CryptoLocker problems abound lately where someone clicks on a link in an e-mail or is drawn to a compromised site. What that means is that _any_ file/folder set the user has permissions to access and modify may end up encrypted by the malware.

The _only_ way to "recover" from this situation is via Shadow Copies or backup.

If the backup drive and/or backup folder destinations for those ShadowProtect backup files, or any other product that lays down files for backup, is open for users to access then we all know what can happen.

Point of order: Any backup product that uses the volume snapshot service should have its backup times staggered over the Volume Shadow Copy snapshots as having two snapshots running simultaneously could end up with data toast on both sides.

Actions if you have been impacted

Determine where backups are stored and how well the backups are. Ensure that encrypted data does not also get backed up. You may need to remove the backup drives temporarily as you work to clean the systems before putting the data back online.

Determine how bad the infection.

Download a tool to scan the computer systems to determine how many files are encrypted: http://download.bleepingcomputer.com/grinler/ListCrilock.exe This file will open up a notepad file and list those files that are now encrypted.

Do not pay the ransom. If your client demands you do so, ensure that you use a prepaid debit card so as to not add identity theft to the issues you are facing.

Advise your client that there is no antivirus program that will clean the files and put them back. The attackers are using normal encryption to use our own computers against us.

Attempt to clean the system

1. Boot to safe mode
2. Browse registry and navigate to Run key under:

Computer\HKEY_Current_User\Software\Microsoft\Windows\CurrentVersion\Run

3. Delete any entry to an exe file that appears to be suspicious
4. Navigate to physical path of these files and delete them

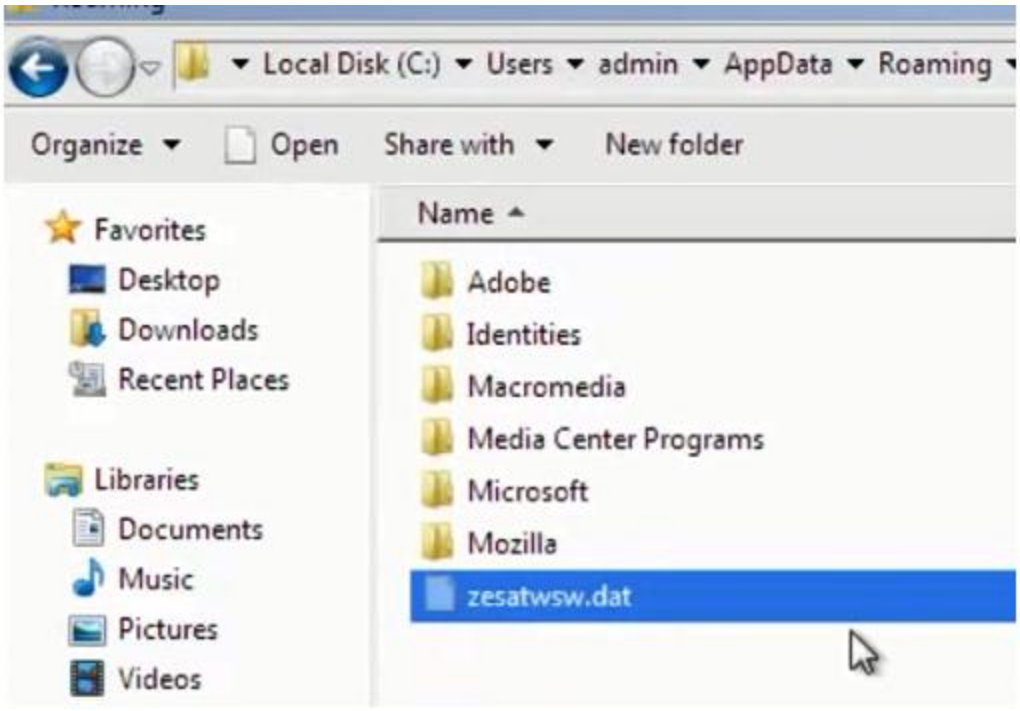


Figure 24 Delete infection points

Note: most of them are in Roaming folder

5. Reboot
6. Delete bmp file that virus left on desktop and change background to regular windows.
7. In windows 7 system restore by default is turned “ON” on the C drive for system settings and files
8. Right click folder affected and click “restore previous versions”

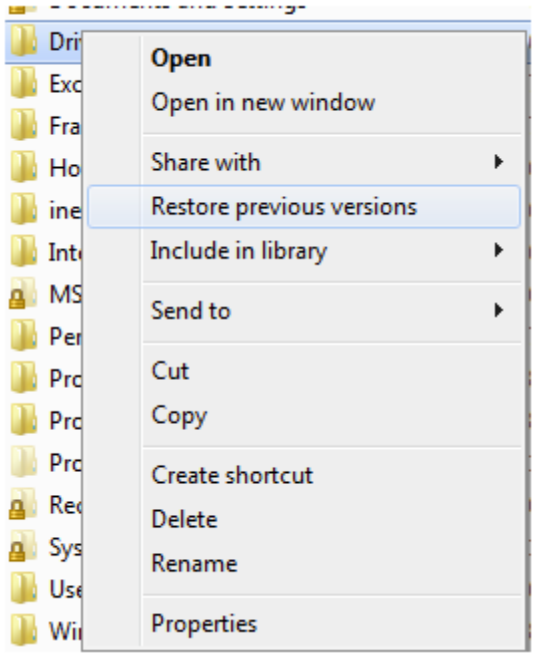
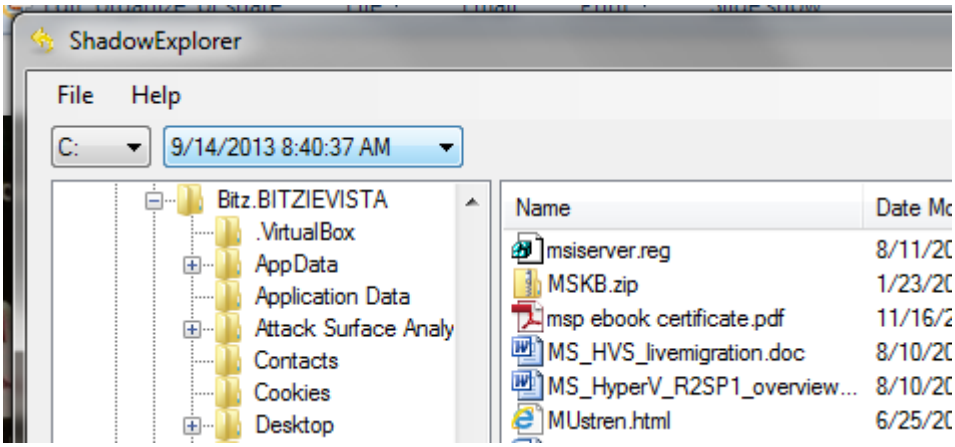


Figure 25 Restore from shadow copies on Windows 7

If this is unavailable, you may need to use Shadow Explorer to recover the files
http://www.shadowexplorer.com/downloads.html



Please note, normal antivirus will not remove this, nor will you be able to unencrypt the files. I cannot stress this enough – the only recovery at this time is to ensure you have a backup that you can get to that is not impacted.

9. Use copy option to restore to a different location

Please note, you may need to remove the drive to an enclosure to scan and edit while the system is not mounted.

But you need to ask yourself if you are truly assured that you have cleaned the system. Without totally rebuilding or rolling back to an image from known good sources, you will always question the health and security of this system.

Talk to your client. Go with your gut. If you do not feel that it is completely secure, (and it probably isn't) rebuild the machine.

From "Help: I got Hacked. Now what do I do?" **http://technet.microsoft.com/en-us/library/cc512587.aspx**

"You can't clean a compromised system by removing the back doors. You can never guarantee that you found all the back doors the attacker put in. The fact that you can't find any more may only mean you don't know where to look, or that the system is so compromised that what you are seeing is not actually what is there."

Post disaster review

Once you get your client back into somewhat working condition, sit them down and review what proactive issues need to be done.

Identify their key business data

Attackers are going after whatever it takes to get to the data and that may be the platform, the applications, the users, the application frameworks... Even the lowest rungs of attackers now possess a lot of useful tools & attacks and they are far more successful than they ought to be.

If there is a takeaway from that statement, it's this: Anybody with interesting data should be taking positive steps to protect it. For me, that means:

1. Classify your data and know where it's stored. Use a rating of low/medium/high sensitivity and consider applying different controls based on which tier the data fits into. This could be as simple as 'public data' and 'sensitive data' -- but it's the first step.

2. Backups. Backup onsite. Backup offsite. Test your backups regularly. We all know how many times you have a customer with no backup of important data or a customer whose backup fails to restore. Backup anything that it would hurt your business to lose. (Note: This is the first place that classification is important. If you don't know where the data is and how sensitive it is, you don't know what to back up and where to back it up from.) If you need to add client workstation backup there are various ways including ShadowProtect or the use of Storage Server 2008 R2 Essentials to a SBS domain, or the upcoming release of

Windows 2012 r2 whereby the Essentials role can be added to a normal Windows domain and be used as a client backup as well.

3. Access Control Lists. Unless you're OK with everybody having that data, everybody shouldn't have access to it. (And everybody definitely shouldn't have full control or write access to it.) Review your networks to determine how much "Everyone Full Access" is used - http://4sysops.com/archives/find-shares-with-powershell-where-everyone-has-full-control-permissions/ or http://thephuck.com/server-management/list-all-shares-with-everyone-having-fullcontrol-access/ or you can use the Get-ACL command - http://blogs.technet.com/b/heyscriptingguy/archive/2009/09/14/hey-scripting-guy-september-14-2009.aspx , or Solarwinds tool from http://www.solarwinds.com/products/freetools/permissions_analyzer_for_active_directory/ or AccessEnum http://technet.microsoft.com/en-us/sysinternals/bb897332.aspx

4. Especially with more and more Cloud services in use, review your use of Encryption at the client and add encryption at rest and encryption in flight.

5. Review what the client did to get infected. If they clicked on an attachment, add email filtering. If they had outdated Java on their systems, remove old outdated versions of Java by using a tool called JavaRA http://sourceforge.net/projects/javara/ or http://singularlabs.com/software/javara/