CRYPTOLOCKER TOOLKIT

Ways to add exemptions

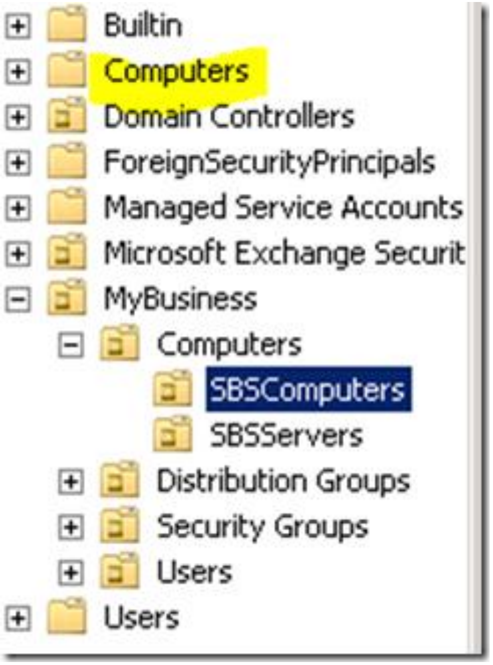
You've downloaded the CryptoLocker Toolkit and it's working to block executables. Too well. As many have found, applications that install may use the user's profile to download and launch the executable. There are several ways to approach the issue.

Group policy OU way

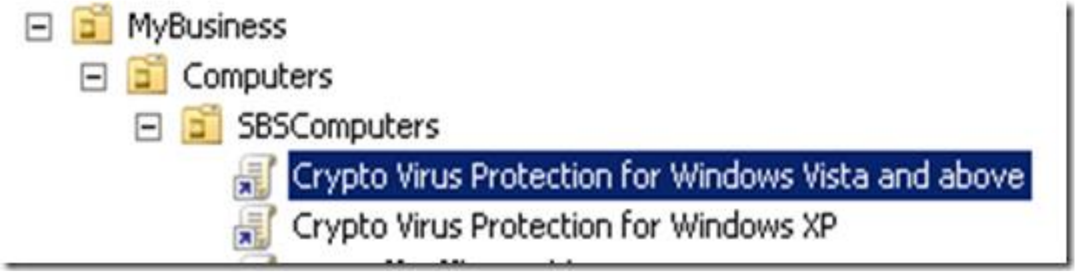
One way to temporarily allow installations of Office 2010 and 2013 and other legitimate software is to move the computer into a new OU (organizational unit) and remove the PC from having the group policies apply to it. This is handy when you are installing a new PC into the network and need to install many items. Move them into a temporary OU called "Install" and ensure that there are no group policies applied. Once you have installed all software, then move the computer into the proper OU.

On the third tier blog you can see how easy this is: http://www.thirdtier.net/2013/10/how-to-move-computers-in-and-out-of-a-group-policy/

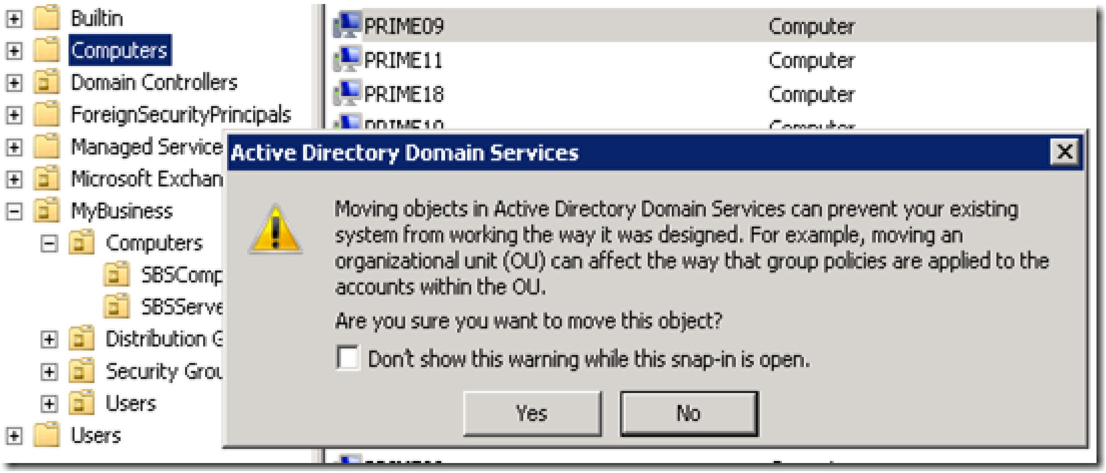
> Group Policy structures are mostly a mirror of your Active Directory structure with one notable exception – Containers aren't included, only Organizational Units. This is because Group Policy's can't be applied to Containers.
>
> Our AD looks like this. The objects with the file inside the folder are the OU's. The ones without them are the Containers. In our example the highlighted in yellow Computers is a Container and highlighted in blue SBSComputers is an OU.



And our GPO structure looks like this. Our GPO is applied to the SBSComputers OU.


MyBusiness
Computers
SBSComputers
Crypto Virus Protection for Windows Vista and above
Crypto Virus Protection for Windows XP

If we need to install software to the computer that is blocked by this policy, then we simply move the computer that we are working on into the Computers container. We install and configure our software. Then we move it back. To move a computer just drag and drop it from the OU it is in into the Computer container. You'll get the message below reminding you that this will prevent group policies from applying to that computer.



Active Directory Domain Services

Moving objects in Active Directory Domain Services can prevent your existing system from working the way it was designed. For example, moving an organizational unit (OU) can affect the way that group policies are applied to the accounts within the OU.

Are you sure you want to move this object?

□ Don't show this warning while this snap-in is open.

On the computer from an elevated command prompt run gpupdate /force to update the policies applied to the computer. Now you can proceed to install the software package. When you are done installing simply drag the computer from the Computers container back into the OU from where it came. You can run gupdate /force again on that computer to update the policies back onto the computer again.

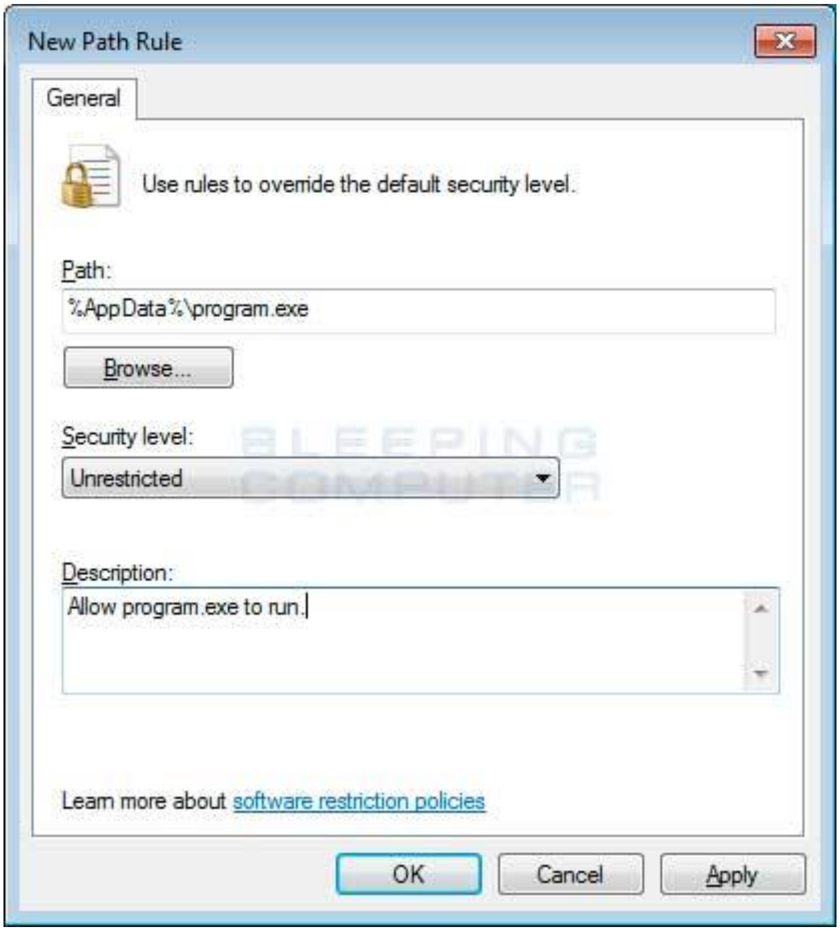
It should take you much less than 5 minutes to perform this task. The benefits of Group Policy far outweigh the inconvenience of this procedure.

Building exception rules

The second way to work around the issue of letting legitimate software be installed it to build whitelist rules. As noted in http://www.thirdtier.net/2013/10/exempting-a-program-from-software-restriction-policies/

> But if you find that you have a repetitive task that requires you to move computers in and out of the policy you may be better off exempting the .exe from the policy. A good explanation of how to do this has been provided at *http://avosec.com*. I've copied it here for you.
>
> ## How to allow specific applications to run when using Software Restriction Policies
>
> *If you use Software Restriction Policies, or CryptoPrevent, to block CryptoLocker you may find that some legitimate applications no longer run. This is because some companies mistakenly install their applications under a user's profile rather than in the Program Files folder where they belong. Due to this, the Software Restriction Policies will prevent those applications from running.*
>
> *Thankfully, when Microsoft designed Software Restriction Policies they made it so a Path Rule that specifies a program is allowed to run overrides any path rules that may block it. Therefore, if a Software*

Restriction Policy is blocking a legitimate program, you will need to use the manual steps given above to add a Path Rule that allows the program to run. To do this you will need to create a Path Rule for a particular program's executable and set the Security Level to ***Unrestricted*** *instead of Disallowed as shown in the image below.*



New Path Rule
General
Use rules to override the default security level.
Browse...
Learn more about software restriction policies
OK
Cancel
Apply

Path: %AppData%\program.exe

Security level: Unrestricted

Description: Allow program.exe to run.

Once you add these Unrestricted Path Rules, the specified applications will be allowed to run again.

Some of the typical exclusions you will need to build are for Chrome, and for Office installs:

By default when you enable software restriction policies, you will see certain paths already with prebuilt exclusions. These are not needed to be added in group policy.

%HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SystemRoot% Path Unrestricted

%HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\ProgramFilesDir% Path Unrestricted

To build these rules do the following:

In your Group Policy Management editor, go to the Group policy object section and edit your built policies.

In Computer configuration>Policies>Windows Settings>Security Settings, find the Software Restriction Policy Section. Click on Additional rules and then right mouse click and click on New path rule.

I would recommend only placing exceptions for the software you have installed.

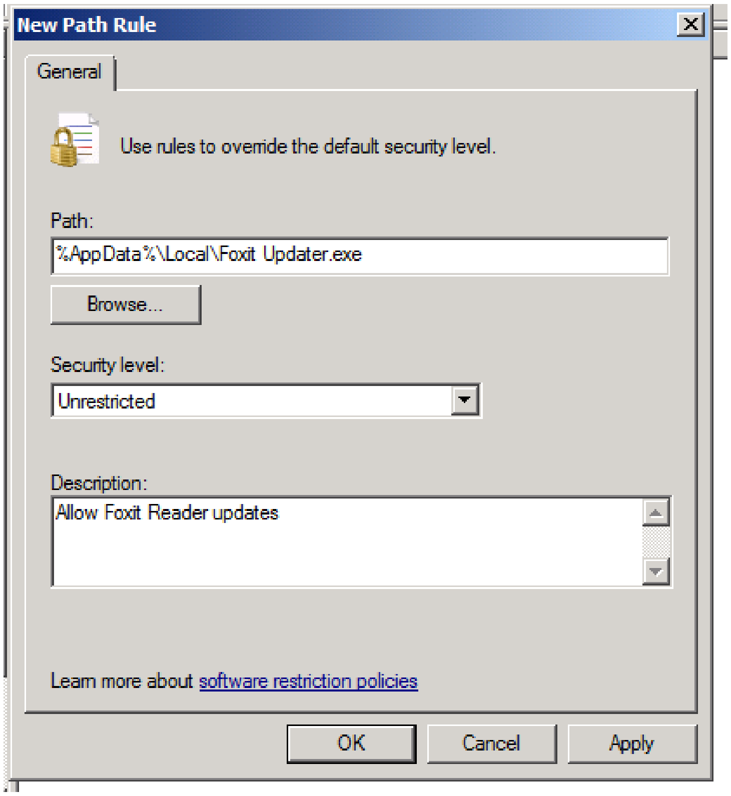
Enter the following values:

For Foxit

Path: %AppData%\Local\Foxit Updater.exe

Security Level: Unrestricted

Description: Allow Foxit Reader updates



New Path Rule

General

Use rules to override the default security level.

Path: %AppData%\Local\Foxit Updater.exe

Security level: Unrestricted

Description: Allow Foxit Reader updates

Learn more about software restriction policies

Figure 1 - Allow exception for Foxit

For Google Chrome:

Path:%AppData%\Local\Google\Update\GoogleUpdate.exe

Security Level: Unrestricted

Description: Allow Google Chrome updates

For Office installs on XP:

Path: %AppData%\Local\Temp\ose00000.exe

Security Level: Unrestricted

Description: Allow MS Office install

For Office installs on Vista and higher:

Path: %localAppData%\Local\Temp\ose00000.exe

Security Level: Unrestricted

Description: Allow MS Office install

For Copilot

Path: %localAppData%\Temp\HelperShell.exe

Security Level: Unrestricted

Description: Allow Copilot to run

For JOINme:

Path %AppData%\join.me\join.me.exe

Security Level: Unrestricted

Description: Allow Join.me to run

The difficult part may be finding what location the app needs to update. For that keep an eye on event 866 in the event logs which indicate what applications have been blocked:

```
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.
```

If you see the application launching from c:\users\username\appdata\local on a Windows 7 machine (or Vista) you'll need to use the variable of %LocalAppData. For an application launching from the roaming folder, this equates to %Appdata%.

Software updating

So far the problem child in this process is Java. As noted by Jason Carpenter, Java http://community.spiceworks.com/topic/396103-cryptolocker-prevention-kit-updated?page=7 Java doesn't keep to a specific name and keeps changing it for each update. Therefore your options can be limited. Jason built (via registry) exemptions for the next 15 update variations.

You may want to see what solution works for your client base.

The basic exception rule is as follows:

Path: %localAppData%\Temp\jre-7u49-windows-i586-iftw.exe

Security Level: Unrestricted

Description: Java auto-update exception.

To add additional exceptions as the Java updater changes revisit this and add values as follows:

%localAppData%\Temp\jre-7u50-windows-i586-iftw.exe

%localAppData%\Temp\jre-7u51-windows-i586-iftw.exe

%localAppData%\Temp\jre-7u52-windows-i586-iftw.exe

..and so on….

What about Home users and Home versions?

There is another site that is graciously offering up a kit for home PCs. Yes the url is … well… interesting … but the intention is still valid. http://www.foolishit.com/vb6-projects/cryptoprevent/ This allows you to place prevention on a home PC that does not have local security policy ability nor group policy ability.