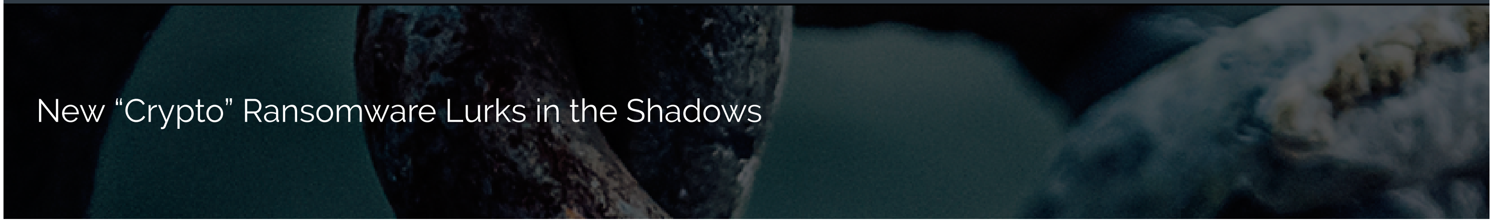
Careers 855-525-2489 Contact Us REQUEST A DEMO

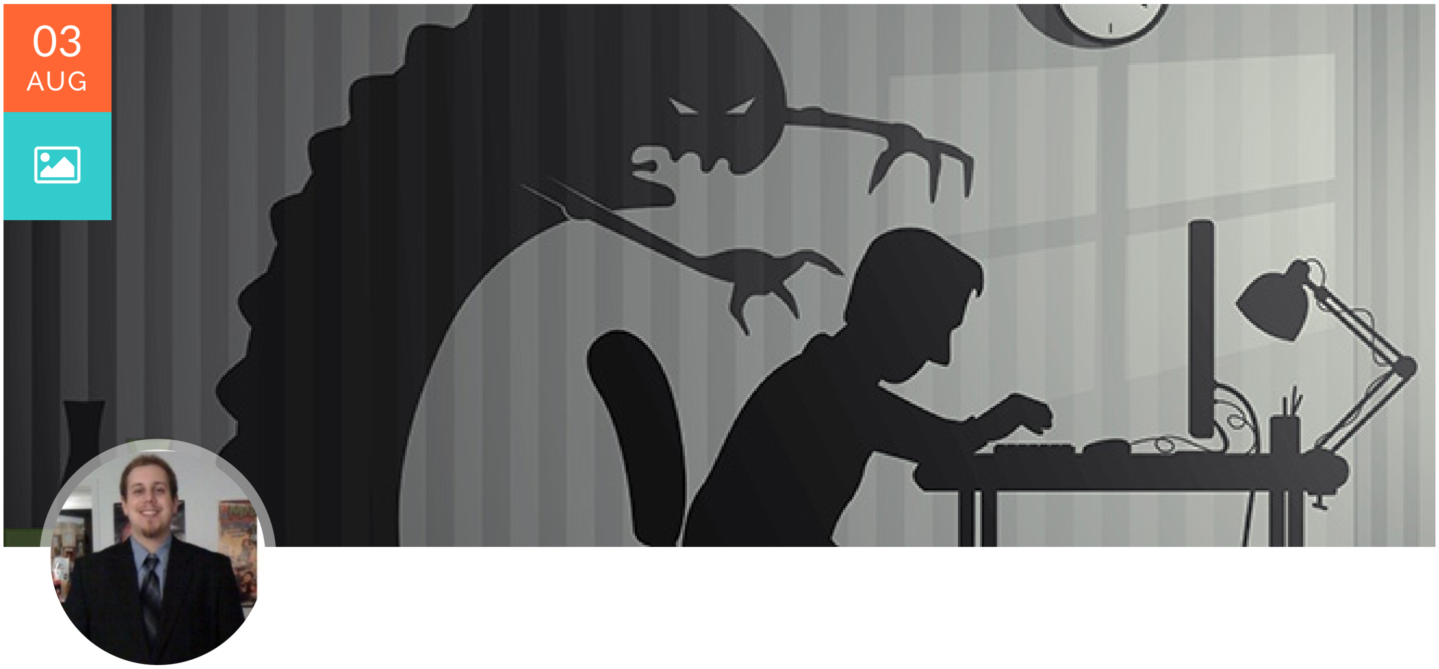
CARBON BLACK
ARM YOUR ENDPOINTS

WHY CARBON BLACK PRODUCTS SOLUTIONS PARTNERS RESOURCES COMPANY

BLOG



New “Crypto” Ransomware Lurks in the Shadows



New “Crypto” Ransomware Lurks in the Shadows

August 3, 2015 / Ryan Nolette / Advanced Threat Protection, Endpoint and Server Security, Prevention, Response, Tech Toolbox

Another “crypto” ransomware variant has been lurking in the shadows and is dastardly removing the volume shadow copies on your system, disallowing you from restoring and then encrypting your files for ransom.

Shadow Copy is a technology included in Microsoft Windows that allows the taking of backup copies (snapshots) of computer files or volumes. The best part is that these backups can be taken even when the files are in use. It is implemented as a Windows service called the “Volume Shadow Copy Service.”

————————————————————————————

Also See: Carbon Black Threat Research Team Unveils Nefarious Intents of “Volume Shadows Copies”

————————————————————————————

Shadow copies can be created on local and external (removable or network) volumes by any Windows component that utilizes it, such as when creating a scheduled Windows backup or automatic system restore point.

Based on that description, you can see why the removing of these files is beneficial to attackers. If you cannot recover from backups, you are at their mercy.

Sample detonated for this post:

- MD5
  - c24605589c71eb4835f3ee2654812315
- SHA1
  - b078772e826eaf2c736b96e7844f3828d2666b6f
- Initial location on the test system
  - C:\Users\master\Desktop\c24605589c71eb4835f3ee2654812315.b078772e826eaf2c736b96e7844f3828d2666b6f.exe

Files Written:

- \Device\KsecDD
- C:\f1f94d81\f1f94d81.exe
- C:\Users\master\AppData\Roaming\f1f94d81.exe
- C:\Users\master\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\f1f94d81.exe

Files Read:

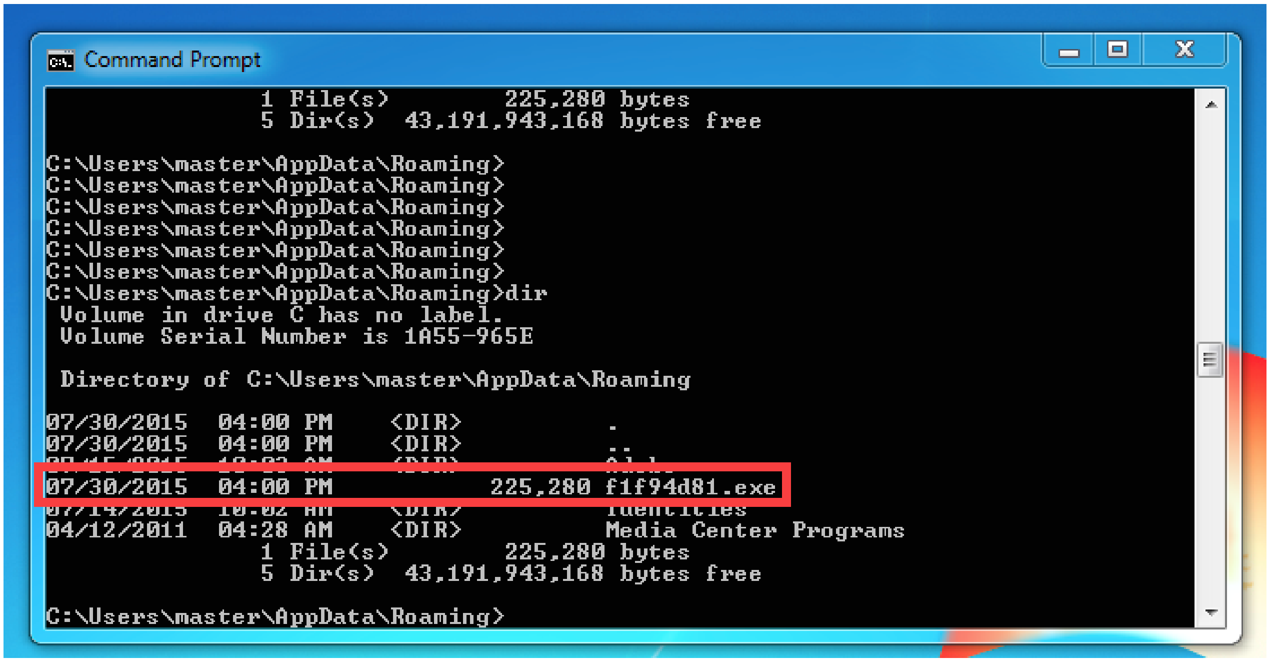
- C:\Windows\syswow64\svchost.exe
- C:\Windows\syswow64\vssadmin.exe

Processes spawned:

- C:\Users\master\Downloads\PDMHSOFE\webpage-38715fa8845ad8844759960e8b8a34b3.zip.exe
- C:\Users\master\Downloads\PDMHSOFE\webpage-38715fa8845ad8844759960e8b8a34b3.zip.exe
- C:\Windows\syswow64\svchost.exe -k netsvcs
- C:\Windows\syswow64\vssadmin.exe vssadmin.exe Delete Shadows /All /Quiet
- C:\Windows\SysWOW64\NOTEPAD.EXE C:\Windows\system32\NOTEPAD.EXE C:\Users\master\Desktop\HELP_DECRYPT.TXT
- C:\Program Files (x86)\Internet Explorer\iexplore.exe “C:\Program Files (x86)\Internet Explorer\iexplore.exe” -nohome
- C:\Program Files (x86)\Internet Explorer\iexplore.exe “C:\Program Files (x86)\Internet Explorer\iexplore.exe” SCODEF:2184 CREDAT:14337

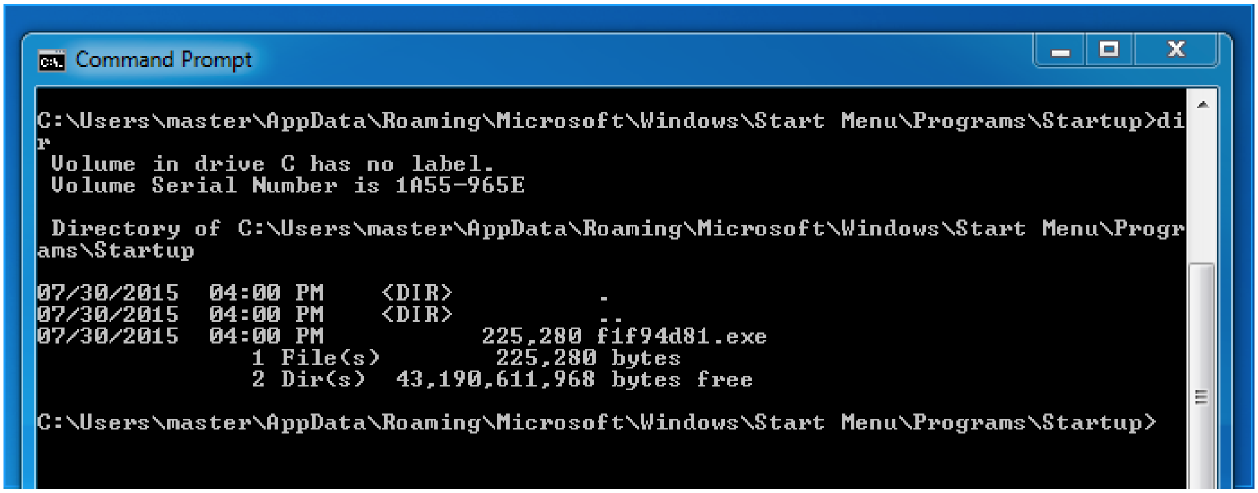
What happens on the host from the host point of view:

The first thing this malware does is delete itself from the original location it was run from and create a new binary in the user’s roaming appdata directory. This is extremely common among Trojan malwares. C:\Users\<username>\appdata\Roaming (Windows 7) is the first place I check for newly created directories and binaries because it is so common.



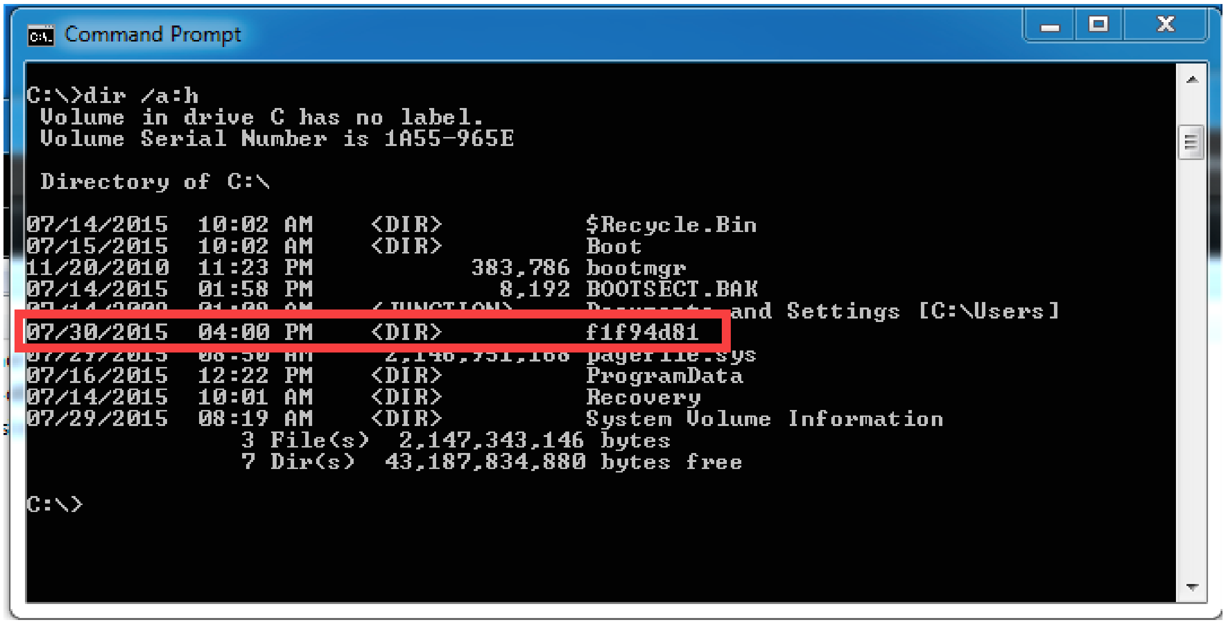
```
               1 File(s)        225,280 bytes
               5 Dir(s)  43,191,943,168 bytes free

C:\Users\master\AppData\Roaming>
C:\Users\master\AppData\Roaming>
C:\Users\master\AppData\Roaming>
C:\Users\master\AppData\Roaming>
C:\Users\master\AppData\Roaming>
C:\Users\master\AppData\Roaming>
C:\Users\master\AppData\Roaming>dir
 Volume in drive C has no label.
 Volume Serial Number is 1A55-965E

 Directory of C:\Users\master\AppData\Roaming

07/30/2015  04:00 PM    <DIR>          .
07/30/2015  04:00 PM    <DIR>          ..
07/15/2015  10:02 AM    <DIR>          Adobe
07/30/2015  04:00 PM           225,280 f1f94d81.exe
07/14/2015  10:02 AM    <DIR>          Identities
04/12/2011  04:28 AM    <DIR>          Media Center Programs
               1 File(s)        225,280 bytes
               5 Dir(s)  43,191,943,168 bytes free

C:\Users\master\AppData\Roaming>
```

Next the malware creates a persistence mechanism by copying itself to the user’s startup programs directory. This is a common technique and is a location that should always be checked for new binaries.



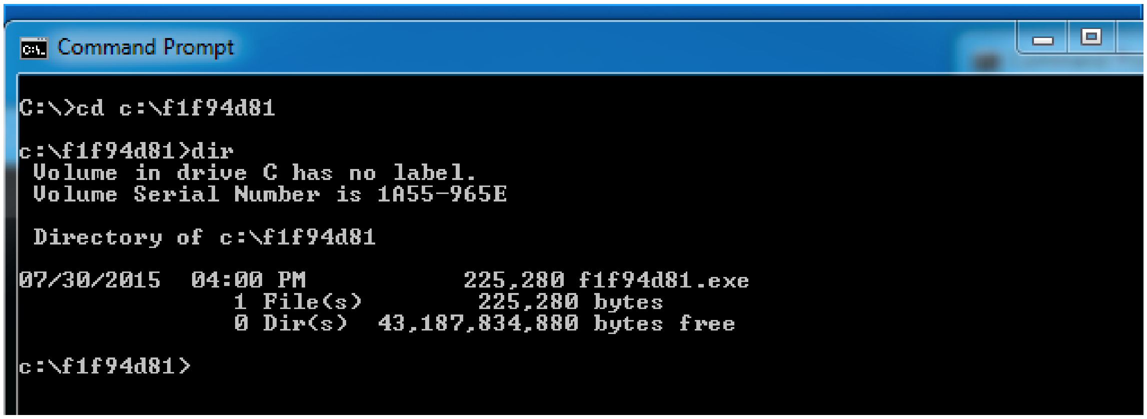
```
C:\Users\master\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup>di
r
 Volume in drive C has no label.
 Volume Serial Number is 1A55-965E

 Directory of C:\Users\master\AppData\Roaming\Microsoft\Windows\Start Menu\Progr
ams\Startup

07/30/2015  04:00 PM    <DIR>          .
07/30/2015  04:00 PM    <DIR>          ..
07/30/2015  04:00 PM           225,280 f1f94d81.exe
               1 File(s)        225,280 bytes
               2 Dir(s)  43,190,611,968 bytes free

C:\Users\master\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup>
```

The third action this malware takes is to create a hidden folder in the root directory of the files system. You can see below that the folder was created within seconds of the original binary being deleted and the other two binaries being written to the filesystem.



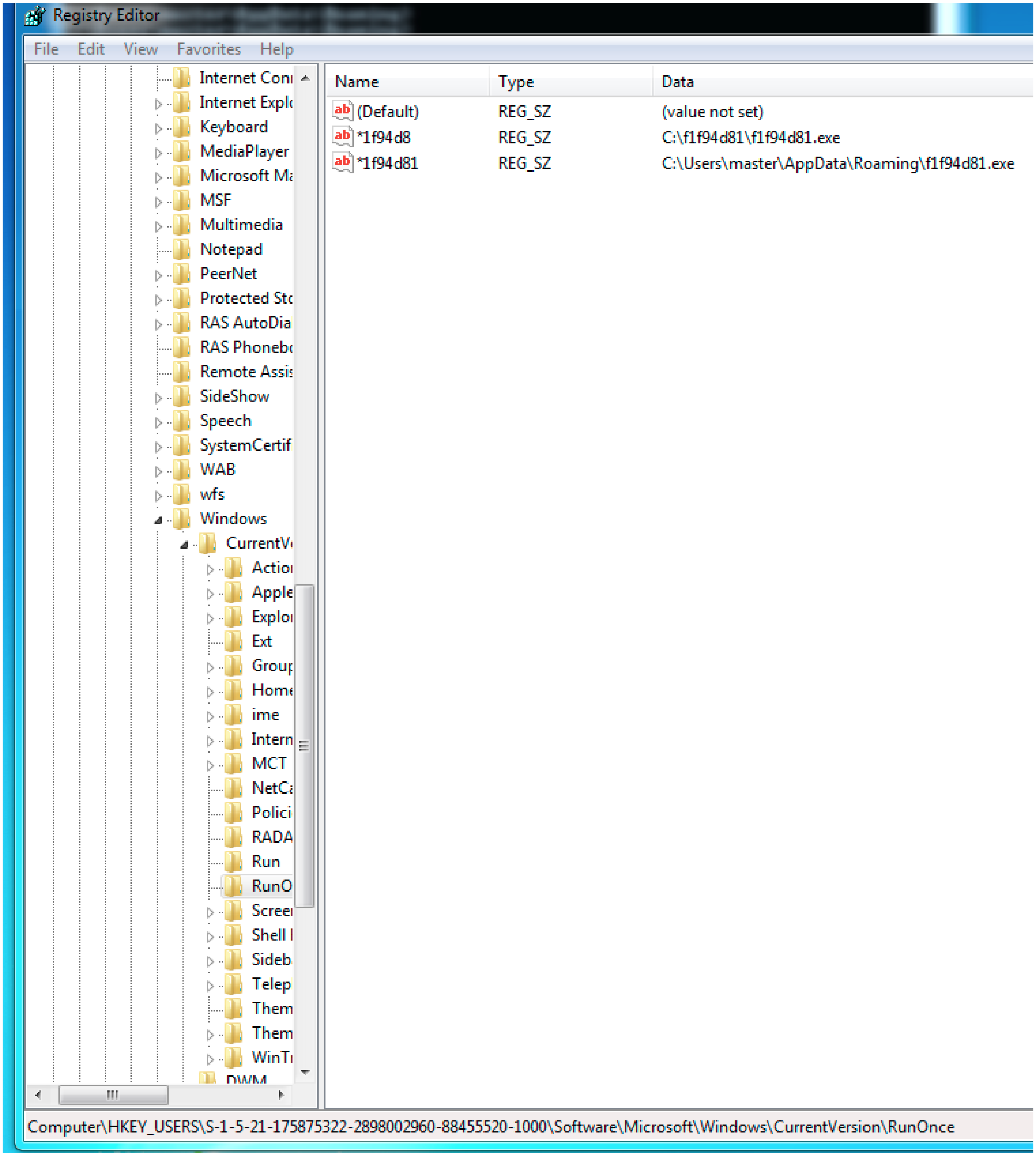
```
C:\>dir /a:h
 Volume in drive C has no label.
 Volume Serial Number is 1A55-965E

 Directory of C:\

07/14/2015  10:02 AM    <DIR>          $Recycle.Bin
07/15/2015  10:02 AM    <DIR>          Boot
11/20/2010  11:23 PM           383,786 bootmgr
07/14/2015  01:58 PM             8,192 BOOTSECT.BAK
07/14/2009  01:00 AM    <JUNCTION>     Documents and Settings [C:\Users]
07/30/2015  04:00 PM    <DIR>          f1f94d81
07/29/2015  08:50 AM     2,146,951,168 pagefile.sys
07/16/2015  12:22 PM    <DIR>          ProgramData
07/14/2015  10:01 AM    <DIR>          Recovery
07/29/2015  08:19 AM    <DIR>          System Volume Information
               3 File(s)  2,147,343,146 bytes
               7 Dir(s)  43,187,834,880 bytes free

C:\>
```

Inside this new file is yet another copy of the binary. It seems like the malware author is afraid of these binaries being found and creates backup plans for their backup plans. That kind of paranoia isn’t healthy.



```
C:\>cd c:\f1f94d81

c:\f1f94d81>dir
 Volume in drive C has no label.
 Volume Serial Number is 1A55-965E

 Directory of c:\f1f94d81

07/30/2015  04:00 PM           225,280 f1f94d81.exe
               1 File(s)         225,280 bytes
               0 Dir(s)  43,187,834,880 bytes free

c:\f1f94d81>
```

Next up, the malware starts creating registry values so it can be started in the background each time the user logs in. I can infer their intent because the “Run” and “RunOnce” keys are run each time a new user logs in. These keys are for background services such as remote registry service and are run only once per boot.

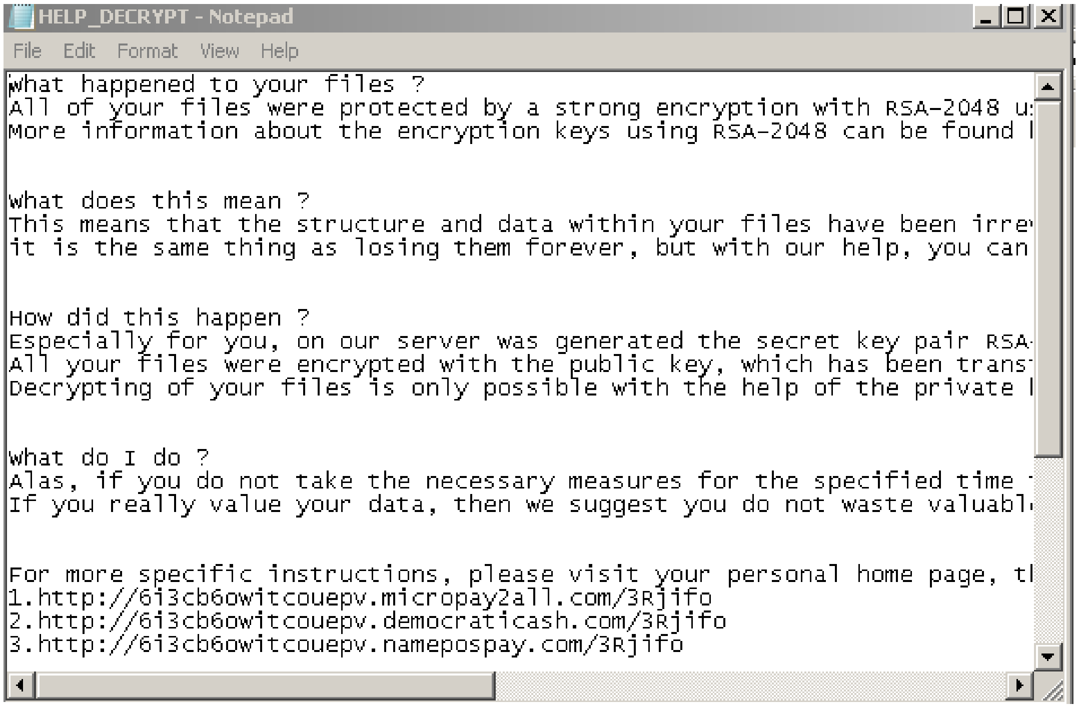


Name	Type	Data
ab (Default)	REG_SZ	(value not set)
ab *1f94d8	REG_SZ	C:\f1f94d81\f1f94d81.exe
ab *1f94d81	REG_SZ	C:\Users\master\AppData\Roaming\f1f94d81.exe

Computer\HKEY_USERS\S-1-5-21-175875322-2898002960-88455520-1000\Software\Microsoft\Windows\CurrentVersion\RunOnce

After the malware has been running for a while on the system, you start to see files created all over the filesystem called “HELP_DECRYPT.txt” and “HELP_DECRYPT.png.”

Below is a sample of what the file contains. This system has now had its files encrypted, backups deleted, and is being held for ransom.



```
what happened to your files ?
All of your files were protected by a strong encryption with RSA-2048 u
More information about the encryption keys using RSA-2048 can be found


what does this mean ?
This means that the structure and data within your files have been irre
it is the same thing as losing them forever, but with our help, you can


How did this happen ?
Especially for you, on our server was generated the secret key pair RSA
All your files were encrypted with the public key, which has been trans
Decrypting of your files is only possible with the help of the private


what do I do ?
Alas, if you do not take the necessary measures for the specified time
If you really value your data, then we suggest you do not waste valuab


For more specific instructions, please visit your personal home page, t
1.http://6i3cb6owitcouepv.micropay2all.com/3Rjifo
2.http://6i3cb6owitcouepv.democraticash.com/3Rjifo
3.http://6i3cb6owitcouepv.namepospay.com/3Rjifo
```

What happens on the host from the Carbon Black point of view?

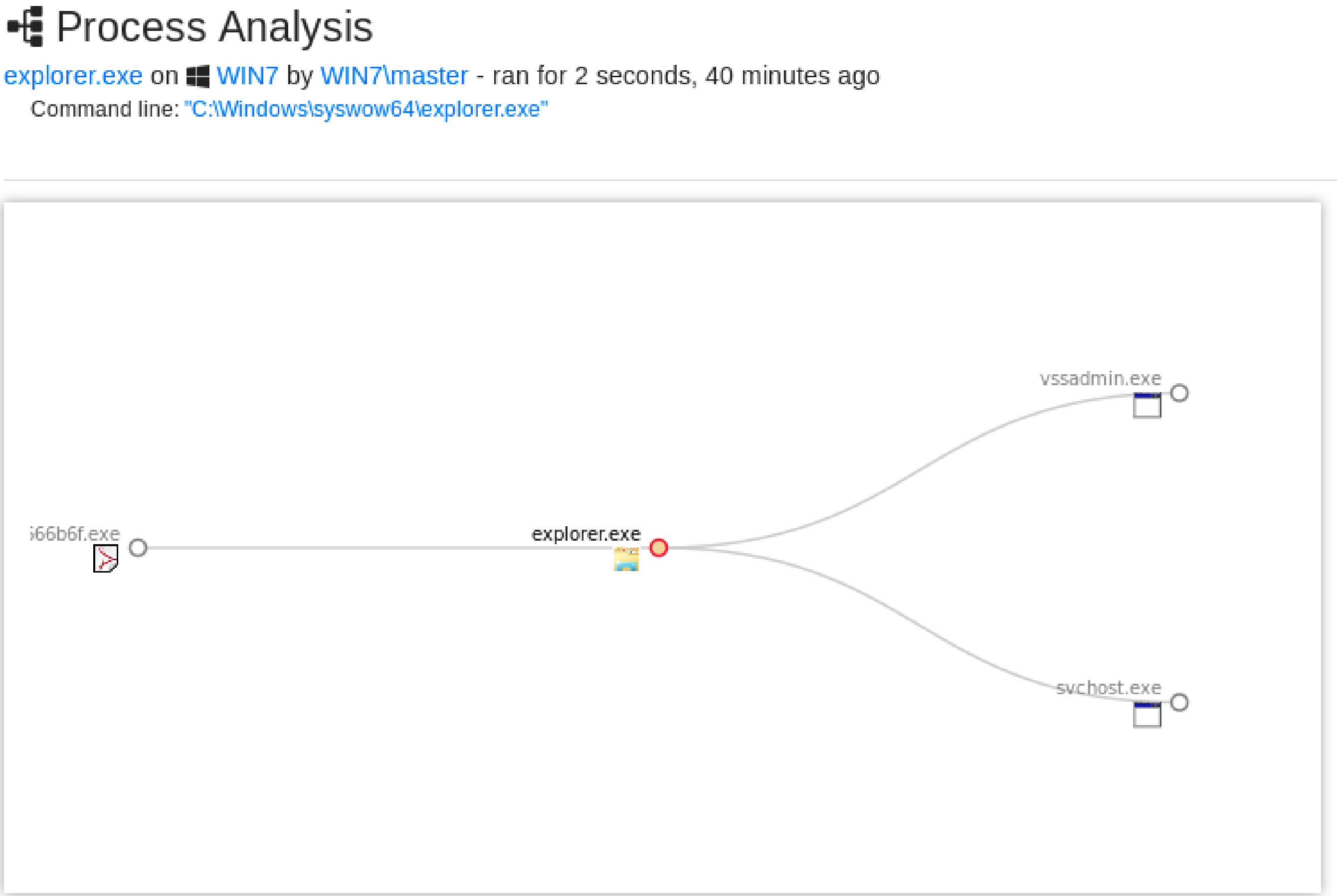
So to cheat a bit, since we detonated this malware on purpose, we already know what to look for based on the original filename. In the real world, we don't have that luxury. To make this workflow as realistic as possible I created a new watchlist on my Carbon Black server. This watchlist looks for the command "C:\Windows\syswow64\vssadmin.exe vssadmin.exe Delete Shadows /All /Quiet" to be issued on systems. This legitimately will not happen on an enterprise system unless operations explicitly does this. If they do, they will know about it, and you can modify the watchlist accordingly with your corporate process and workflow.

(Side note: We can stop this action from happening by using a custom Bit9 rule that blocks normal user accounts from running vssadmin. This rule effectively neuters the crypto malware's ability to delete shadow copies and allows the impacted company to restore from backup instead of paying the ransom. It also removes the ability to execute vssadmin from a native script or command line. This could cause some collateral damage, so modify accordingly with your corporate policy and use cases.)

The next step is waiting for an alert to come through. Once that has happened, we investigate.

Below, we can see the process tree of this file. Based on the alert, which led me to the vssadmin.exe execution, I was able to backtrack up the tree to see that the original process was:

C:\Users\master\Desktop\c24605589c71eb4835f3ee2654812315.b078772e826eaf2c736b96e7844f3828d2666b6f.exe.

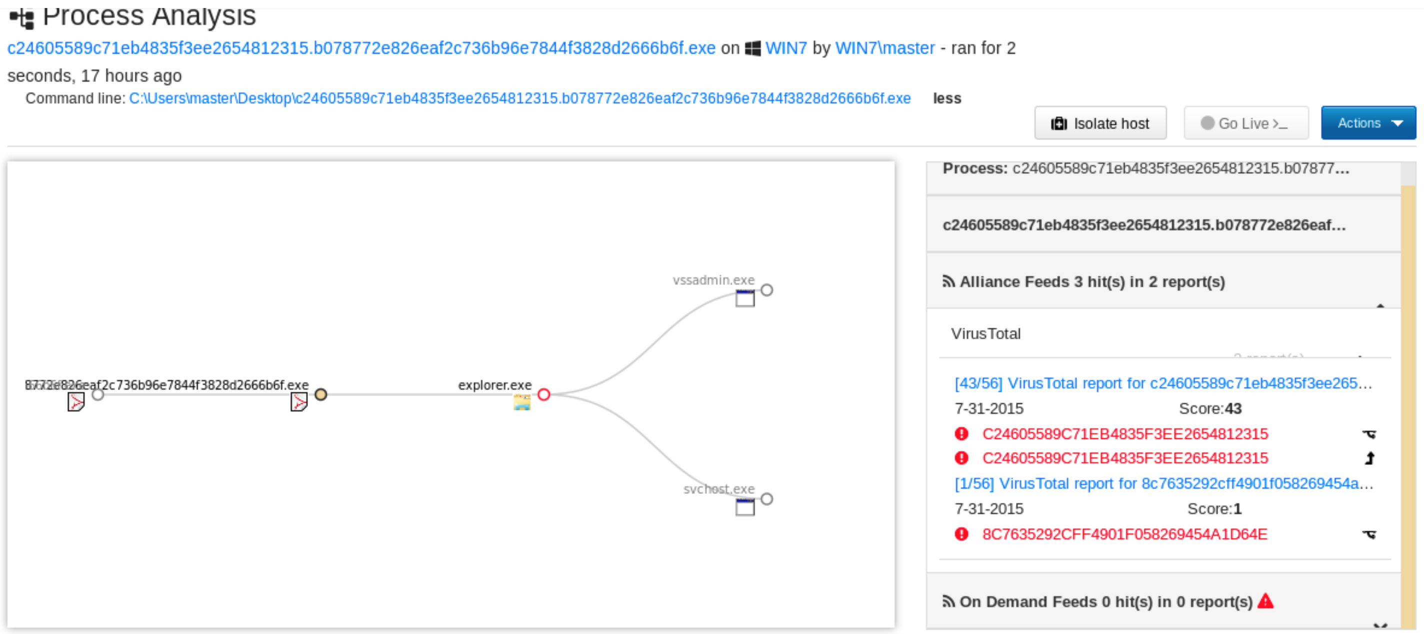


Process Analysis

explorer.exe on WIN7 by WIN7\master - ran for 2 seconds, 40 minutes ago

Command line: "C:\Windows\syswow64\explorer.exe"

This binary has a score of 43/56. I should probably look into what this binary did.



Process Analysis

c24605589c71eb4835f3ee2654812315.b078772e826eaf2c736b96e7844f3828d2666b6f.exe on WIN7 by WIN7\master - ran for 2 seconds, 17 hours ago

Command line: C:\Users\master\Desktop\c24605589c71eb4835f3ee2654812315.b078772e826eaf2c736b96e7844f3828d2666b6f.exe less

Process: c24605589c71eb4835f3ee2654812315.b07877…

c24605589c71eb4835f3ee2654812315.b078772e826eaf…

Alliance Feeds 3 hit(s) in 2 report(s)

VirusTotal

[43/56] VirusTotal report for c24605589c71eb4835f3ee265…

7-31-2015 Score:**43**

C24605589C71EB4835F3EE2654812315

C24605589C71EB4835F3EE2654812315

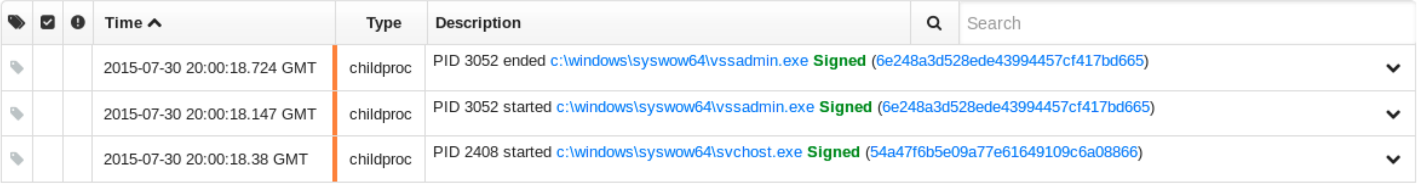
[1/56] VirusTotal report for 8c7635292cff4901f058269454a…

7-31-2015 Score:**1**

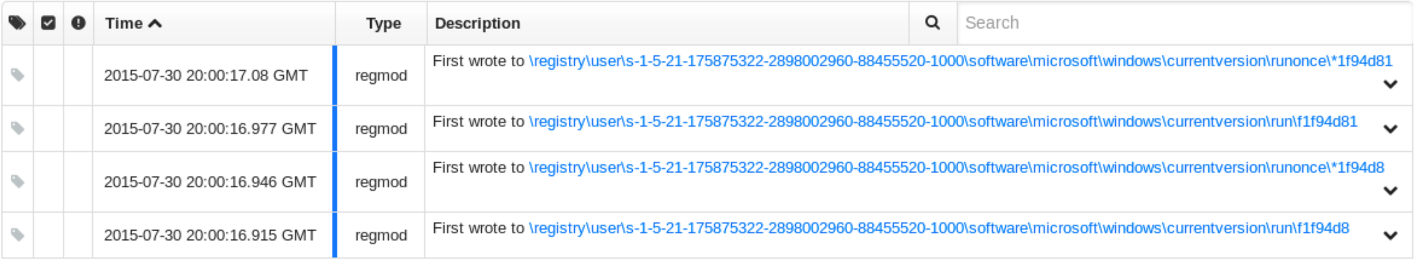
8C7635292CFF4901F058269454A1D64E

On Demand Feeds 0 hit(s) in 0 report(s)

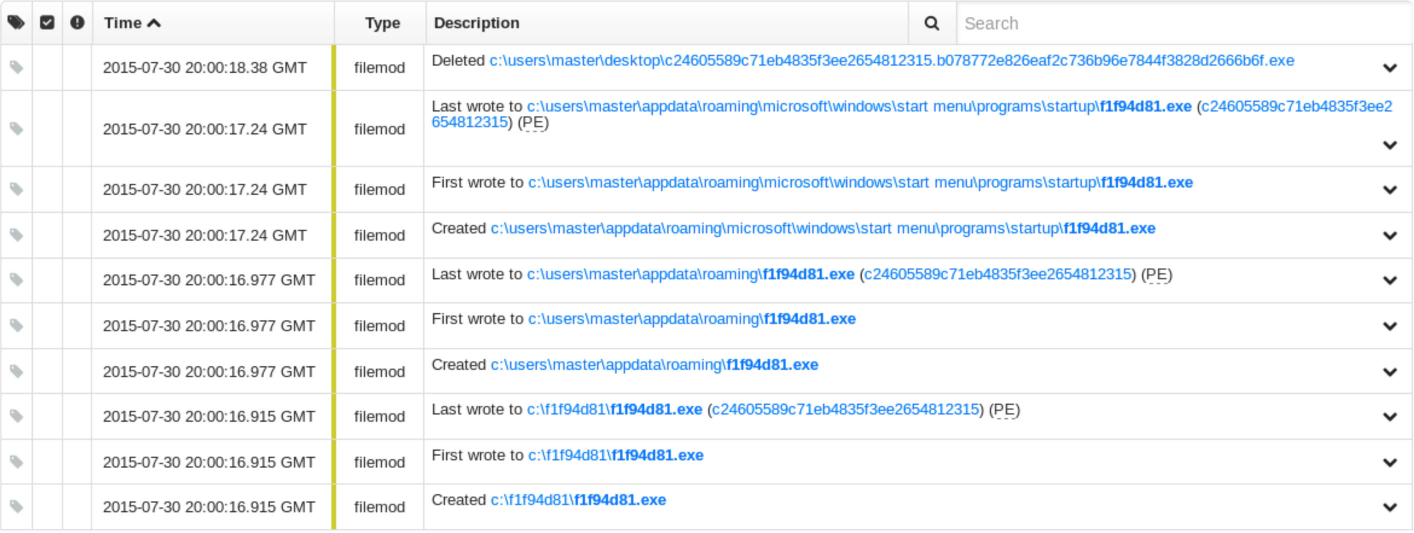
Below, we can see that it spawned three new processes, created four new registry entries, and created 10 new files on the system.



Time	Type	Description	Search
2015-07-30 20:00:18.724 GMT	childproc	PID 3052 ended c:\windows\syswow64\vssadmin.exe **Signed** (6e248a3d528ede43994457cf417bd665)	
2015-07-30 20:00:18.147 GMT	childproc	PID 3052 started c:\windows\syswow64\vssadmin.exe **Signed** (6e248a3d528ede43994457cf417bd665)	
2015-07-30 20:00:18.38 GMT	childproc	PID 2408 started c:\windows\syswow64\svchost.exe **Signed** (54a47f6b5e09a77e61649109c6a08866)	



Time	Type	Description	Search
2015-07-30 20:00:17.08 GMT	regmod	First wrote to \registry\user\s-1-5-21-175875322-2898002960-88455520-1000\software\microsoft\windows\currentversion\runonce\*1f94d81	
2015-07-30 20:00:16.977 GMT	regmod	First wrote to \registry\user\s-1-5-21-175875322-2898002960-88455520-1000\software\microsoft\windows\currentversion\run\f1f94d81	
2015-07-30 20:00:16.946 GMT	regmod	First wrote to \registry\user\s-1-5-21-175875322-2898002960-88455520-1000\software\microsoft\windows\currentversion\runonce\*1f94d8	
2015-07-30 20:00:16.915 GMT	regmod	First wrote to \registry\user\s-1-5-21-175875322-2898002960-88455520-1000\software\microsoft\windows\currentversion\run\f1f94d8	



Time	Type	Description	Search
2015-07-30 20:00:18.38 GMT	filemod	Deleted c:\users\master\desktop\c24605589c71eb4835f3ee2654812315.b078772e826eaf2c736b96e7844f3828d2666b6f.exe	
2015-07-30 20:00:17.24 GMT	filemod	Last wrote to c:\users\master\appdata\roaming\microsoft\windows\start menu\programs\startup\f1f94d81.exe (c24605589c71eb4835f3ee2654812315) (PE)	
2015-07-30 20:00:17.24 GMT	filemod	First wrote to c:\users\master\appdata\roaming\microsoft\windows\start menu\programs\startup\f1f94d81.exe	
2015-07-30 20:00:17.24 GMT	filemod	Created c:\users\master\appdata\roaming\microsoft\windows\start menu\programs\startup\f1f94d81.exe	
2015-07-30 20:00:16.977 GMT	filemod	Last wrote to c:\users\master\appdata\roaming\f1f94d81.exe (c24605589c71eb4835f3ee2654812315) (PE)	
2015-07-30 20:00:16.977 GMT	filemod	First wrote to c:\users\master\appdata\roaming\f1f94d81.exe	
2015-07-30 20:00:16.977 GMT	filemod	Created c:\users\master\appdata\roaming\f1f94d81.exe	
2015-07-30 20:00:16.915 GMT	filemod	Last wrote to c:\f1f94d81\f1f94d81.exe (c24605589c71eb4835f3ee2654812315) (PE)	
2015-07-30 20:00:16.915 GMT	filemod	First wrote to c:\f1f94d81\f1f94d81.exe	
2015-07-30 20:00:16.915 GMT	filemod	Created c:\f1f94d81\f1f94d81.exe	

Based on our findings in Carbon Black, combined with open-source intelligence from searching around the Internet, and the score results, we can safely assume this machine is owned and needs to be reimaged. Or you can take the more manual approach and kill the active processes, remove all the files and registry entries that were created, and restore from backups.

All those steps, by the way, can be done via Carbon Black Live Response.

How to restore files encrypted using Shadow Volume Copies

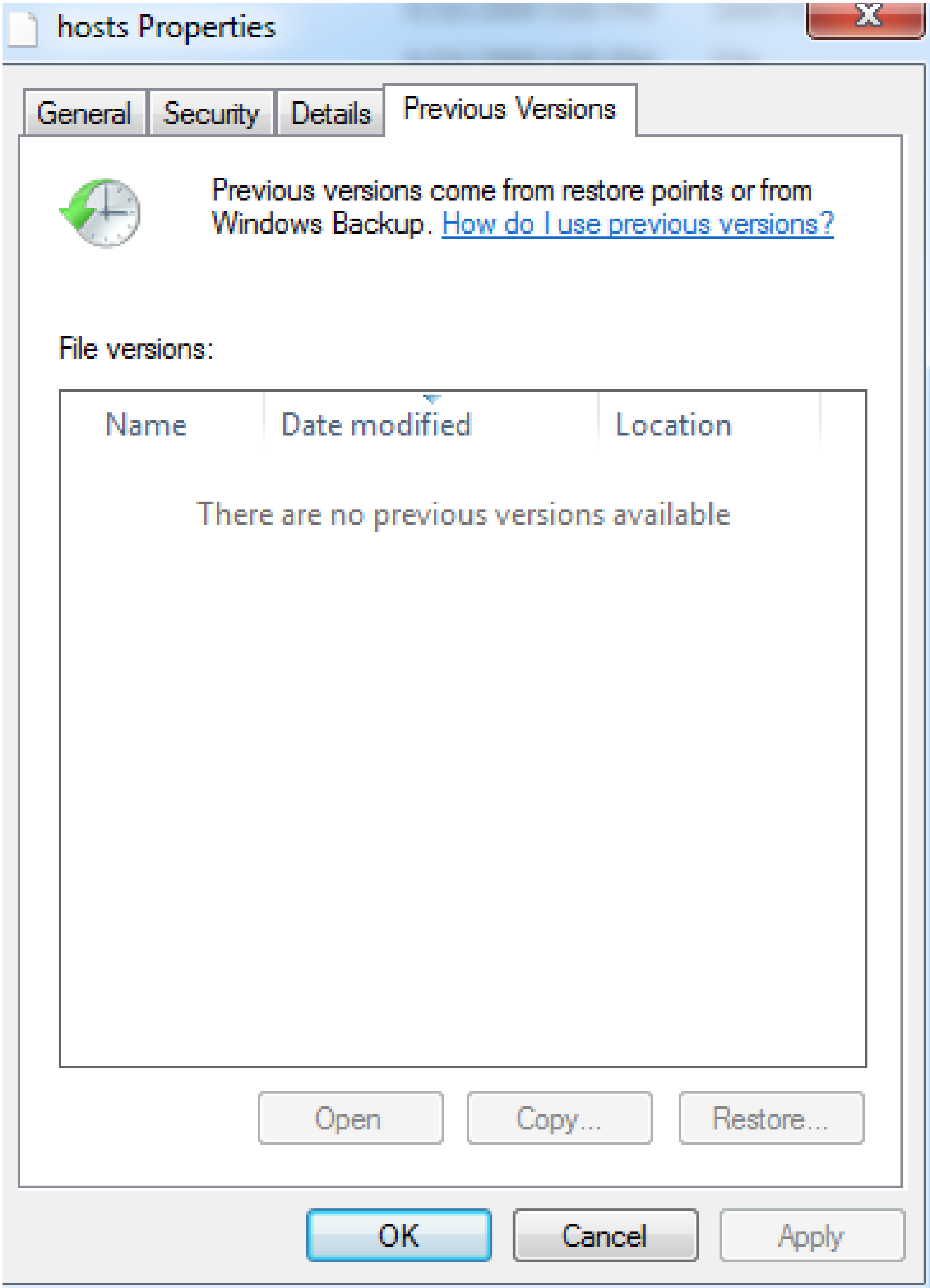
If you have “System Restore” enabled, your system will create shadow copies that hold copies of your files from that moment back. These copies “may,” and I use the term “may” dripping with hope, allow you to restore your files from before they were encrypted. Using shadow copies is not foolproof. Also, the version of the files in the shadow copy may not be the latest version and code be useless to you.

(***Note: Shadow volume copies are a feature only available with WinXP SP2, Vista, Win7, and Win8/8.1.)

There are multiple methods online documenting how to recover with a shadow copy. The method I normally use is the native Windows option. I use it because it has the most probability of being available to me on a Windows system.

To restore individual files:

1. Right-click on the file
2. Go into “Properties”
3. Select the “Previous Versions” tab
    1. This tab lists copies of the file stored in a shadow volume copy and the date backed up.



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

File versions:

Name	Date modified	Location

There are no previous versions available

To restore a particular version of the file:

1. Click on the “Copy” button
2. Select the directory to which you wish to restore the file.

To restore the selected file and replace the existing one:

1. Click on the “Restore” button.

To view the contents of the actual file:

1. Click on the “Open” button
    1. You can do this before you restore it.

This same method described above can be used to restore an entire folder.

How to prevent this infection

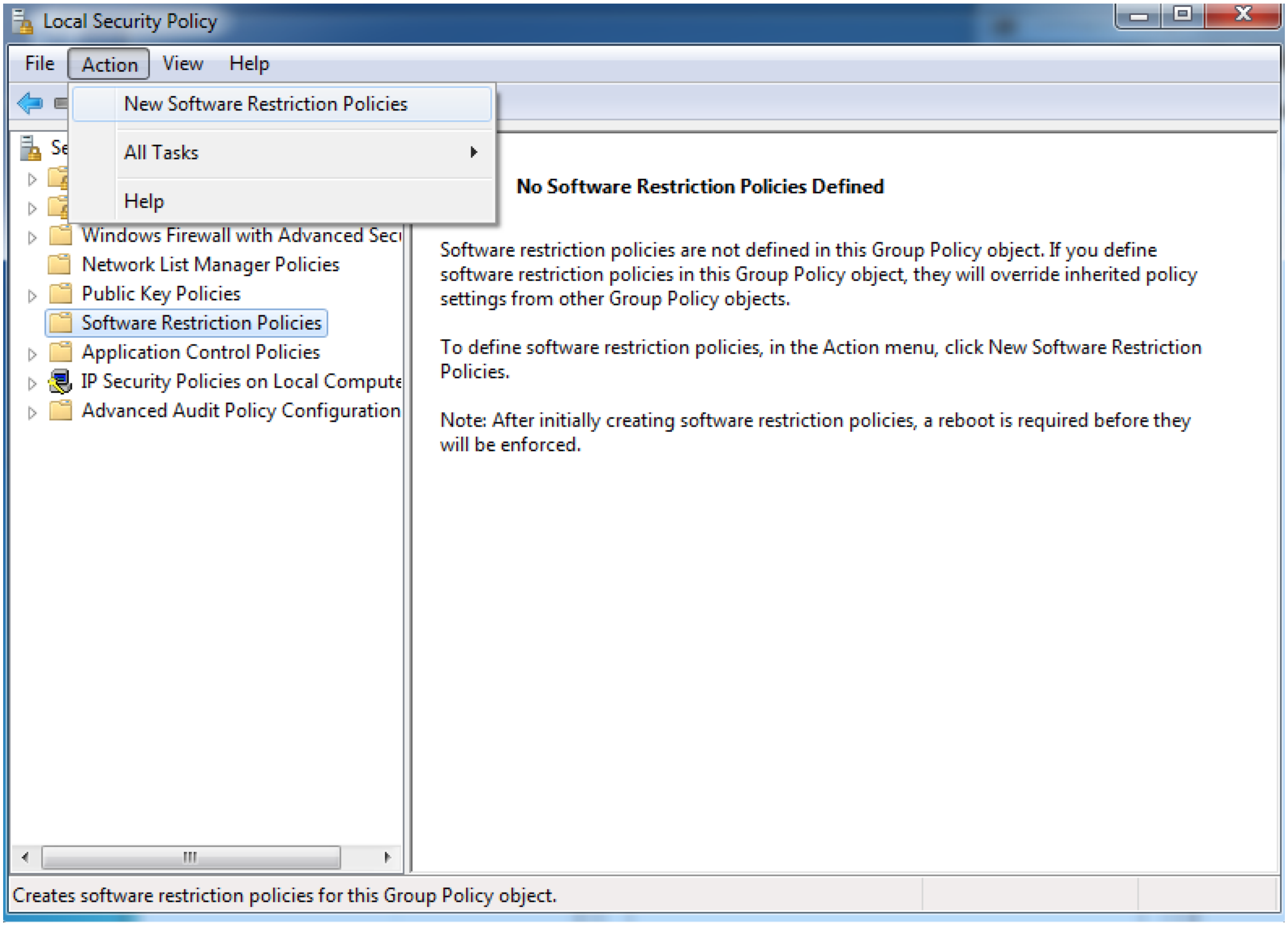
If possible, put any system you can in high-enforcement mode via the Bit9 console. This will prevent the execution of any unknown binary. Short of that, you can implement a few different types of rules depending on your use case, unique to you environmental variables, and desired outcome.

Below are a few rules I have created for different use cases. This rules are being represented in their most high-level form and not in the format they appear in the Bit9 console. I did this because even if you aren't using our products, you can still apply this logic and most of these rules to your environment by leveraging GPO, witchcraft and cursing.

The file paths that have been used by this infection and its droppers are:

- C:\f1f94d81\f1f94d81.exe
- C:\Users\master\AppData\Roaming\f1f94d81.exe
- C:\Users\master\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\f1f94d81.exe

You can create a software restriction policy using Windows Professional or Windows Server (for a single computer use the Local Security Policy Editor, for an entire domain use the Group Policy Editor).


Local Security Policy
File
Action
View
Help
New Software Restriction Policies
All Tasks
Help
Se
Windows Firewall with Advanced Secu
Network List Manager Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Local Compute
Advanced Audit Policy Configuration

No Software Restriction Policies Defined

Software restriction policies are not defined in this Group Policy object. If you define software restriction policies in this Group Policy object, they will override inherited policy settings from other Group Policy objects.

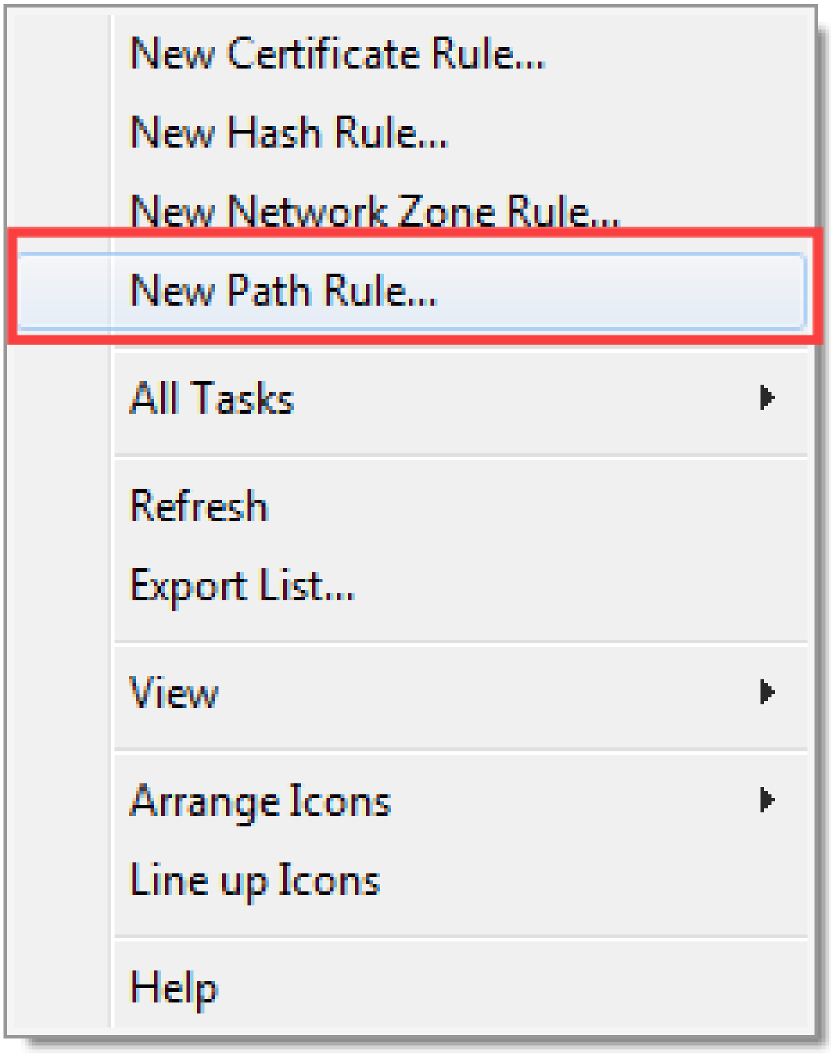
To define software restriction policies, in the Action menu, click New Software Restriction Policies.

Note: After initially creating software restriction policies, a reboot is required before they will be enforced.

Creates software restriction policies for this Group Policy object.

To open the Local Security Policy editor:

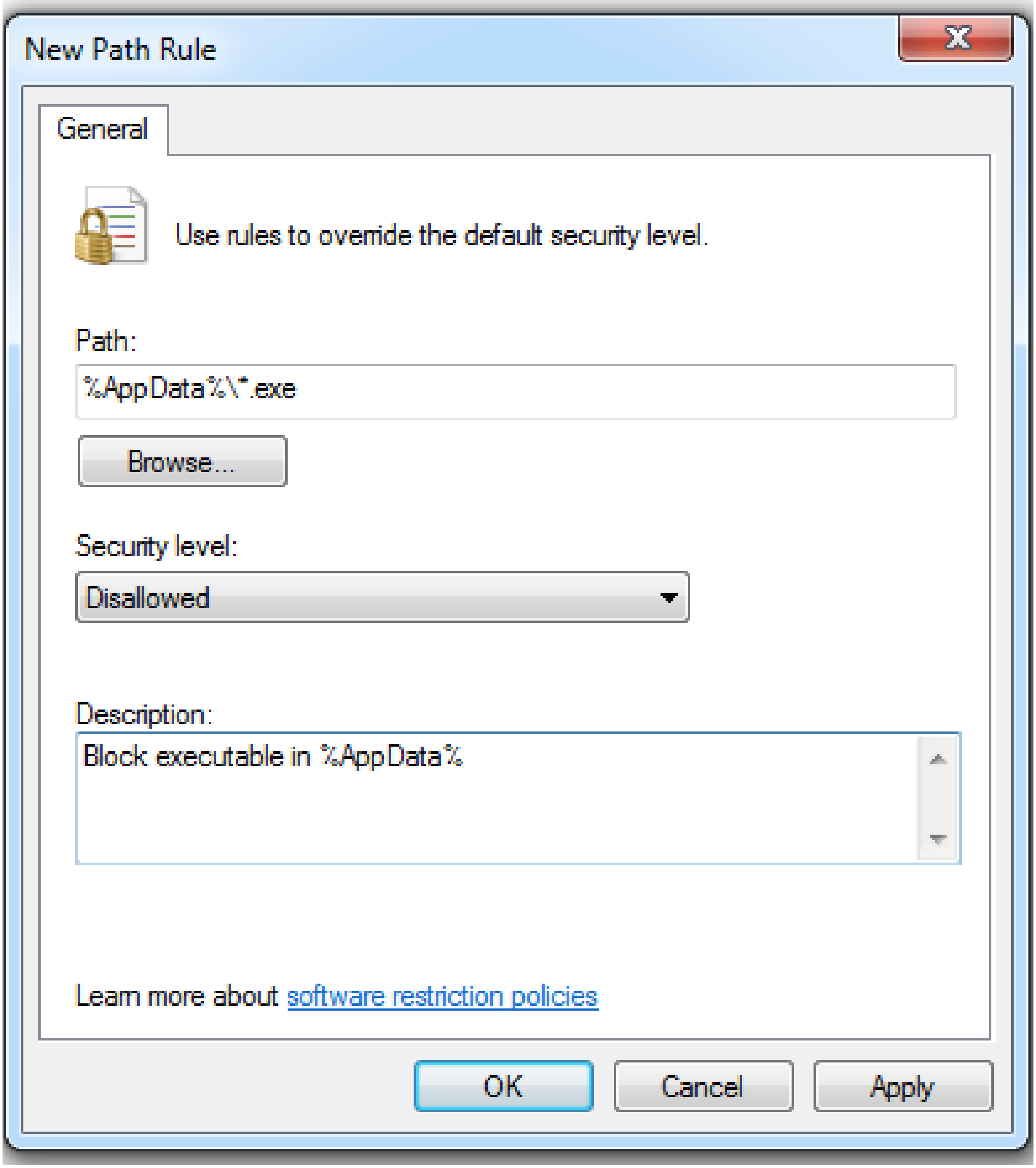
1. Click on the “Start” button
2. Type “Local Security Policy”
3. Select the search result that appears
4. Expand security settings
5. Click on the “Software Restriction Policies” section



If you do not see the items in the right pane as shown above, you will need to add a new policy.

1. Click on the “Action” button
2. Select “New Software Restriction Policies”
3. Click on the “Additional Rules” category
4. Right-click in the right pane
5. Select “New Path Rule”
    1. You should then add a Path Rule for each of the items listed below.

(***NOTE: *If the software restriction policies cause issues when trying to run legitimate applications, you will need to add exception rules. This is where Bit9 trust scores come in handy.)*



New Path Rule

Use rules to override the default security level.

Path: %AppData%*.exe

Security level: Disallowed

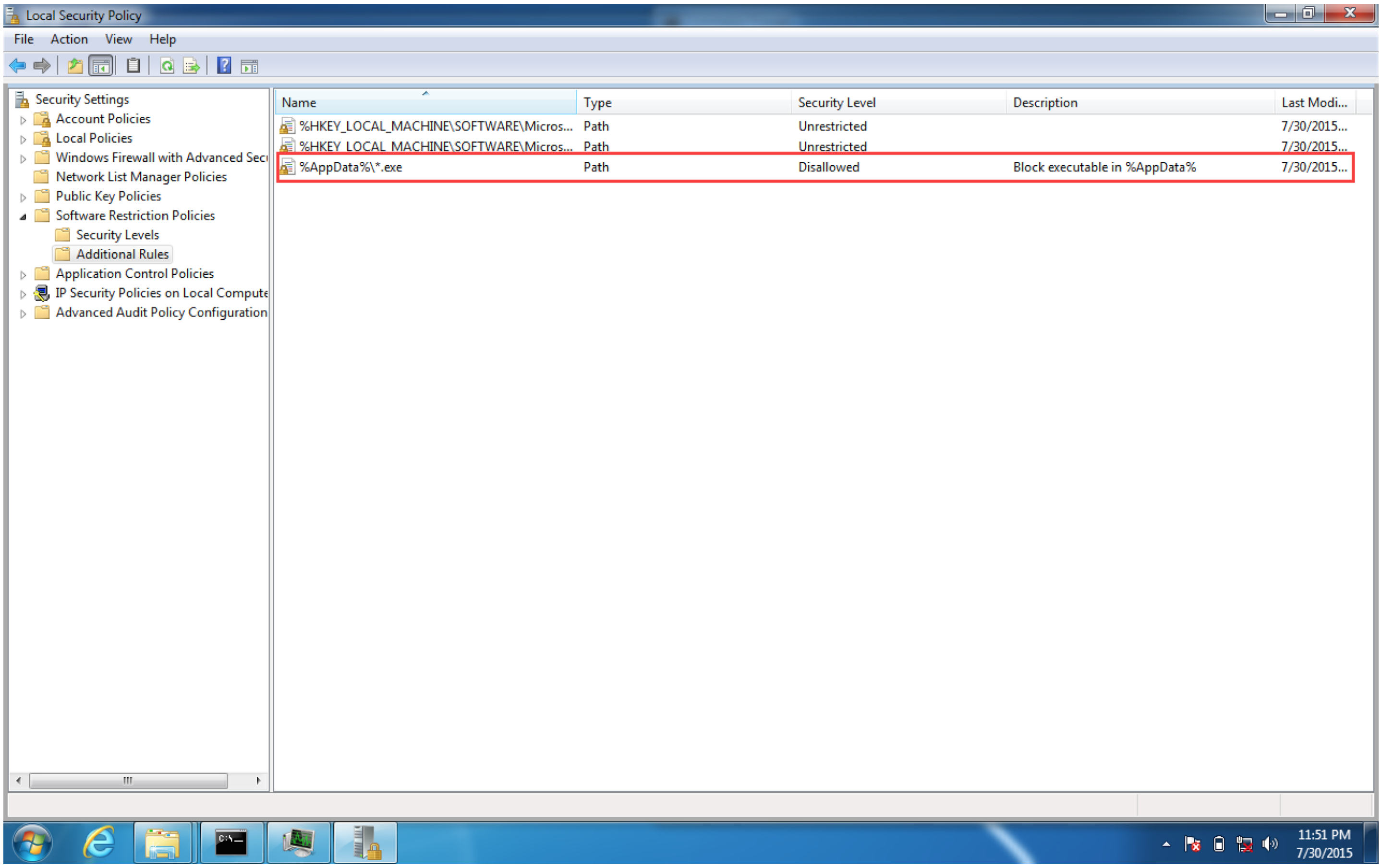
Description: Block executable in %AppData%

Block executable in %AppData%

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

Block executable in %LocalAppData%

- Path if using Windows XP: %UserProfile%\Local Settings*.exe
- Path if using Windows Vista/7/8: %LocalAppData%*.exe
- Security Level: Disallowed
- Description: Don’t allow executables to run from %AppData%


Local Security Policy
File
Action
View
Help
Security Settings
Account Policies
Local Policies
Windows Firewall with Advanced Secu
Network List Manager Policies
Public Key Policies
Software Restriction Policies
Security Levels
Additional Rules
Application Control Policies
IP Security Policies on Local Compute
Advanced Audit Policy Configuration
11:51 PM
7/30/2015

Name	Type	Security Level	Description	Last Modi...
%HKEY_LOCAL_MACHINE\SOFTWARE\Micros...	Path	Unrestricted		7/30/2015...
%HKEY_LOCAL_MACHINE\SOFTWARE\Micros...	Path	Unrestricted		7/30/2015...
%AppData%*.exe	Path	Disallowed	Block executable in %AppData%	7/30/2015...

Ransomware is annoyingly effective. The recent additions of features such as removing shadow copies makes it even more dangerous. I hope this guide on recovering from ransomware using Shadow Volume Copies is helpful to some poor soul who got hit. Regardless of what security products you use, your best defense to any attack is user training and backups. Anything preventative you can implement proactively, whether it’s Bit9 or a manual implementation using native Microsoft tools is going to protect you and your company.

Until next time, remember my motto: “Flag it, Tag it and Bag it.”