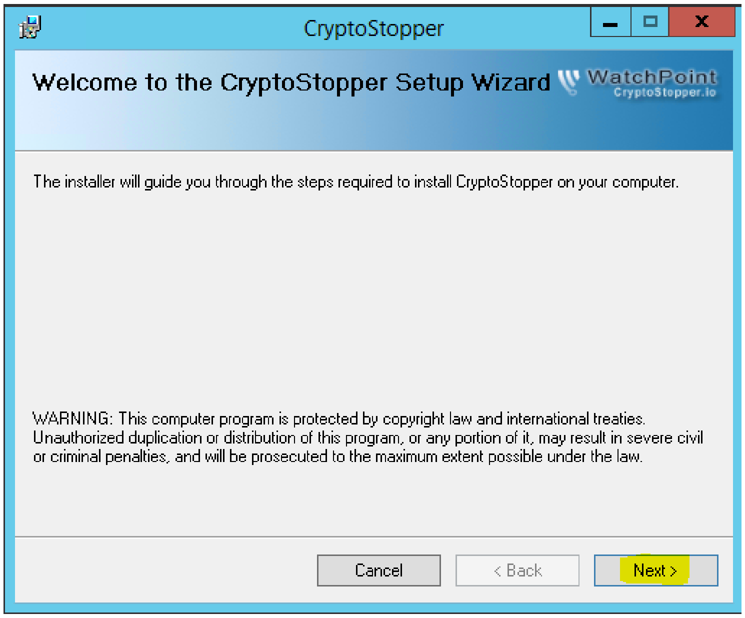
WatchPoint™
CryptoStopper.io

CryptoStopper.io – Installation and User Guide

Table of Contents

Installation

1) Click Next at ‘Welcome Screen’

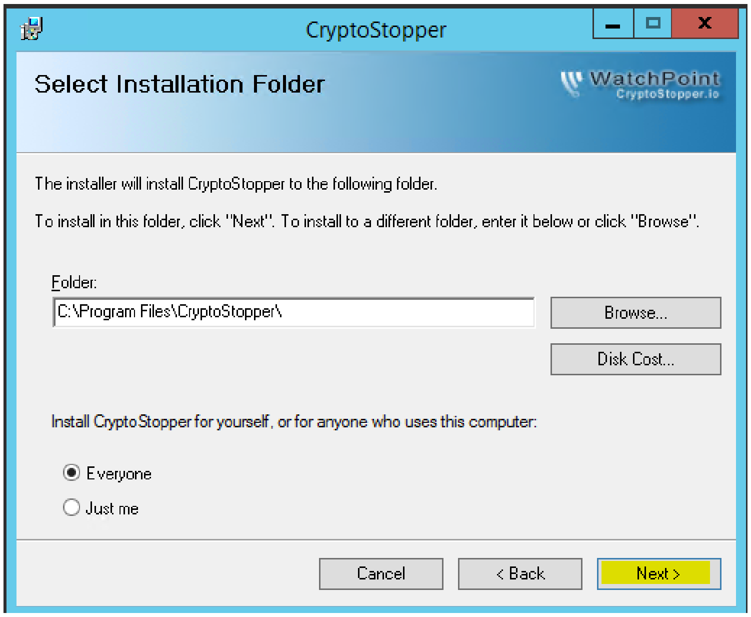


Welcome to the CryptoStopper Setup Wizard

The installer will guide you through the steps required to install CryptoStopper on your computer.

WARNING: This computer program is protected by copyright law and international treaties. Unauthorized duplication or distribution of this program, or any portion of it, may result in severe civil or criminal penalties, and will be prosecuted to the maximum extent possible under the law.

2) Accept the defaults and click Next, then Next again to confirm.



Select Installation Folder

The installer will install CryptoStopper to the following folder.

To install in this folder, click "Next". To install to a different folder, enter it below or click "Browse".

Folder: C:\Program Files\CryptoStopper\

Install CryptoStopper for yourself, or for anyone who uses this computer:

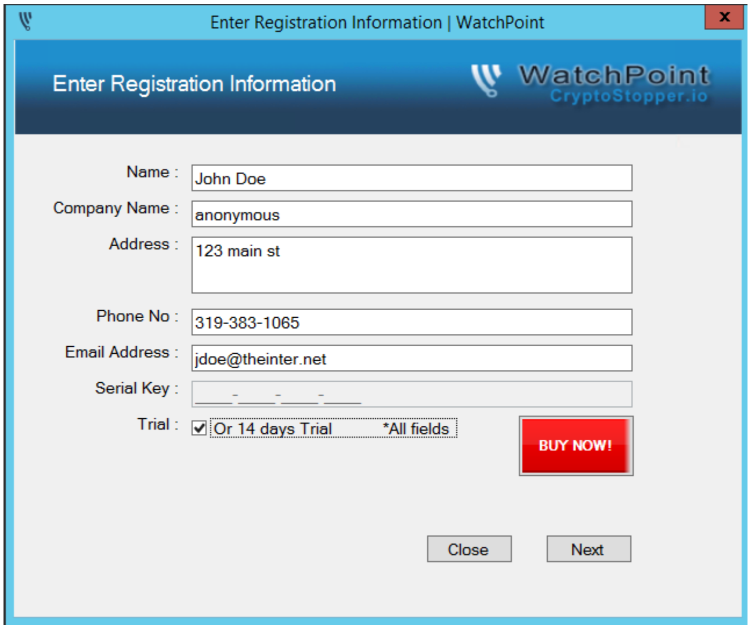
● Everyone

○ Just me

3) Accept the EULA, click Next.

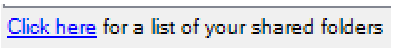
4) Enter registration information.
   a. Select the trial checkbox to begin the 14 day trial. Or enter a valid license key if purchased.

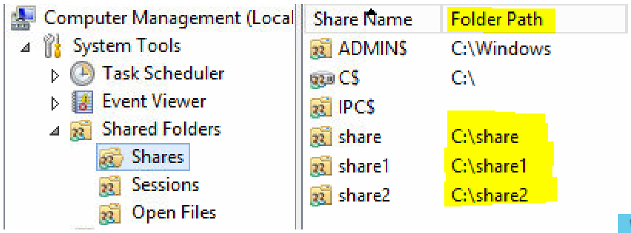
5) When complete click next


Enter Registration Information | WatchPoint
Enter Registration Information
WatchPoint
CryptoStopper.io
BUY NOW!
Close
Next

Name :	John Doe
Company Name :	anonymous
Address :	123 main st
Phone No :	319-383-1065
Email Address :	jdoe@theinter.net
Serial Key :	____-____-____-____
Trial :	☑ Or 14 days Trial *All fields

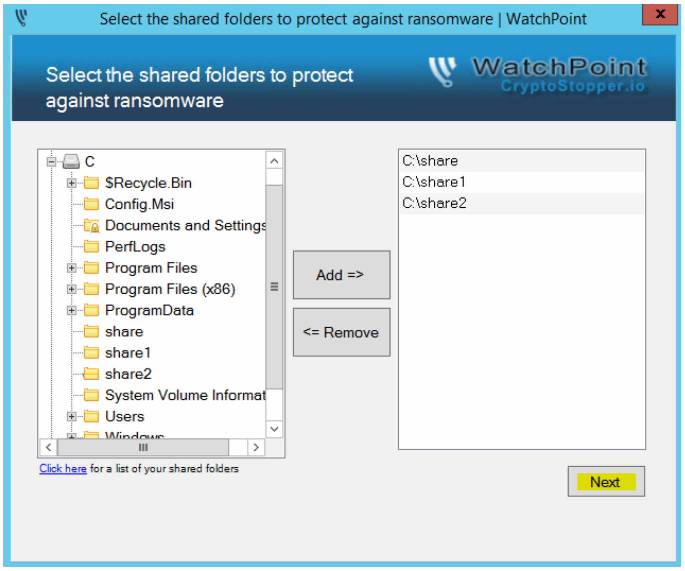
6) Now we need to select the shared folders that should be protected against ransomware. If you need assistance identifying your shared folders, select 'Click Here' and make a note of 'Folder Path' (see below).


Click here for a list of your shared folders



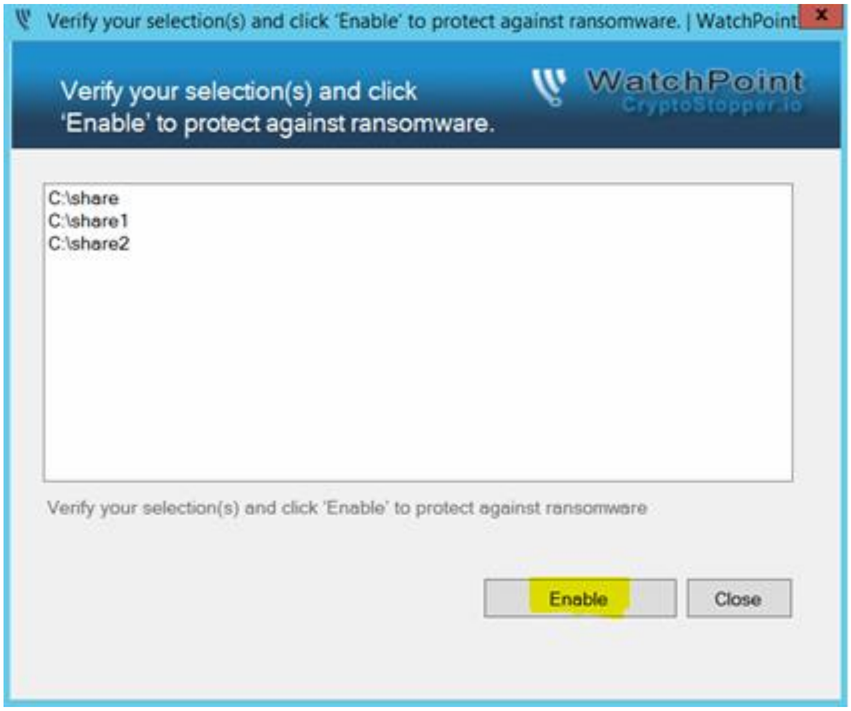
Share Name	Folder Path
ADMIN$	C:\Windows
C$	C:\
IPC$	
share	C:\share
share1	C:\share1
share2	C:\share2

7) Use the 'Add" button to select a folder and when ready click Next (see right).



C:\share
C:\share1
C:\share2

8) Verify the selection's and click Enable to protect the folders against ransomware. Wait for the command window to close, then select the close button.



Verify your selection(s) and click 'Enable' to protect against ransomware. | WatchPoint

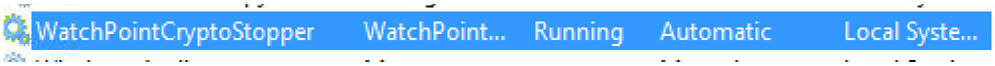
Verify your selection(s) and click 'Enable' to protect against ransomware.

C:\share
C:\share1
C:\share2

Verify your selection(s) and click 'Enable' to protect against ransomware

9) That's it.

But default CryptoStopper™ is running in the background but if you'd like to confirm that it's running you can do so via the Windows services. Verify that 'WatchPoint CryptoStopper' is running.

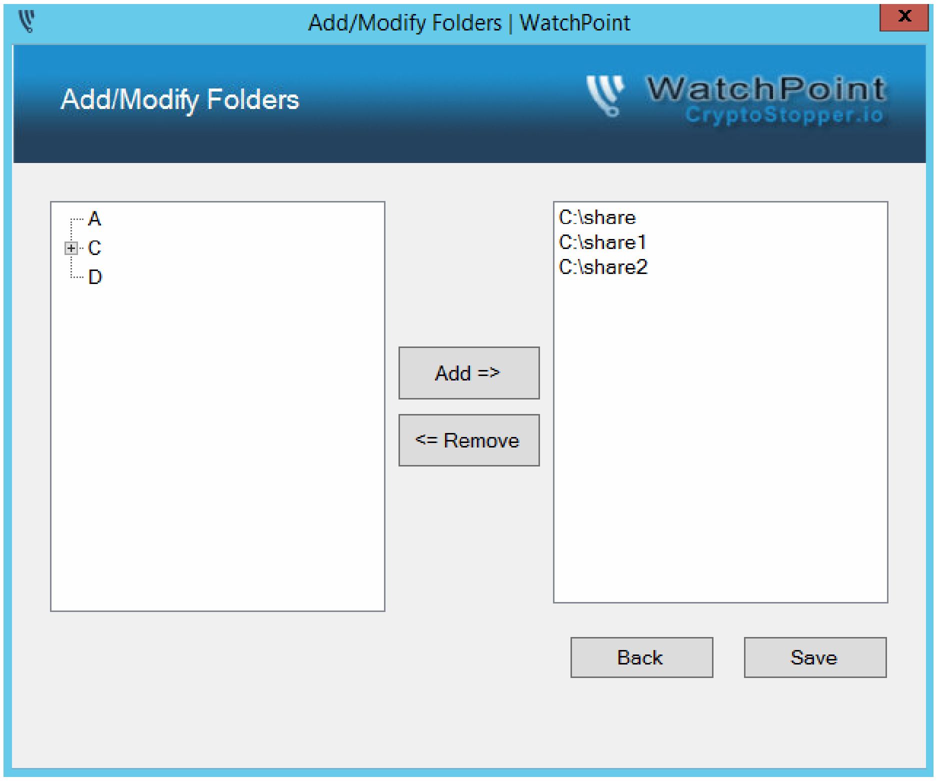


WatchPointCryptoStopper WatchPoint... Running Automatic Local Syste...

User Guide

Add/ Modify Protected Folders

In the right hand pane, you'll see the protected folders. In the left hand pane you'll see the local disk drives. Use the + sign to expand the drive and use the Add/Remove buttons to add or remove folders from CryptoStoppers protection. Use the Back button to go back to the previous screen. Be sure to Save any changes!

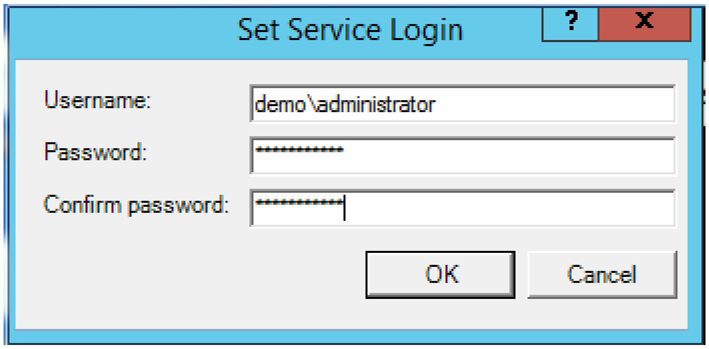


C:\share
C:\share1
C:\share2

Configure Service

As a recommended parameter you can configure the service to run as an administrator account. This allows CryptoStopper to send messages to the infected computers desktop and initiate the shutdown timer. The account should also have local admin rights to all of the domain computers.

Enter the username in 'domain\username' format. When ready click OK.


Set Service Login

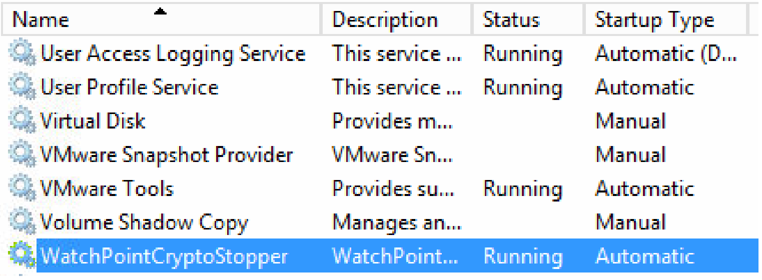
Username: demo\administrator

Password: *************

Confirm password: *************

To verify you've entered the correct information, check the 'WatchPointCryptoStopper' service.

When entered correctly, the status will be running:



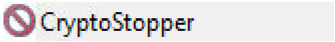
Name	Description	Status	Startup Type
User Access Logging Service	This service ...	Running	Automatic (D...
User Profile Service	This service ...	Running	Automatic
Virtual Disk	Provides m...		Manual
VMware Snapshot Provider	VMware Sn...		Manual
VMware Tools	Provides su...	Running	Automatic
Volume Shadow Copy	Manages an...		Manual
WatchPointCryptoStopper	WatchPoint...	Running	Automatic

When entered incorrectly, the status will be blank:

Remediation/Windows Firewall

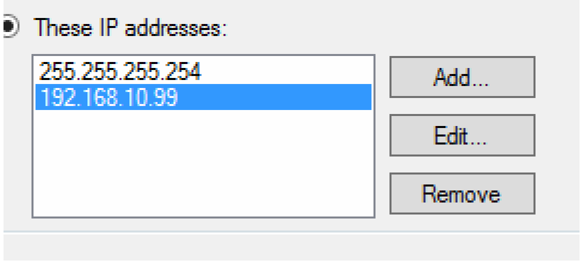
You should know what to do once an infected computer is identified and disconnected from the server. CryptoStopper™ creates a Windows firewall rule that blocks an infected computer and prevents it from connecting to the server.

By default the CryptoStopper™ rule is added, but no computers are blocked until ransomware activity is identified.


CryptoStopper

Once, an infected computer is identified, you'll use the scope tab to remove the infected computers IP address. Please note that 255.255.255.254 is there by default.

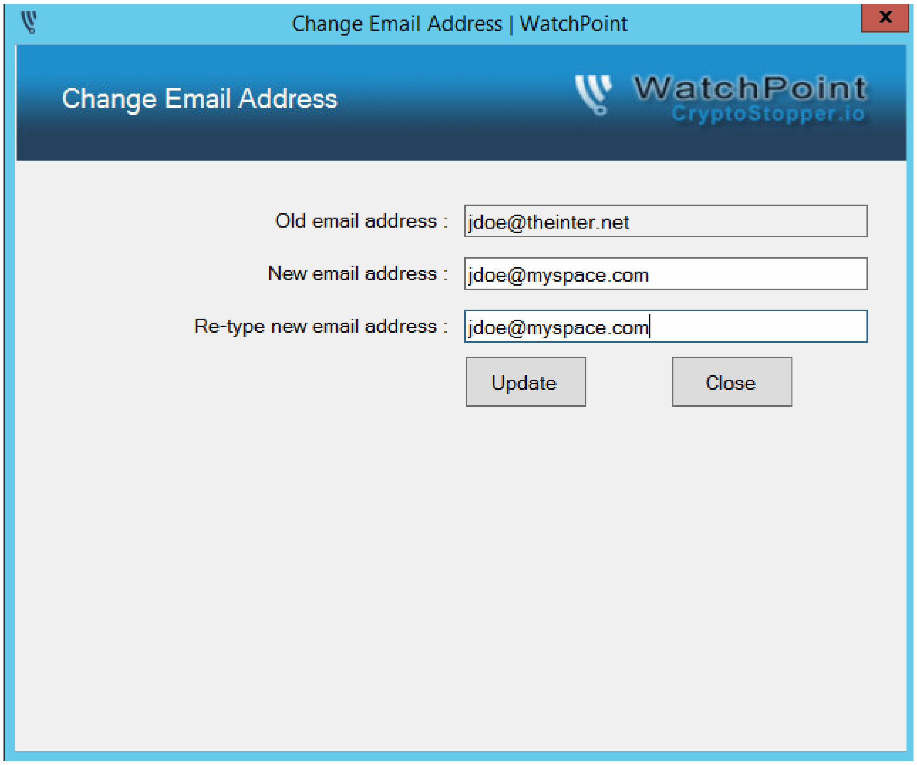
Simply select the infected computers IP address and click remove, then OK.


● These IP addresses:

255.255.255.254
192.168.10.99

Change Email Address

Note, this feature is only available with a valid license. To change your email address type the new email address once, and second time to confirm. Then select Update. Close when finished.


Change Email Address | WatchPoint

Change Email Address

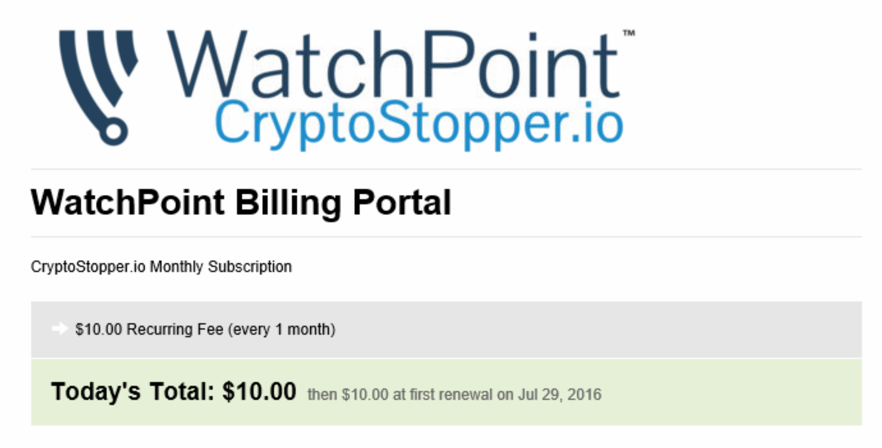
Old email address : jdoe@theinter.net

New email address : jdoe@myspace.com

Re-type new email address : jdoe@myspace.com

Buy Now

For just $10/server/month you can protect your server and the valuable data it holds from ransomware. We also have a 10 for 10 referral program. For every successful referral, you'll get free month of service!



WatchPoint™
CryptoStopper.io

WatchPoint Billing Portal

CryptoStopper.io Monthly Subscription

$10.00 Recurring Fee (every 1 month)

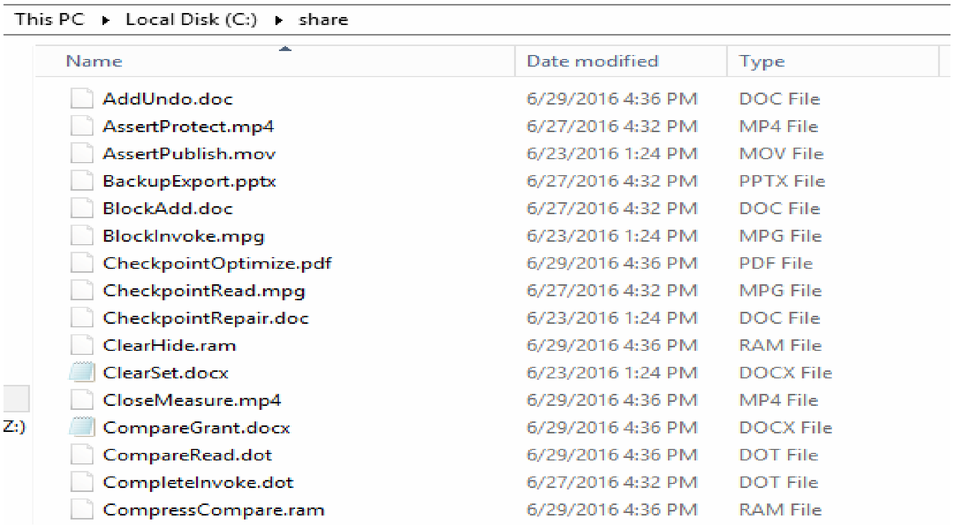
Today's Total: $10.00 then $10.00 at first renewal on Jul 29, 2016

Enter License Information

This is for paid licenses only. The license key will be emailed to you at the time of purchase. Simply enter the license key to activate the full version of CryptoStopper™.

Watcher Files

CryptoStopper™creates ‘Watcher Files’ within the directories selected for protection. The Watcher Files are used as bait by CryptoStopper™ as it continuously monitors the files for signs of ransomware activity. Below is an example of the Watcher Files created by CryptoStopper:



Name	Date modified	Type
AddUndo.doc	6/29/2016 4:36 PM	DOC File
AssertProtect.mp4	6/27/2016 4:32 PM	MP4 File
AssertPublish.mov	6/23/2016 1:24 PM	MOV File
BackupExport.pptx	6/27/2016 4:32 PM	PPTX File
BlockAdd.doc	6/27/2016 4:32 PM	DOC File
BlockInvoke.mpg	6/23/2016 1:24 PM	MPG File
CheckpointOptimize.pdf	6/29/2016 4:36 PM	PDF File
CheckpointRead.mpg	6/27/2016 4:32 PM	MPG File
CheckpointRepair.doc	6/23/2016 1:24 PM	DOC File
ClearHide.ram	6/29/2016 4:36 PM	RAM File
ClearSet.docx	6/23/2016 1:24 PM	DOCX File
CloseMeasure.mp4	6/29/2016 4:36 PM	MP4 File
CompareGrant.docx	6/29/2016 4:36 PM	DOCX File
CompareRead.dot	6/29/2016 4:36 PM	DOT File
CompleteInvoke.dot	6/27/2016 4:32 PM	DOT File
CompressCompare.ram	6/29/2016 4:36 PM	RAM File

The files are given random filenames and are created with the ‘Hidden’ attribute. The hidden attribute allows you to hide the Watcher Files from end users but not from ransomware. If ransomware ignored hidden files, then end users all around the world could simply hide their files to thwart ransomware. Ransomware developers are aware of this and thus they’ll always build their malware to search for hidden files.