Skip to content

Search… Search
Advanced search

- Anvisoft Forums ‹ Computer Help ‹ Malware Removal Guide
- Change font size
- Print view

- FAQ
- Register
- Login

How to Remove Citadel Malware Reveton Ransomware (Counterfeit IC3, FBI Malware Removal Guide)

Post a reply

Search this topic… Search

13 posts • Page 1 of 2 • 1, 2

How to Remove Citadel Malware Reveton Ransomware (Counterfeit IC3, FBI Malware Removal Guide)

by Sophia » 2012-08-17 3:24

This post depicts the Reveton ransomware which is delivered by Citadel Trojan and how to remove it in details. Read more.

What is Citadel Malware Reveton Ransomware?

Citadel malware/Trojan is a group which produces and delivers malware/Trojans while Reveton is ransomware created by Citadel malware/Trojan this is designed to serve the sole purpose of extorting money from unsuspicious online victims using credit schemes.

Similar to other ransomware like the FBI Moneypak virus and the Police Central e-crime Unit Virus, the Reveton ransomware is also known as Trojan: **W32/Reveton**. What sets Citadel Reveton malware and "ransomware" apart from others is that it locks computer system and lures victims to a drive by download site looking like the FBI or Internet Complaint Center (IC3.gov) with a message that claims the victims' IP address was identified by the Computer Crime & Intellectual Property Section (FBI) as visiting child pornography and other illegal content. To unlock their computer, victims are instructed to pay a $ 100 fine (or even more) to the US Department of Justice, using prepaid money card services (Green Dot Moneypak) which are complied based on the victims' IP geo location. That is to say, the malware will look up which payment platform properly suites the computer, as well as fraudulent authority organization. That is why it is called ransomware, which is malware that prevent users from accessing their computer unless a penalty fine is paid.

However, till now this is not all. Reveton ransomware could also installs to the computer systems and hides, waiting for credit systems to be initiated to steal privacy credit information and numbers. It is totally a scam to extort money as possible as it could be. If you are unfortunately locked by this ransomware out from your computer and asked for a ransom to pay to unlock, never let it do the trick and instantly move to below removal guide in details to get rid of it as soon as possible.

Threat Classification:

• Ransomware malware

Similar Ransomware Infections: FBI moneypak virus, PCeU virus (aka Metropolitan Police Ukash virus), Malex ransomware, Citadel Reventon Malware, United States Cyber Security virus, Your computer is locked for violating the Law of Great Britain virus, DOJ virus, File Encryption Virus, SGAE virus, Ay Cards Sí[illegible], Iceland's National Police Service virus, ISGA 2012 virus, Automated Information Control System virus

ACCDFISA Protection Program ransomware, Celas ransomware, Votre ordinateur est bloque! Gendarmerie Ukash virus, FBI Ultimate Game Card virus, Canadian Police Association Virus, Urausy virus/ransomware, Office Central de Lutte contre la Criminalité Virus, Bundesamt fur Polizei Virus, Canadian Police Cybercrime Investigation Department Virus, GEMA: Your computer has been locked virus, All Activity on This Computer Has Been Recorded-Fake FBI Warning infection, Den Svenska Polisen IT-Sakerhet Ransomware, Bundes Polizei Ukash virus, Australian Federal Police Ukash Virus, Internet Crime Crime Compliant Center ransomware virus, United States Department of Justice virus, Politia Romana virus, etc.

First off, be aware of the Symptoms of Reveton Ransomware Infection below:

1> Desktop and the OS is locked up.

2> Fraudulent authority message appears with a fraudulent claim

3> Internet redirects to a fake FBI or Internet Complaint Center (IC3) page and asks for a payment to unlock your computer system (Online complaint bureau depends on user's IP location)

Webcam control

Once infected, there would be a little more than usual that this ransomware virus would even attempt to trick the user into thinking they are under surveillance by webcam, as it always shows a fake screen in "recording" status. Actually this even makes no difference on the infected computer with no web cam at all. Apparently, the truth is ready to jump out at your call.

Deny Flash

Most ransomware exploits Java or Flash vulnerabilities to load the malicious code. In some cases denying or disabling flash on your system may suspend the Citadel Malware Reveton ransomware and enable the user to navigate through the infected system. If this not a necessity for removal, skip to the removal options below these steps.

To disable (deny) flash

1.Visit:http://www.macromedia.com/support/documentation/en/flashplayer/help/help09.html

2. Select the "Deny" radio option

3. Proceed to a removal option (detailed below).

How to Remove Citadel Malware Reveton Ransomware (Reveton Removal Guide)

Note! This tutorial is effective for all GreenDot MoneyPak, Ukash and Paysafecard ransomware.

There are several ways out to remove Citadel ransomware depending on the progression of the parasite. If you can still restart your computer to safe mode, you may opt to the Option 1 to remove the virus with ease. If the computer can still boot into safe mode, please follow the Option 1 removal steps to go. If the computer is completely blocked from anything, including safe mode running, then bet on Option 2 removal steps to go.

Removal Option 1-Safe Mode with Command Prompt Restore

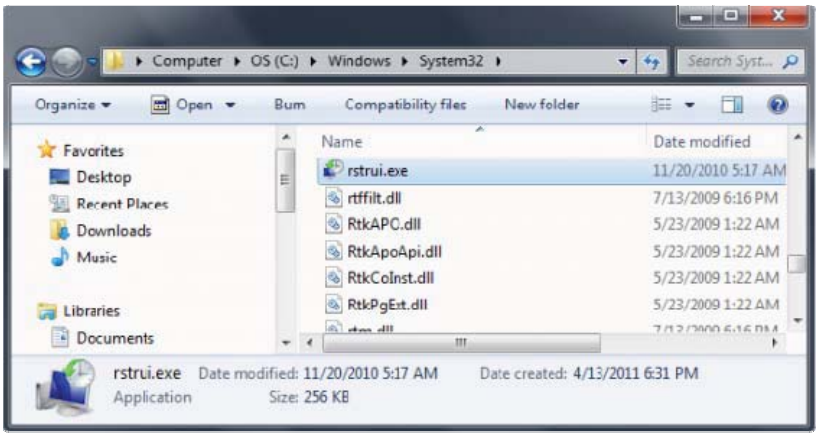
Step 1> Launch your PC into **Safe Mode with Command Prompt**. During the start, keep pressing **F8** key till the Advanced Windows Options Menu shows up and then use the arrow key on the keyboard to highlight the Safe Mode with Command Prompt option and then press **Enter**.
See detailed instructions on how to boot Windows to Safe Mode

Note: make sure you login your computer with administrative privileges. (login as admin)

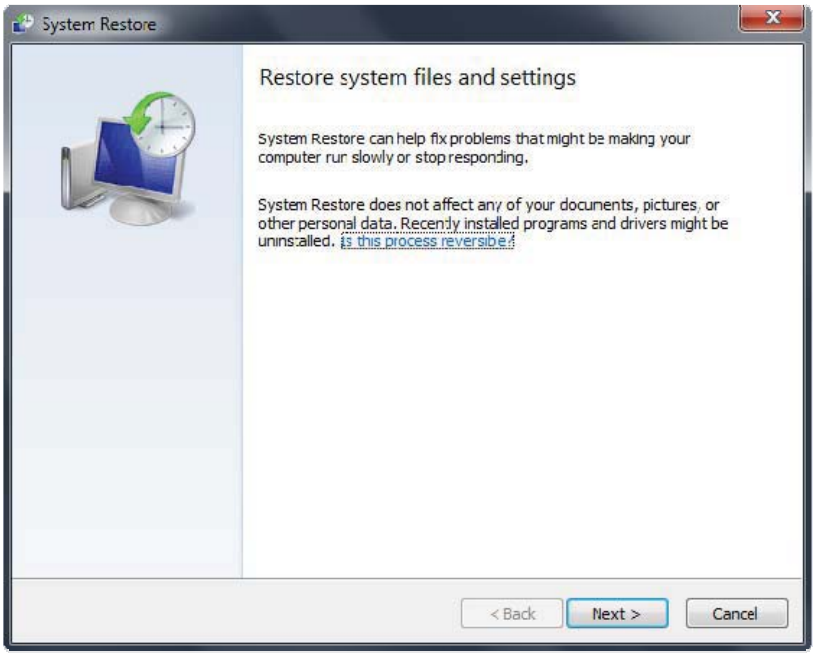
Step 2> Once the Command Prompt appears you only have few seconds to type “explorer” and hit Enter. If you fail to do so within 2-3 seconds, the ransomware virus will not allow you to type anymore.

Step 3> Once Windows Explorer shows up browse to:

Win XP: C:\windows\system32\restore\rstrui.exe and press Enter
Win Vista/Seven: C:\windows\system32\rstrui.exe and press Enter



Step 4> Follow all steps to restore or recover your computer system to an earlier time and date (restore point), before infection.

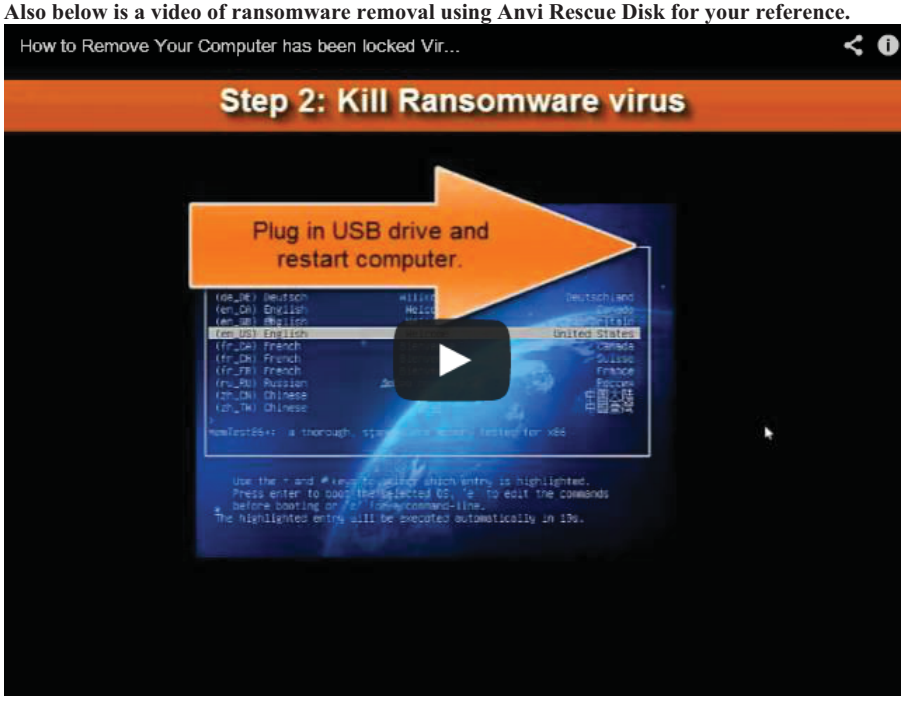


Step 5> Download, install, update and run**Anvi Smart Defender**(http://www.anvisoft.com/software/asd/. Remove all threats detected and reboot your PC.

Removal Option 2 Using Anvi Rescue Disk to Remove the Ransomware and Repair the Infected Computer

Chances are your PC is heavily infected by this ransomware that it is blocked from safe mode running as well. If such is the case, the removal may be a little bit complex and here we use Anvi Rescue Rescue Disk to demonstrate the removal steps and good luck to you. If any question in the process, just let us know.

Also below is a video of ransomware removal using Anvi Rescue Disk for your reference.



Step 1> Download the Anvi Rescue Disk isoimage file **Rescue.iso** and the USB disk production tool **BootUsb.exe** from Anvisoft official site.

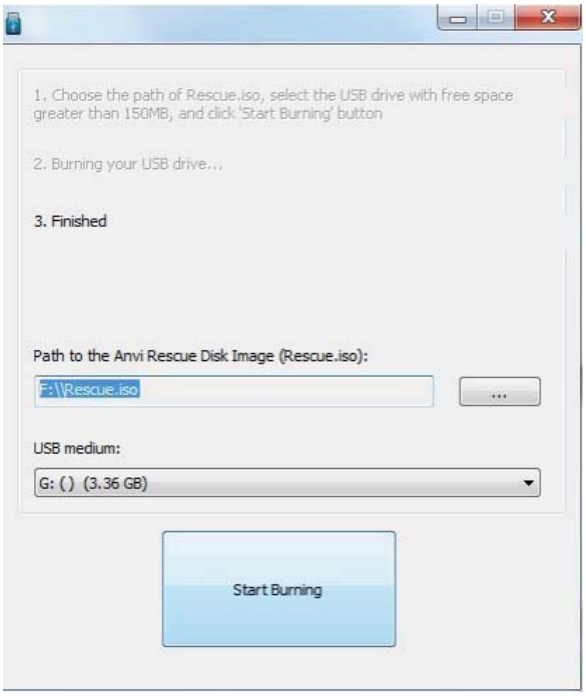
Direct download link: **http://download.anvisoft.com/software/rescuedisk.zip**

Please kindly note that **Rescue.iso** is a large file download; please be patient while it downloads.

Step 2> Record Anvi Rescue Disk iso image to USB drive. You can also record the iso image to a CD/DVD. We will introduce the steps to record iso image to a CD/DVD in following guide.

Connect USB to computer. You'd better backup your important data and format your USB drive before use it to record the iso image.

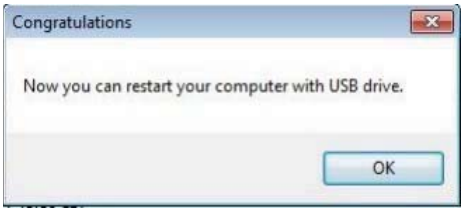
Locate your download folder and double-clicking on **BootUsb.exe** to start it. And then click "Choose File" button to browser into your download folder and select **Rescue.iso** file as your source file.



Select the path of USB drive, such as **Drive H:**

Click "**Start Burning**" to start the burn of USB Rescue Disk boot drive.

Please close BootUsb.exe tool after you successfully burn the file to USB drive when you get following message.

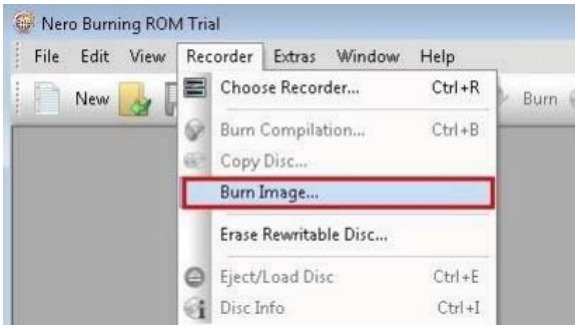


Now, you have bootable Anvi Rescue Disk to repair your computer.

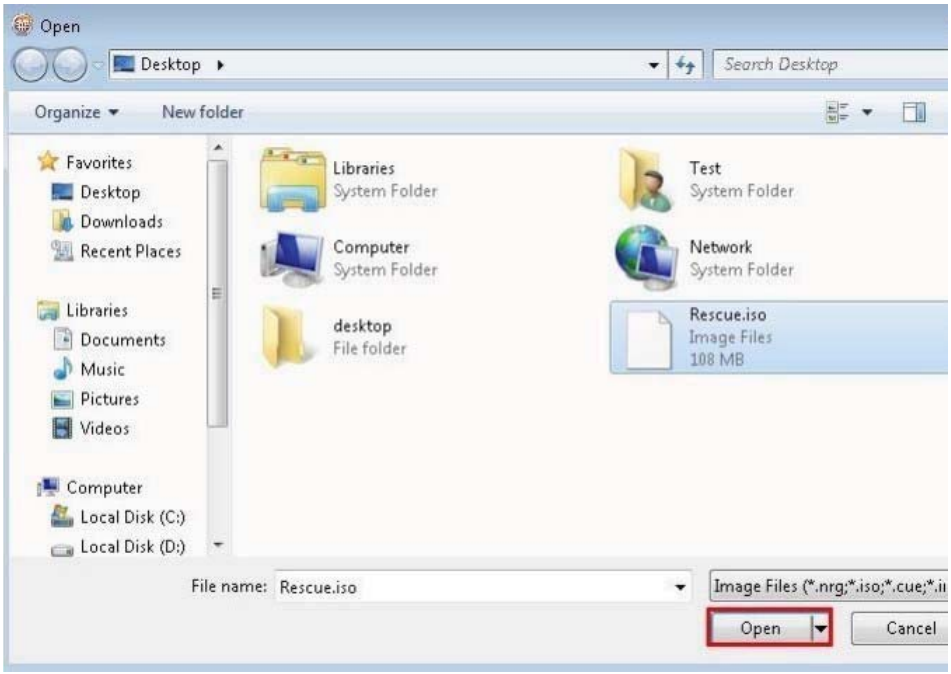
Alternative Option

You can also record Anvi Rescue Disk iso image to a DV/DVD. Any CD/DVD record software is fine for burn iso image. If you don't have any, you can download and install **Nero Burning ROM** and **ImgBurn**. Here we will use Nero Burning ROM for demonstration purpose.

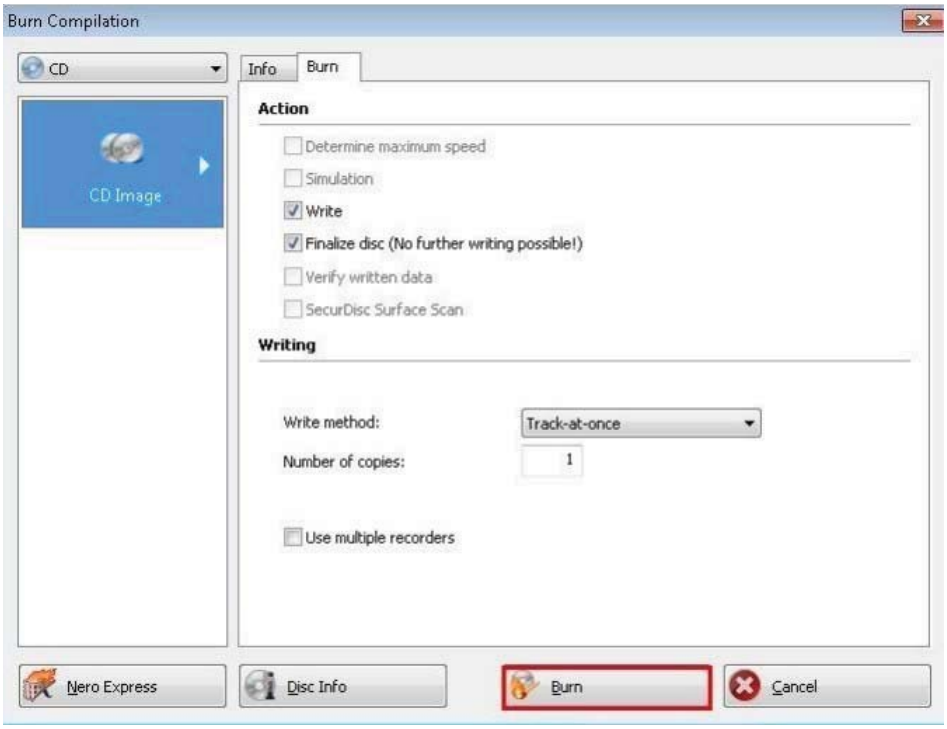
Please open and start Nero Burning ROM and select Burn Image from the drop-down menu of the Recorder.



Locate your download folder and select **Rescue.iso** file as your source file and then click **Open** button.



Click Burn button to start record the iso image. After a few minutes, you will have a bootable Anvi Rescue Disk to repair your computer.



Step 3>Restart your computer and configure your computer to boot from USB drive/DV/DVD that recorded Anvi Rescue Disk. Basically , you can use **F8** to load USB boot menu.

For different motherboard, you may need to use the **Delete** or **F2, F11** keys, to load the **BIOS** menu. Normally, the information how to enter the BIOS menu is displayed on the screen at the start of the OS boot.

The keys F1, F8, F10, F12 might be used for some motherboards, as well as the following key combinations:

• Ctrl+Esc
• Ctrl+Ins
• Ctrl+Alt
• Ctrl+Alt+Esc
• Ctrl+Alt+Enter
• Ctrl+Alt+Del
• Ctrl+Alt+Ins
• Ctrl+Alt+S

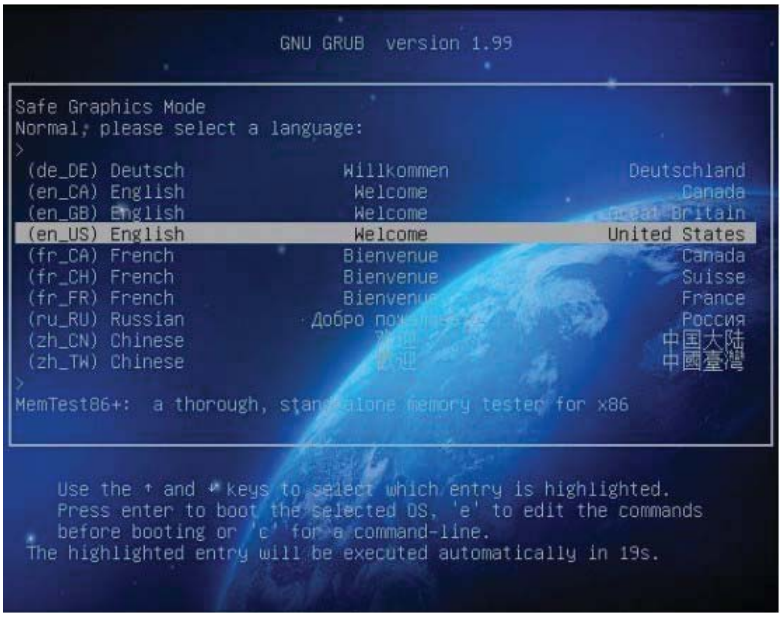
If you can enter **Boot Menu** directly then simply select your CD/DVD-ROM as your **1st boot device**.

If you can't enter **Boot Menu** directly then simply use Delete key to enter BIOS menu. Select Boot from the main BIOS menu and then select **Boot Device Priority**. After that, set CD/DVD-ROM as your 1st Boot Device. Save changes and exist BIOS menu.

Step> 4 After that let's boot your computer from Anvi Rescue Disk.

Restart your computer. After restart, a message will appear on the screen: press any key to enter the menu. So, press **Enter** or any other key to load the Anvi Rescue Disk

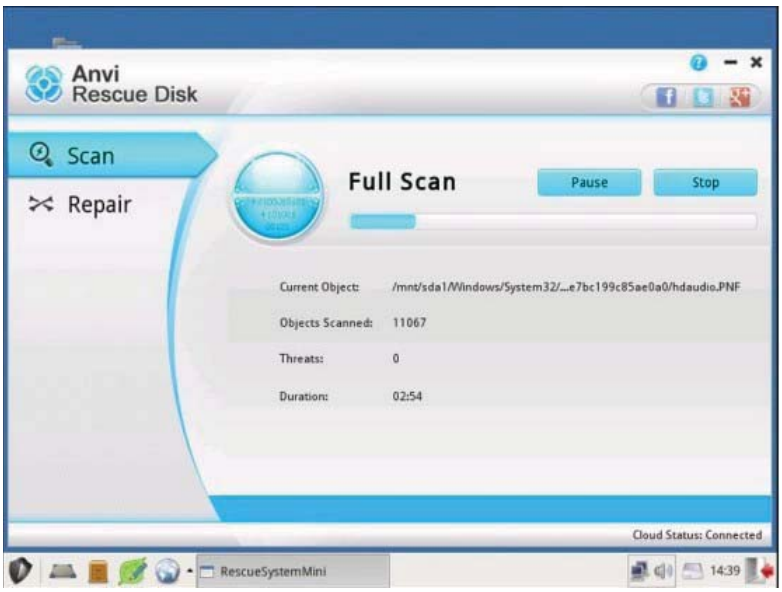
please selected your preferred language and press **Enter** to continue.



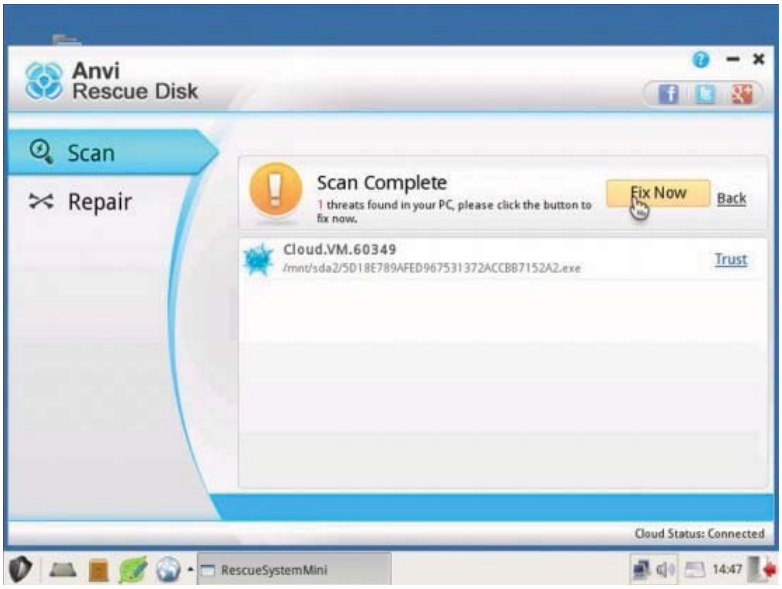
Step> 5 Now you are in the mini Operating system, please double click **Rescue** tool to start Anvi Rescue disk.

Step> 6 Make sure that your computer is connected to **network connection** before you run a scan on your computer. Please scroll down the file and check the tutorial if you fail to connect your computer to Internet.

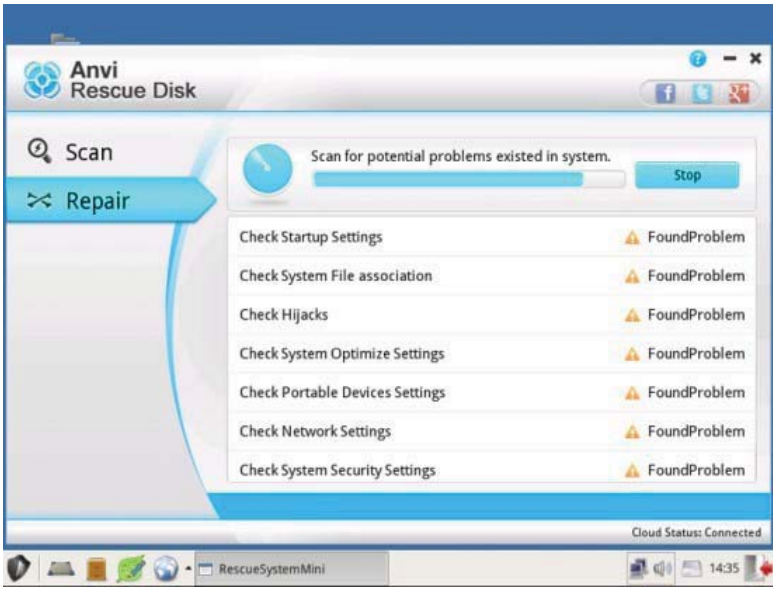
Step> 7 Please run a full scan by clicking the “Scan Computer” button in the middle of the program to detect and kill the PC lockup virus.



Step>8 Clicking “Fix Now” to Remove the detected threat by Anvi Rescue Disk.



Step> 9 Switch to Repair tab. Scan and fix the registry error with the “Repair” module of Anvi Rescue Disk.



Important Notice: You must repair the registry error after kill the virus. You are probably disabled to boot your Windows without fixing registry damaged by the virus.

Step>10 Now your computer should be clean and rescued from the virus infection. Please restart your computer into the normal Windows mode.

Please note, some ransomware infection variant is seriously persistent, so you are highly recommended to download the antimalware Anvi Smart Defender in the rescue disk menu when the scan and repair is finished just as shown in below picture:

In the prompt window, click **Yes** button to download and install Anvi Smart Defender and perform a full scan to ensure all possible files of the infection is removed.

To prevent the computer from infecting by such ransomware or related Trojans, please ensure you get proper protection on your computer and you may just keep the **Anvi Smart Defender** for this. Safe and direct download link: http://www.anvisoft.com/software/asd/

Else

You are suggested to turn on Security Features of your browser to better secure your surfing activities online. See detailed steps to turn on security features of IE, or Firefox or Google Chrome.

Good luck and be safe online.

Sophia
Anvisoft Staff

Posts: 532
Joined: 2012-04-16 3:32

Top

Re: How to Remove Citadel Malware Reveton Ransomware (Counterfeit IC3, FBI Malware Removal Guide)

by **Sophia** » 2012-08-17 3:30

Hi, all

Just hope this article help to you. If any questions/practices/experiences related, please leave your reply here for further discussion. We Anvisoft team have been dedicated to provide useful information and practical software to help you solve the PC issue, particularly in the field of online security and computer maintenance. If you may just share any of your practices or practical needs here to let us know your needs better, we believe this may encourage us a lot to work harder to meet your needs and improve our services and software. Thanks for any support from you in advance.

Wish you good luck and be safe online.
Imagination is more important than Knowledge!

Sophia
Anvisoft Staff

Posts: 532
Joined: 2012-04-16 3:32

Top

Re: How to Remove Citadel Malware Reveton Ransomware (Counterfeit IC3, FBI Malware Removal Guide)

by **tina** » 2012-08-20 0:41

I finally found the information I wanted here. Thank you so much

tina
Member

Posts: 30
Joined: 2012-08-16 1:13

Top

Re: How to Remove Citadel Malware Reveton Ransomware (Counterfeit IC3, FBI Malware Removal Guide)

by **Sophia** » 2012-08-20 22:07

> *tina wrote:*I finally found the information I wanted here. Thank you so much

Hi, Tina

Happy to be helpful and thanks for your appreciation.

Wish you good luck and be safe online

Imagination is more important than Knowledge!

Sophia
Anvisoft Staff

Posts: 532
Joined: 2012-04-16 3:32

Top

Re: How to Remove Citadel Malware Reveton Ransomware (Counterfeit IC3, FBI Malware Removal Guide)

by **Lynne Henry** » 2012-10-05 23:51

So is there anything I can do for my dad's pc he has had this installed on his pc and I tried everything that I can do with not being an IT Pro including the "starting in command prompts" and what happens to his pc is whenever I try to install the anvi program it shuts down totally and when I was in the command prompts doing the search it did the same thing and shut down totally. Can you give me an idea of what to do or does he need to just take it to a pro. Also once I install the anvi program how can i keep this from getting installed on my pc will it automatically catch it if they try or will I get notification? I plan on running it every night before the total shut down for the day but I was just wondering if there is a preventative measure that will catch it before it can be installed.

Lynne H

Member

Posts: 1
Joined: 2012-10-05 23:46

Top

Re: How to Remove Citadel Malware Reveton Ransomware (Counterfeit IC3, FBI Malware Removal Guide)

by **FrustratedInMaine** » 2012-10-06 21:16

Hi. New here, sorry to bump this thread. I've become infected with this bastard, and I've followed your instructions for self-removal. However, none of the files appear in appdata/local/temp. None. What should I do?

I've done searches. No .mof files appear.

FrustratedInMaine
Member

Posts: 1
Joined: 2012-10-06 21:13

Top

Re: How to Remove Citadel Malware Reveton Ransomware (Counterfeit IC3, FBI Malware Removal Guide)

by **Sophia** » 2012-10-07 15:17

> *FrustratedInMaine wrote:*Hi. New here, sorry to bump this thread. I've become infected with this bastard, and I've followed your instructions for self-removal. However, none of the files appear in appdata/local/temp. None. What should I do?
>
> I've done searches. No .mof files appear.

Hello

Well, then you may try the system restore method there to fix the issue since the injected files or infected files may vary a lot across computer. By the way, the System Restore could 90% do the trick to help you out. However, after you do that, if the issue is still stubborn there, please get in touch and better send us the technical data for our engineer to figure it out and help.

Good luck. Any further feedback, just let us know.
Imagination is more important than Knowledge!

Sophia
Anvisoft Staff

Posts: 532
Joined: 2012-04-16 3:32

Top

Re: How to Remove Citadel Malware Reveton Ransomware (Counterfeit IC3, FBI Malware Removal Guide)

by **Sophia** » 2012-10-16 2:22

> *Lynne Henry wrote:*So is there anything I can do for my dad's pc he has had this installed on his pc and I tried everything that I can do w

> program it shuts down totally and when I was in the command prompts doing the search it did the same thing and shut down totally. Can you give me an idea of what to do or does he need to just take it to a pro. Also once I install the anvi program how can i keep this from getting installed on my pc will it automatically catch it if they try or will I get notification? I plan on running it every night before the total shut down for the day but I was just wondering if there is a preventative measure that will catch it before it can be installed.

Hi, Lynne Henry

Sorry for the late reply. Just hope the issue has been fixed now. Actually, according to what you said, this virus belongs to the boot-sector virus that is considerably stubborn. However, to handle such a situation, you may just check out the removal guide here: http://forums.anvisoft.com/viewtopic-45-905-0.html See the alternative removal part for another try (this removal guide can also apply to your situation as well).

If all the measures failed to work, I'm afraid that you need to reinstall the Windows OS for complete repair.

Good luck and be safe online.
Imagination is more important than Knowledge!

Sophia
Anvisoft Staff

Posts: 532
Joined: 2012-04-16 3:32

Top

Re: How to Remove Citadel Malware Reveton Ransomware (Counterfeit IC3, FBI Malware Removal Guide)

by **Careohline Amblur** » 2012-10-17 19:37

From Saskatoon, Canada.. thanks so much for the info.. all is good as new! the inlaws got infected & freaked out when the webcam turned on! lol

Careohline Amblur
Member

Posts: 1
Joined: 2012-10-17 19:32

Top

Re: How to Remove Citadel Malware Reveton Ransomware (Counterfeit IC3, FBI Malware Removal Guide)

by **Ivy** » 2012-10-18 3:52

> *Careohline Amblur wrote:*From Saskatoon, Canada.. thanks so much for the info.. all is good as new! the inlaws got infected & freaked out when the webcam turned on! lol

Hi,
Welcome to Anvisoft forum. Please feel free to post here and communicate with other members.
Anvisoft--A leading Internet security solutions provider

Ivy
Anvisoft Staff

P

Joined: 2012-01-16 21:05
- Website

Top

Next Display posts from previous: All posts · Sort by Post time · Ascending · Go

Post a reply
13 posts • Page **1** of **2** • **1**, 2

Return to Malware Removal Guide

Jump to: Malware Removal Guide · Go

Random Threads

Thread	Thread Starter	Views
How to Remove Reveton Trojan Ransomware from Your Computer Completely? (Manual Removal Guide)	Autumn	3904
How to Remove search.conduit.com Hijacker (search.conduit.com Toolbar Uninstall Instructions)	Sophia	57767
Microsoft Windows "Su Licencia ha Caducado" SMS Verification Scam-how to Remove and Prevent	Sophia	146
How to Change the Default Search Provider in IE/FF/Chrome?	Ocean	2085
How to Remove Google Redirect Virus Completely from Your Computer? (Manual Removal Guide)	Autumn	2074

Who is online

Users browsing this forum: No registered users

- Anvisoft Forums
- The team • Delete all board cookies • All times are UTC - 5 hours

How To Remove Citadel Malware Reveton Ransomware (Fake IC3, FBI Malware)

What Is Citadel Malware Reveton Ransomware?

Citadel Malware is a group which produces and supplies malware as well as a name for malware distributed by cyber criminals for public use. **Reveton** is **ransomware** malware created by Citadel Malware that is designed for the sole purpose of extorting money from unsuspecting online victims using credit schemes.

Similar ransomware includes the FBI Moneypak Virus (FBI Virus) and the Police Central e-crime Unit Virus.

Reveton ransomware is also known as **Trojan:W32/Reveton.**

What makes Citadel Reveton malware and “ransomware” unique is that it locks computer systems and lures victims to a drive by download site appearing like the FBI or Internet Complaint Center (IC3.gov) with a message that alleges the victims IP address was identified by the Computer Crime & Intellectual Property Section (FBI) as visiting child pornography and other illegal content. To unlock their computer, victims are instructed to pay a $100 fine (or more) to the US Department of Justice, using prepaid money card services (Green Dot Moneypak) which are compiled based upon the victims IP geo location. (Meaning the malware will look up which payment platform properly suites the computer, as well as fraudulent authority organizaion) This is where the term

“ransomware” derives from, as ransomware is malware which prevents users from accessing their computer unless a penalty fine is paid.

That is not the only issue with Reveton Ransomware. Reveon Ransomware also downloads to computer systems and hides, waiting for credit systems to be initiated to steal private credit information and numbers. Reveon Ransomware is used in a lot of credit card schemes to extort money.

Reveton ransomware symptoms

1. Desktop and operating system locks up
2. Fraudulent authority message appears with a fraudulent claim
3. Internet redirects to a fake FBI or Internet Complaint Center (IC3) page and demands a payment to unlock your computer sytem (online complaint bureau depends on user IP location)

How to remove Citadel Malware Reveton Ransomware

There are many ways to remove Citadel ransomware depending on the progression of the parasite. If you can access the internet while infected it is suggested to proceed to option 1 and install the free version of Malwarebytes to scan and remove the ransomware virus from your computer. If you know your way around Window’s OS, it is suggested to chose the manual removal option (option 2). For other issues a solution to remove Reveton is to restore your computer to a date and time before infection (option 3).
For additional removal steps and symptoms please check out the FBI Moneypak removal steps.

1. Malware Removal Sofware

Malwarebytes offers a free and paid version. The free version has been publicly documented to remove Citadel’s malware and the paid version will ensure that ransomware infections will never happen to your system again.

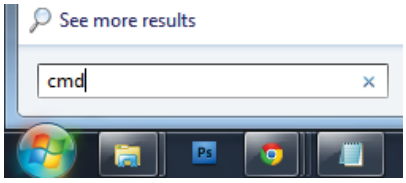
Remove Malware

2. Manual Removal Instructions

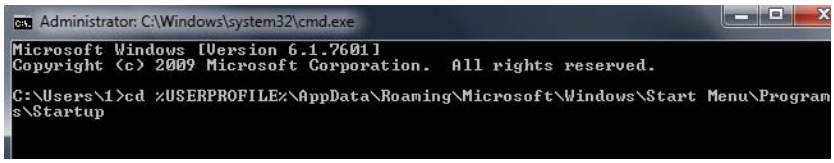
The hardest of the manual removal process part is finding the appropriate dll file to remove. Citadel’s malware is mass distributed (we all could go acquire it right now online for free if we wanted) and because of this the exact dll. file for Reveton ransomware can be hard to locate.

Windows command

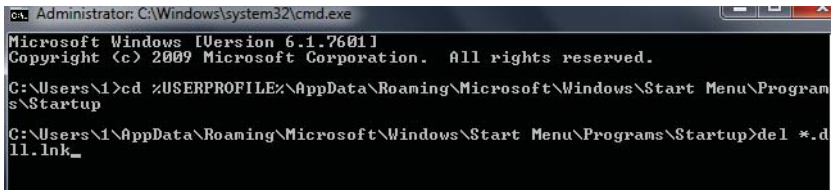
Access Windows **start menu**
Type: **cmd** (or c:\windows\system32\cmd.exe) and press **enter** to run program



In the command prompt displayed, type in one of the following commands below and press Enter, depending on your operating system:
Windows XP: **cd %USERPROFILE%\Start Menu\Programs\Startup**
Windows 7: **cd %USERPROFILE%\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup**



From the same command prompt type: **del *.dll.lnk** and press Enter



Reboot or restart your machine to complete, then move to the step below.

Remove the .dll file

Upon execution, Reveton malware will create the following which must be removed:

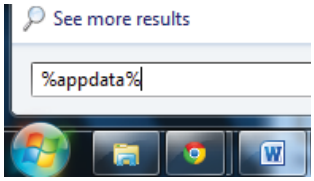
Search and remove the .dll file. If you can not find the correct file (which can be tricky) malware removal is strongly suggested.

<*reveton_filename*> can be a sequence of random letters and numbers.

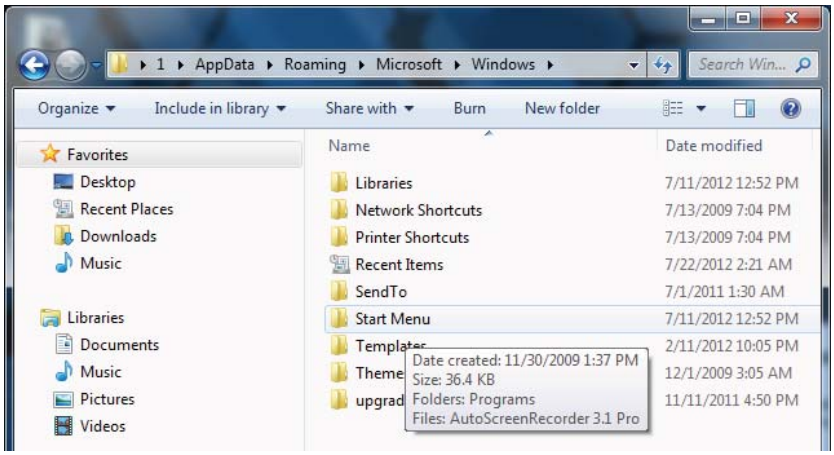
- **On Windows XP**
  %USERPROFILE%\Start Menu\Programs\Startup\<*reveton_filename*>.dll.lnk
- **On Windows 7**
  %USERPROFILE%
  \AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\<*reveton_filename*>dll.lnk

Other manual removal options

These following removal steps are taken from the FBI Moneypak virus removal instructions essentially the same virus, just different progressions for geographic locations).
1. Open Windows Start Menu and type %appdata% into the search field, press Enter.

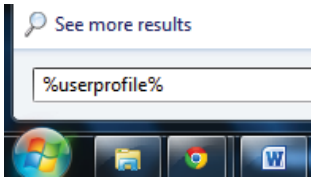


2. Navigate to: Microsoft\Windows\Start Menu\Programs\Startup



3. Remove ctfmon (ctfmon.lnk if in dos) – this is what's calling the virus on startup

4. Open Windows Start Menu and type %userprofile% into the search field and press enter.



5. Navigate to: Appdata\Local\Temp
6. Remove rool0_pk.exe
7.Remove [random].mof file
8. Remove V.class

The virus can have names other than "rool0_pk.exe" but it should appear similar, there may also be 2 files, 1 being a .mof. Removing the .exe file will fix FBI Moneypak. The class file uses a java vulnerability to install the virus, removal of V.class is done for safe measure.

All FBI Moneypak files:

The files listed above are what causes FBI Moneypak to function. To ensure FBI Moneypak is completely removed via manually, please delete all given files. Keep in mind, [random] can be any sequence of numbers or letters.

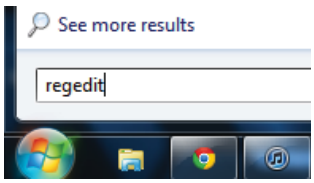
```
%Documents and Settings%\[UserName]\Desktop\[random].lnk
%Program Files%\FBI Moneypak Virus
%AppData%\Protector-[rnd].exe
```

```
%AppData%\Inspector-[rnd].exe
%Windows%\system32\[random].exe
%appdata%\[random].exe
%Documents and Settings%\[UserName]\Application Data\[random].exe
%UserProfile%\Desktop\FBI Moneypak Virus.lnk
%Documents and Settings%\All Users\Application Data\FBI Moneypak Virus
%AppData%\result.db
%CommonStartMenu%\Programs\FBI Moneypak Virus.lnk

Kill ROGUE_NAME processes:


Access Windows Task Manager (Ctrl+Alt+Delete) and kill the rogue process. P
```

```
[random].exe
```

Remove Registry Values

To access Window's Registry Editor type **regedit** into the Windows Start Menu text field and press Enter.

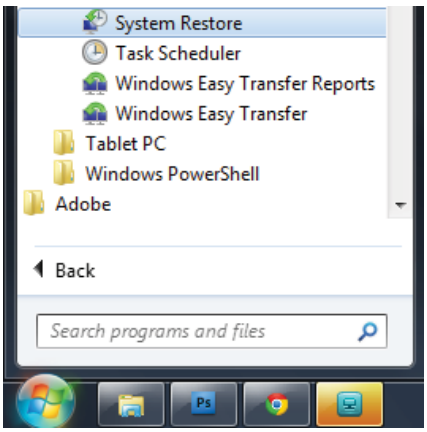



```
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\[random].ex
HKEY_LOCAL_MACHINE\SOFTWARE\FBI Moneypak Virus
HKEY_CURRENT_USER \Software\Microsoft\Windows\CurrentVersion\Policies\Syste
HKEY_LOCAL_MACHINE \SOFTWARE\Microsoft\Windows\CurrentVersion\policies\syst
HKEY_CURRENT_USER \Software\Microsoft\Windows\CurrentVersion\Internet Setti
HKEY_CURRENT_USER \Software\Microsoft\Windows\CurrentVersion\Policies\Syste
HKEY_CURRENT_USER\Software\FBI Moneypak Virus
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run 'Inspector'
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\FBI
HKEY_CURRENT_USER \Software\Microsoft\Windows\CurrentVersion\Policies\Syste
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\Inspector %
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settin
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Settings\net [d
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\policies\syste
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\System
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\System
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\policies\syste
```

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\policies\syste
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\policies\syste
```

3. System Restore

Start Menu Restore



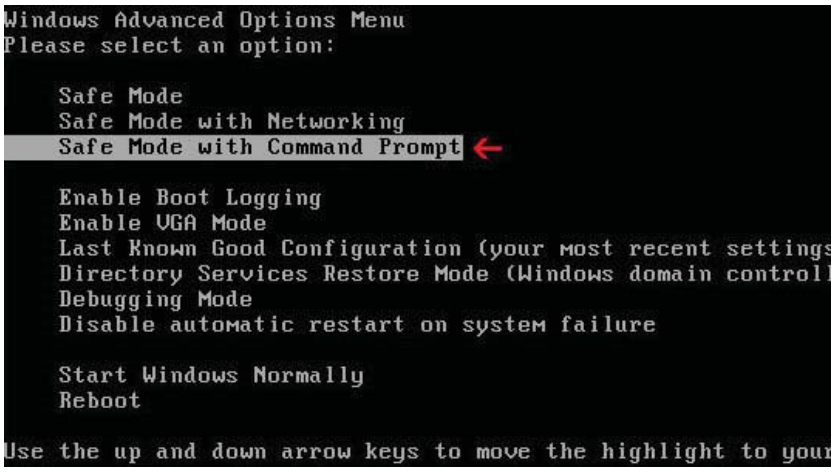
Standard directions to quickly access Window's System Restore Wizard (rstrui).

1. Access windows **Start menu** and click **All Programs.**
2. Click and open **Accessories,** click **System Tools,** and then click **System Restore.**
If you are prompted for an administrator password or confirmation, type the password or provide confirmation.
3. Restore your computer to a date and time before infection.

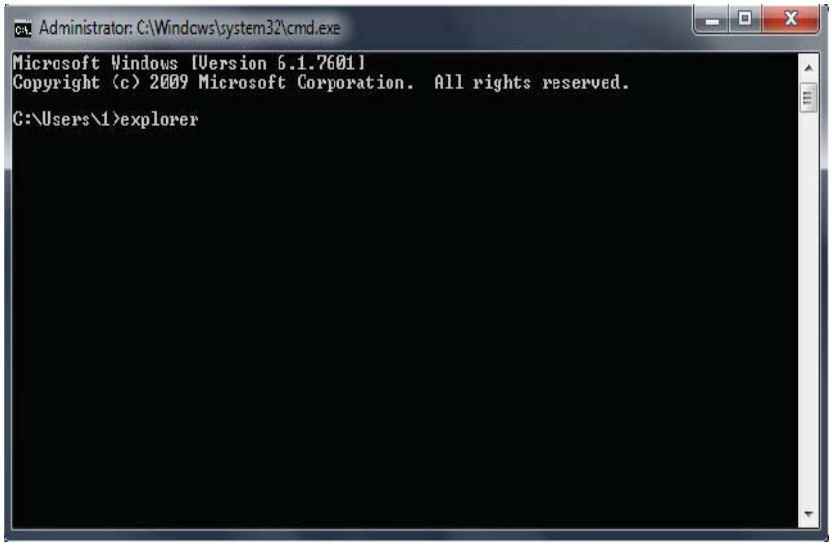
Safe Mode With Command Prompt Restore

If you can not access your operating system, this is the suggested step.

1. **Restart/reboot** your computer system. Unplug if necessary.
2. Enter your computer in **"safe mode with command prompt"**. To properly enter safe mode,repeatedly press**F8** upon the opening of the boot menu.

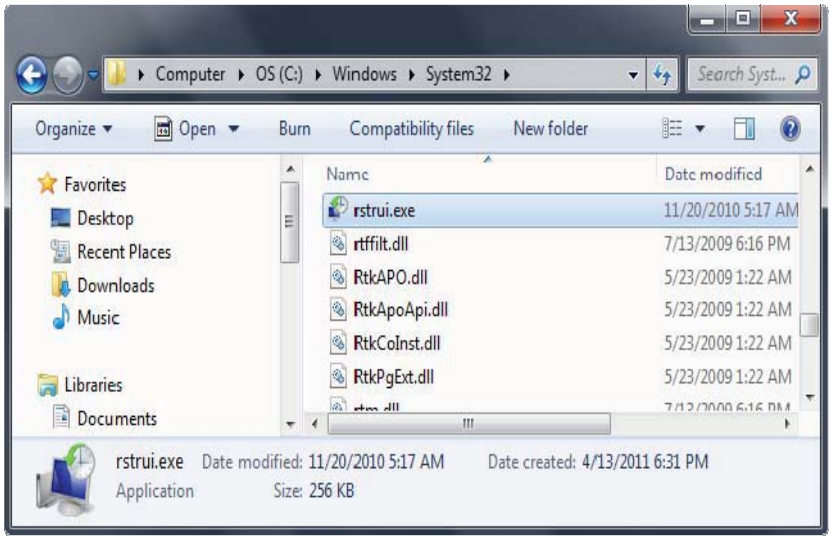


3. Once the Command Prompt appears you only have few seconds to type **"explorer"** and **hit Enter.** If you fail to do so within 2-3 seconds, the FBI MoneyPak ransomware virus will not allow you to type anymore.

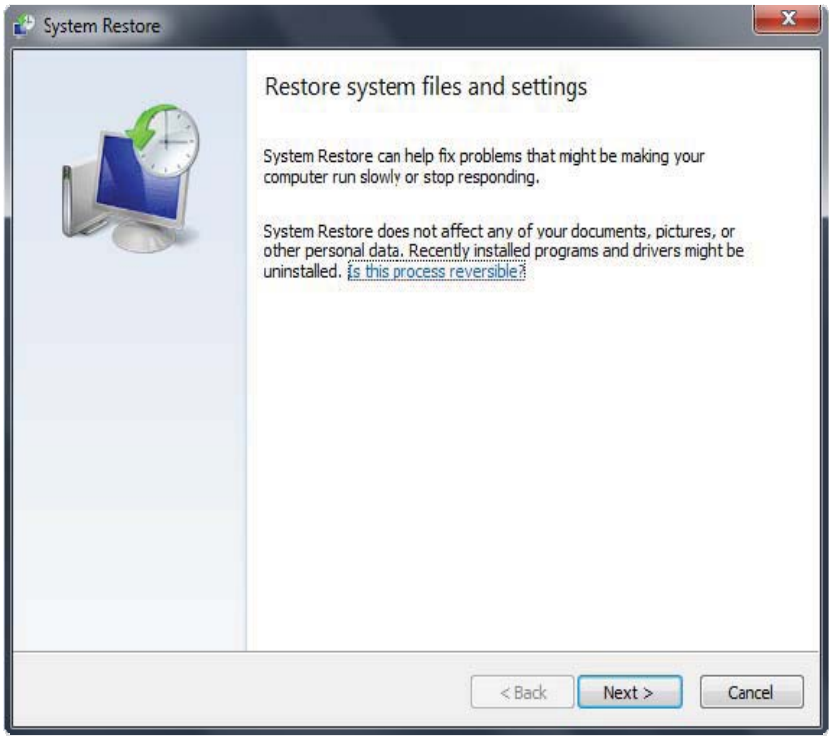


4. Once Windows Explorer shows up browse to:

- *Win XP:* **C:\windows\system32\restore\rstrui.exe** and press Enter
- *Win Vista/Seven:* **C:\windows\system32\rstrui.exe** and press Enter



5. Follow all steps to restore or recover your computer system to an earlier time and date, before infection to complete.



More information on Window's system restore: http://botcrawl.com/how-to-restore-microsoft-windows-vista-microsoft-windows-xp-and-microsoft-windows-7/ http://windows.microsoft.com/en-US/windows-vista/System-Restore-frequently-asked-questions

Here is an example of what multiple ransomware attacks look like in different countries.

This entry was posted in Malware, Blog and tagged Ransomware, Trojan, Windows on July 3, 2012 by Sean Doyle.

About Sean Doyle

Sean Doyle is a Cyber Security Expert from Thousand Oaks, CA (USA).

View all posts by Sean Doyle →

← How To Replace HTML Characters With HTML Entities In WordPress Comments

Does Https Create Duplicate Content On Search Engines? (SSL Certificates) →

11 replies to “How To Remove Citadel Malware Reveton Ransomware (Fake IC3, FBI Malware)”

Mike **August 16, 2012 at 4:08 am**
Did the restore it worked ran the malware, I do I know that it is completely off the computer

Mike **August 16, 2012 at 4:08 am**
How do I know??

Post author

Sean Doyle **August 16, 2012 at 4:21 am**
A suggestion to ensure removal is complete is to install the free version of Malwarebytes, perform a scan, and search through the results (since Malwarebytes does detect and remove FBI related malware). Once you are satisfied with your results you may remove the free version of Malwarebytes or continue to use it for scans in the future.
The free version of AVG has been documented to detect and remove the infection as well.

Harry **August 11, 2012 at 3:25 pm**
The virus took control of our server and blocked the screen with the message demanding money. The server runs Windows Business Server 2003. I can’t access the server using remote desktop connection. Also, DOS program on workstations won’t open. Is that because the server is blocked? I hope someone can help.
Thanks, Harry

Anonymous **August 10, 2012 at 9:32 pm**
restore system worked. thanks Tim

Post author

Sean Doyle **August 10, 2012 at 9:35 pm**
Glad to hear you got rid of it, I was just about to reply to your previous comment with the information below.
1. Open Windows Start Menu and type %appdata% into the search field, press Enter.
2. Navigate to: Microsoft\Windows\Start Menu\Programs\Startup
3. Remove ctfmon (ctfmon.lnk if in dos) – this is what’s calling the virus on startup
4. Open Windows Start Menu and type %userprofile% into the search field and press enter.
5. Navigate to: Appdata\Local\Temp
6. Remove rool0_pk.exe
7.Remove [random].mof file
8. Remove V.class
The virus can have names other than “rool0_pk.exe” but it should appear similar, there may also be 2 files, 1 being a .mof. Removing the .exe file will fix the virus. The class file uses a java vulnerability to install the virus, removal of V.class is done for safe measure.
Source: http://botcrawl.com/how-to-remove-the-fbi-moneypak-ransomware-virus-fake-fbi-malware-removal/

Anonymous **August 10, 2012 at 8:38 pm**
I am running Malware bytes and it finds the Citadel malware and quarantines it, however the file when quarantined or deleted, keeps reproducing it’s self. File is ctfmon.lnk. How do I stop it? Thanks Tim
tmutahi **August 10, 2012 at 4:58 am**
How To Remove Citadel Malware Reveton Ransomware (Fake IC3, FBI Malware) http://t.co/cNfXaaAp cc @iamugendi @dungdungu

Anonymous **July 15, 2012 at 8:23 am**
None of these methods have worked for me. As soon as I go back to explorer the FBI screen is back.

Post author

Sean Doyle **July 15, 2012 at 9:31 am**
If you performed a restore via Safe Mode With Command Prompt you will have no issue.
It's the last option under 3. System Restore. I suggest you try it out.

Anonymous **July 13, 2012 at 7:48 pm**
Whoever created this – THANKS! Did the restore and it worked perfectly!