

# EXAMPLE OF A VIRUS & MALWARE CLEANUP FOR A "WINDOWS" COMPUTER

## SUMMARY:

Here is an example of the successful use of our malware cleanup procedure on December 3, 2011.

## MALWARE INFECTION

A computer user running "Windows XP" with "Service Pack 3", inadvertently downloaded a malicious file attachment in a bogus e-mail message. The malicious file attachment infected her computer with a cocktail of malware. Within minutes, the malware had opened approximately 70 windows of malicious adware. Each window claimed that the computer had contracted various items of malware. The computer user was no longer able to use her computer for any function including Internet access.

The bogus e-mail message looked like this:

From: "DHL US Services" <customer.services@dhl.com>  
To: [REDACTED]  
Date: 30 Nov 2011 18:21:21 -0600  
Subject: DHL Shipment NR NR#708881

Dear customer,

Your parcel has arrived at the post office on November 22.

Our Driver was unable to deliver the parcel to your address.

To receive a parcel you must go to the nearest DHL office and show your post label.

The post label is attached to this letter.

Thank you for your attention.

DHL Global Mail.

Places for DHL for near Tucson, AZ 85730

DHL Global Forwarding

[www.dhl-dgf.com](http://www.dhl-dgf.com)

Place page

2949 191

Tucson

(520) 294-2659

DHL Express

[www.dhl-usa.com](http://www.dhl-usa.com)

Place page

3757 E Columbia St

Tucson, Arizona

(520) 748-2883

# MALWARE CLEANUP

We meticulously followed Harry Elver's cleanup procedure that is described at

[http://aztcs.org/meeting\\_notes/winhardsig/malwarecleanup/malwarecleanup.htm](http://aztcs.org/meeting_notes/winhardsig/malwarecleanup/malwarecleanup.htm)

and the computer was returned to full functionality.

# MALWARE CLEANUP POSTMORTEM

Here are some screenshots that we made while cleaning up the computer:



## Potential threat details

Security Essentials detected 1 potential threat that might compromise your privacy or damage your computer. Your access to these items may be suspended until you take an action.

Click Show details to learn more. [What are alert levels?](#)

Detected items	Alert level	Status	Recommended act...
Trojan:Win32/FakeSysdef	Severe	Suspended	Remove

**Category:** Trojan

**Description:** This program is dangerous and executes commands from an attacker.

**Recommended action:** Remove this software immediately.

Security Essentials detected programs that may compromise your privacy or damage your computer. You can still access the files that these programs use without removing them (not recommended). To access these files, select the Allow action and click Apply actions. If this option is not available, log on as administrator or ask the security administrator for help.

**Items:**

file:H:\Documents and Settings\All Users\Application Data\iCEqKGW\mg.exe->(UPX)  
filelocalcopy:\\?\C:\ProgramData\Microsoft\Microsoft Antimalware\LocalCopy\{B150DD65-58BF-4941-84D3-ADD8F2E4BEE7}-iCEqKGW\mg.exe

[Get more information about this item online.](#)

Hide details <<

Apply actions

Close



## Your actions were applied successfully

Security Essentials successfully applied your actions and will continue monitoring your computer.

Detected items	Alert level	Status	Recommended act...
Trojan:Win32/FakeSysdef	Severe	Succeeded	Remove

**Category:** Trojan

**Description:** This program is dangerous and executes commands from an attacker.

**Recommended action:** Remove this software immediately.

Security Essentials detected programs that may compromise your privacy or damage your computer. You can still access the files that these programs use without removing them (not recommended). To access these files, select the Allow action and click Apply actions. If this option is not available, log on as administrator or ask the security administrator for help.

**Items:**

file:H:\Documents and Settings\All Users\Application Data\iCEqKGW\xmg.exe->(UPX)

filelocalcopy:\\?\C:\ProgramData\Microsoft\Microsoft Antimalware\LocalCopy\{B150DD65-588F-4941-84D3-ADD8F2E48EE7}-iCEqKGW\xmg.exe

[Get more information about this item online.](#)

Hide details <<

Apply actions

Close



## Potential threat details

Security Essentials detected 3 potential threats that might compromise your privacy or damage your computer. Your access to these items may be suspended until you take an action.

Click Show details to learn more. [What are alert levels?](#)

Detected items	Alert level	Status	Recommended act...
DDoS:Win32/Dofoil.A	Severe	Suspended	Remove ▼
Trojan:Win32/Danmec.L	Severe	Suspended	Remove
Trojan:Win32/FakeSysdef	Severe	Suspended	Remove

**Category:** Trojan Denial of Service

**Description:** This program can be used to perform a denial of service attack.

**Recommended action:** Remove this software immediately.

Security Essentials detected programs that may compromise your privacy or damage your computer. You can still access the files that these programs use without removing them (not recommended). To access these files, select the Allow action and click Apply actions. If this option is not available, log on as administrator or ask the security administrator for help.

**Items:**

file:H:\Documents and Settings\Owner\Local Settings\Temp\9E6.tmp->(UPX)

filelocalcopy:\\?\C:\ProgramData\Microsoft\Microsoft Antimalware\LocalCopy\{80E9E3F8-9BA6-4B2D-95C5-5DEF07A1129E}-9E6.tmp

[Get more information about this item online.](#)

Hide details <<

Apply actions

Close



## Potential threat details

Security Essentials detected 3 potential threats that might compromise your privacy or damage your computer. Your access to these items may be suspended until you take an action.

Click Show details to learn more. [What are alert levels?](#)

Detected items	Alert level	Status	Recommended act...
DDoS:Win32/Dofail.A	Severe	Suspended	Remove
Trojan:Win32/Danmec.L	Severe	Suspended	Remove
Trojan:Win32/FakeSysdef	Severe	Suspended	Remove

**Category:** Trojan

**Description:** This program is dangerous and executes commands from an attacker.

**Recommended action:** Remove this software immediately.

Security Essentials detected programs that may compromise your privacy or damage your computer. You can still access the files that these programs use without removing them (not recommended). To access these files, select the Allow action and click Apply actions. If this option is not available, log on as administrator or ask the security administrator for help.

**Items:**

file:H:\Documents and Settings\Owner\Local Settings\Temp\9E8.tmp->(UPX)

filelocalcopy:\\?\C:\ProgramData\Microsoft\Microsoft Antimalware\LocalCopy\{F7494470-92CE-45C1-B7EE-EFE17AF8ABE5}-9E8.tmp

[Get more information about this item online.](#)

Hide details <<

Apply actions

Close



## Potential threat details

Security Essentials detected 3 potential threats that might compromise your privacy or damage your computer. Your access to these items may be suspended until you take an action.

Click Show details to learn more. [What are alert levels?](#)

Detected items	Alert level	Status	Recommended act...
DDoS:Win32/Dofail.A	Severe	Suspended	Remove
Trojan:Win32/Danmec.L	Severe	Suspended	Remove
Trojan:Win32/FakeSysdef	Severe	Suspended	Remove <span style="float: right;">▼</span>

**Category:** Trojan

**Description:** This program is dangerous and executes commands from an attacker.

**Recommended action:** Remove this software immediately.

Security Essentials detected programs that may compromise your privacy or damage your computer. You can still access the files that these programs use without removing them (not recommended). To access these files, select the Allow action and click Apply actions. If this option is not available, log on as administrator or ask the security administrator for help.

**Items:**

file:H:\Documents and Settings\Owner\Local Settings\Temp\9E3.tmp

filelocalcopy:\\?\C:\ProgramData\Microsoft\Microsoft Antimalware\LocalCopy\{2E4A3652-E347-49E8-8997-5FB1787B6EC4}-9E3.tmp

[Get more information about this item online.](#)

Hide details <<

Apply actions

Close

\*



## Your actions were applied successfully

Security Essentials successfully applied your actions and will continue monitoring your computer.

Detected items	Alert level	Status	Recommended act...
DDoS:Win32/Dofail.A	Severe	Succeeded	Remove
Trojan:Win32/Danmec.L	Severe	Succeeded	Remove
Trojan:Win32/FakeSysdef	Severe	Succeeded	Remove

**Category:** Trojan

**Description:** This program is dangerous and executes commands from an attacker.

**Recommended action:** Remove this software immediately.

Security Essentials detected programs that may compromise your privacy or damage your computer. You can still access the files that these programs use without removing them (not recommended). To access these files, select the Allow action and click Apply actions. If this option is not available, log on as administrator or ask the security administrator for help.

**Items:**

file:H:\Documents and Settings\Owner\Local Settings\Temp\9E3.tmp

filelocalcopy:\\?\C:\ProgramData\Microsoft\Microsoft Antimalware\LocalCopy\{2E4A3652-E347-49E8-8997-5FB1787B6EC4}-9E3.tmp

[Get more information about this item online.](#)

Hide details <<

Apply actions

Close



Scanner | Protection | Update | Quarantine | Logs | Ignore List | Settings | More Tools | About



### Scanner

Malwarebytes' Anti-Malware is now scanning your system. Please wait until the scan is complete.

### Scanning filesystem objects for infection.

Objects scanned: 107996

**Objects infected: 1**

Scan type: Full scan (H:\)

Time elapsed: 46 minute(s), 32 second(s)

Currently scanning:

H:\System Volume Information\\_restore{CEF1DB5E-40BA-413A-8702-C1F38F44769E}\RP274\A0096245.EXE


Pause Scan

Abort Scan

Exit

\*

Malwarebytes' Anti-Malware (PRO)



Scanner Protection Update Quarantine Logs Ignore List Settings More Tools About


**Scanner**  
Below is a list of malicious software found on your system. Close all unnecessary applications to ensure successful threat removal.

Vendor	Category	Item	Other	Action taken
<input checked="" type="checkbox"/> Trojan.P2P.Worm	File	h:\system volume information\_restore{cef1db5...		No action taken.

Remove Selected Ignore Save Log Main Menu Exit

\*

Malwarebytes' Anti-Malware



All selected items have been removed successfully. A log file has been saved to the logs folder.

Your computer needs to be restarted to complete the removal process. Would you like to restart now?

Yes No

\*



## Potential threat details

Security Essentials detected 1 potential threat that might compromise your privacy or damage your computer. Your access to these items may be suspended until you take an action.

Click Show details to learn more. [What are alert levels?](#)

Detected items	Alert level	Status	Recommended act...
Trojan:Win32/Orsam!rts	High	Suspended	Quarantine <span style="float: right;">▼</span>

**Category:** Trojan

**Description:** This program is dangerous and executes commands from an attacker.

**Recommended action:** Permit this detected item only if you trust the program or the software publisher.

Security Essentials detected programs that may compromise your privacy or damage your computer. You can still access the files that these programs use without removing them (not recommended). To access these files, select the Allow action and click Apply actions. If this option is not available, log on as administrator or ask the security administrator for help.

**Items:**

file:H:\System Volume Information\\_restore{CEF1DB5E-40BA-413A-8702-C1F38F44769E}\RP274  
\A0098553.exe

filelocalcopy:\\?\C:\ProgramData\Microsoft\Microsoft Antimalware\LocalCopy\{6CC6557F-9A23-425F-A95F-539F6576E7C7}-A0098553.exe

[Get more information about this item online.](#)

Hide details <<

Apply actions

Close

\*



## Your actions were applied successfully

Security Essentials successfully applied your actions and will continue monitoring your computer.

Detected items	Alert level	Status	Recommended act...
Trojan:Win32/Orsam!rts	High	Succeeded	Quarantine

**Category:** Trojan

**Description:** This program is dangerous and executes commands from an attacker.

**Recommended action:** Permit this detected item only if you trust the program or the software publisher.

Security Essentials detected programs that may compromise your privacy or damage your computer. You can still access the files that these programs use without removing them (not recommended). To access these files, select the Allow action and click Apply actions. If this option is not available, log on as administrator or ask the security administrator for help.

**Items:**

file:H:\System Volume Information\\_restore{CEF1DB5E-40BA-413A-8702-C1F38F44769E}\RP274  
\A0098553.exe

filelocalcopy:\\?\C:\ProgramData\Microsoft\Microsoft Antimalware\LocalCopy\{6CC6557F-9A23-425F-A95F-539F6576E7C7}-A0098553.exe


[Get more information about this item online.](#)

Hide details <<

Apply actions

Close

Malwarebytes' Anti-Malware (PRO)



**Malwarebytes' Anti-Malware**

Scanner | Protection | Update | Quarantine | Logs | Ignore List | Settings | More Tools | About


**Scanner**  
Below is a list of malicious software found on your system. Close all unnecessary applications to ensure successful threat removal.

Vendor	Category	Item	Other	Action taken
<input checked="" type="checkbox"/> Trojan.P2P.Worm	File	h:\system volume information\ restore{cef1 db5...		No action taken.
<input checked="" type="checkbox"/> PUP.PSWTool.Pr...	File	h:\system volume information\_restore{cef1 db5...		No action taken.

Remove Selected | Ignore | Save Log | Main Menu | Exit

\*

Malwarebytes' Anti-Malware



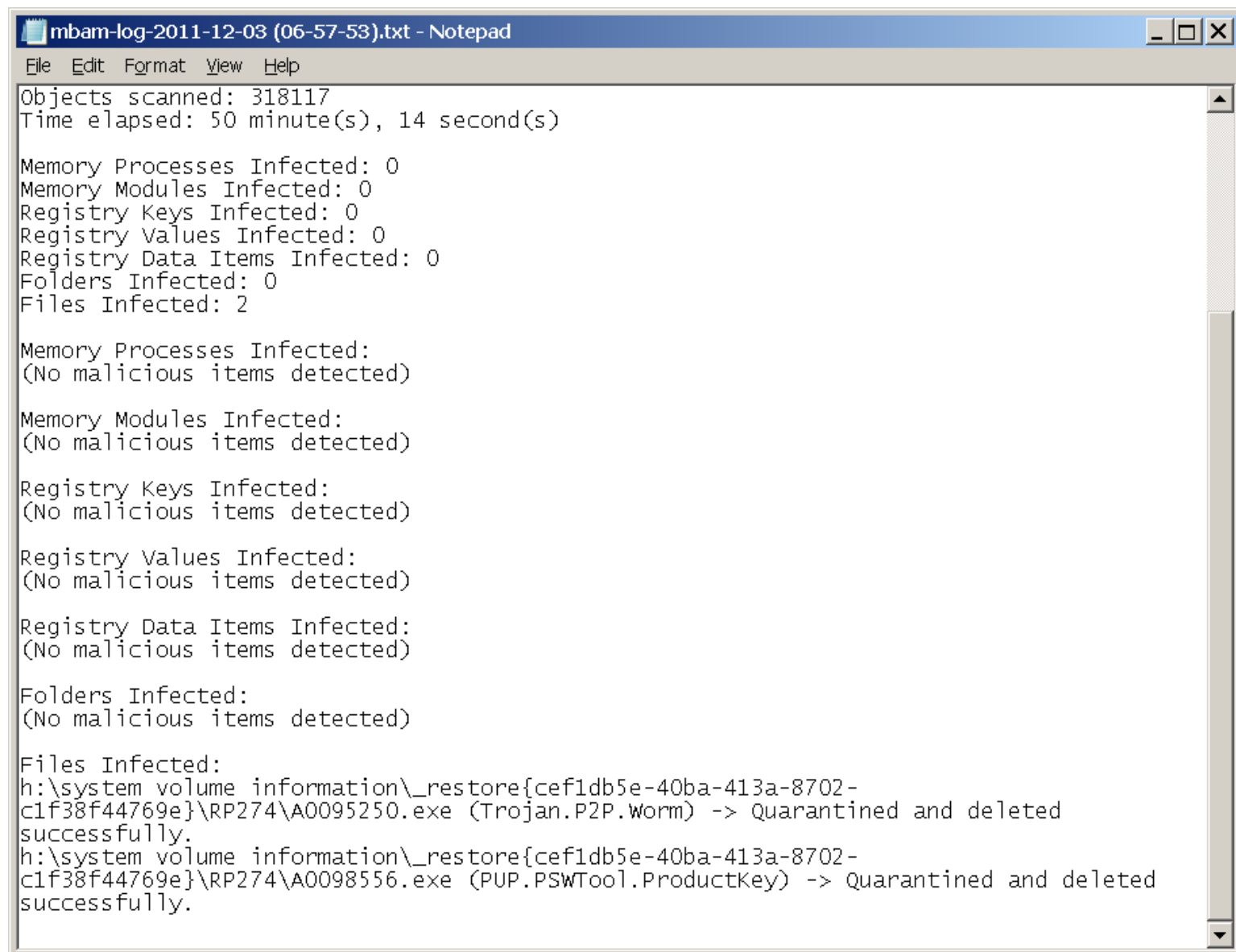
All selected items have been removed successfully. A log file has been saved to the logs folder.

Your computer needs to be restarted to complete the removal process. Would you like to restart now?

Yes | No

\*

"SuperAntiSpyware" found and removed 17 items of malware that "Microsoft Security Essentials" and "MalwareBytes" were unable to detect.



```
mbam-log-2011-12-03 (06-57-53).txt - Notepad
File Edit Format View Help
Objects scanned: 318117
Time elapsed: 50 minute(s), 14 second(s)

Memory Processes Infected: 0
Memory Modules Infected: 0
Registry Keys Infected: 0
Registry Values Infected: 0
Registry Data Items Infected: 0
Folders Infected: 0
Files Infected: 2

Memory Processes Infected:
(No malicious items detected)

Memory Modules Infected:
(No malicious items detected)

Registry Keys Infected:
(No malicious items detected)

Registry Values Infected:
(No malicious items detected)

Registry Data Items Infected:
(No malicious items detected)

Folders Infected:
(No malicious items detected)

Files Infected:
h:\system volume information\_restore{cef1db5e-40ba-413a-8702-
c1f38f44769e}\RP274\A0095250.exe (Trojan.P2P.Worm) -> Quarantined and deleted
successfully.
h:\system volume information\_restore{cef1db5e-40ba-413a-8702-
c1f38f44769e}\RP274\A0098556.exe (PUP.PSWTool.ProductKey) -> Quarantined and deleted
successfully.
```

"ComboFix" removed "W32.IRCBot" which "Microsoft Security Essentials", "MalwareBytes", and "SuperAntiSpyware" were all unable to detect.

#####

An excerpt from the ComboFix.txt report:

ComboFix 11-12-03.01 - Owner 12/03/2011 11:18:09.1.1 - x86  
Microsoft Windows XP Home Edition  
5.1.2600.3.1252.1.1033.18.1270.771 [GMT -7:00]  
Running from: D:\ComboFix.exe  
AV: Microsoft Security Essentials \*Disabled/Updated\*  
{BCF43643-A118-4432-AEDE-D861FCBCFCDF}  
AV: Microsoft Security Essentials \*Enabled/Updated\*  
{EDB4FA23-53B8-4AFA-8C5D-99752CCA7095}

(((((((((((((((((((((((((((((((((((((((((((((((((((((((( Other Deletions  
))))))))))))))))))))))))))))))))))))))))))))))))))))))

C:\Documents and Settings\All Users\Application Data\TEMP  
C:\Documents and Settings\All Users\Start  
Menu\Programs\Smart Flash Recovery  
C:\Documents and Settings\All Users\Start  
Menu\Programs\Smart Flash Recovery\Check other products\1-  
2-3 Spyware Free.Ink  
C:\Documents and Settings\All Users\Start  
Menu\Programs\Smart Flash Recovery\Check other  
products\Customize Start Menu.Ink

C:\Documents and Settings\All Users\Start  
Menu\Programs\Smart Flash Recovery\Check other  
products\Document Trace Remover.Ink

C:\Documents and Settings\All Users\Start  
Menu\Programs\Smart Flash Recovery\Check other products\My  
Privacy.Ink

C:\Documents and Settings\All Users\Start  
Menu\Programs\Smart Flash Recovery\Check other  
products\Safe Surfer.Ink

C:\Documents and Settings\All Users\Start  
Menu\Programs\Smart Flash Recovery\Check other  
products\Smart PC.Ink

C:\Documents and Settings\All Users\Start  
Menu\Programs\Smart Flash Recovery\Smart Flash Recovery  
Help.Ink

C:\Documents and Settings\All Users\Start  
Menu\Programs\Smart Flash Recovery\Smart Flash Recovery  
HomePage.Ink

C:\Documents and Settings\All Users\Start  
Menu\Programs\Smart Flash Recovery\Smart Flash Recovery  
ReadMe.Ink

C:\Documents and Settings\All Users\Start  
Menu\Programs\Smart Flash Recovery\Smart Flash  
Recovery.Ink

C:\Documents and Settings\All Users\Start  
Menu\Programs\Smart Flash Recovery\Uninstall Smart Flash  
Recovery.Ink

C:\Documents and Settings\Owner\WINDOWS

C:\Program Files\Smart Flash Recovery

C:\Program Files\Smart Flash Recovery\1-2-3 Spyware Free.url

C:\Program Files\Smart Flash Recovery\Customize Start  
Menu.url

C:\Program Files\Smart Flash Recovery\Document Trace Remover.url  
C:\Program Files\Smart Flash Recovery\history.txt  
C:\Program Files\Smart Flash Recovery\homepage.url  
C:\Program Files\Smart Flash Recovery\license.txt  
C:\Program Files\Smart Flash Recovery\My Privacy.url  
C:\Program Files\Smart Flash Recovery\readme.txt  
C:\Program Files\Smart Flash Recovery\Safe Surfer.url  
C:\Program Files\Smart Flash Recovery\Smart PC.url  
C:\Program Files\Smart Flash Recovery\SmartFlashRecovery.cnt  
C:\Program Files\Smart Flash Recovery\SmartFlashRecovery.exe  
C:\Program Files\Smart Flash Recovery\SmartFlashRecovery.hlp  
C:\Program Files\Smart Flash Recovery\SmartPC.ico  
C:\Program Files\Smart Flash Recovery\unins000.dat  
C:\Program Files\Smart Flash Recovery\unins000.exe  
C:\Thumbs.db  
C:\WINDOWS\system32\MrvGINA.dll  
C:\WINDOWS\system32\rnaph.dll  
C:\WINDOWS\system32\usmt\migwiz\_a.exe

#####

"W32.IRCBot" is described at

<http://www.threatexpert.com/report.aspx?md5=b086087633ad99bb1fbbf8f856d679fe>