

PCSL 全方位安全軟體測試

2009 年第 3 期

測試總結報告

2009 年 3 月 30 日星期一

作者：Jeffrey Wu

網址：http://www.pcsecuritylabs.net

合作媒體：電腦之家（首發）：　http://antivirus.pchome.net/

中關村線上：　http://xiazai.zol.com.cn/

太平洋電腦網：　http://pcedu.pconline.com.cn/

測試產品（按照英文名稱首字母 A-Z 排序）

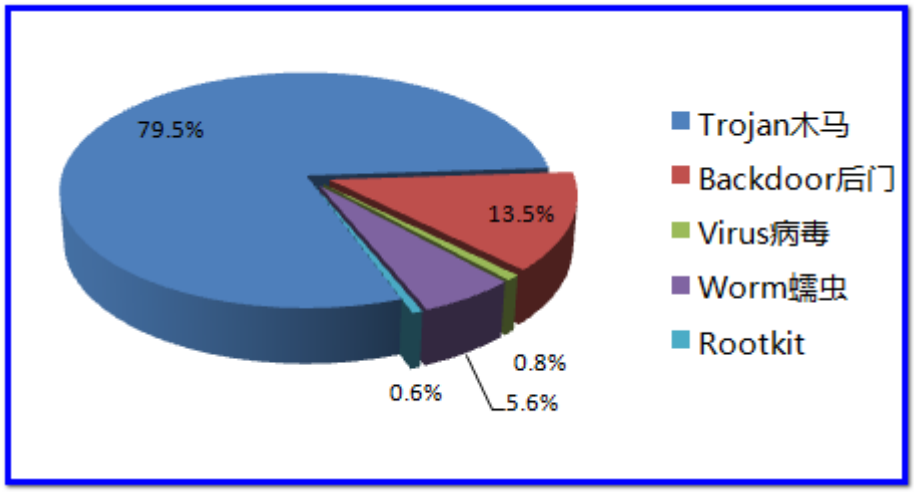
- a-squared Anti-Malware 4.0
  Emsi Software GmbH（奧地利）
- Avira Premium Security Suite 8
  Avira GmbH（德國）
- Dr.Web® Security Space
  Doctor Web, Ltd. (俄羅斯)
- F-Secure Internet Security 2009
  F-Secure Corporation（芬蘭）
- G DATA InternetSecurity 2009
  G DATA Software AG.（德國）
- IKARUS virus utilities T3
  IKARUS Security Software GmbH（奧地利）
- 江民殺毒軟體 KV2009
  江民新科技術有限公司（中國）
- 卡巴斯基網路安全套裝 2009
  Kaspersky Lab（俄羅斯）
- 金山毒霸 2009 殺毒軟體套裝
  金山軟體有限公司（中國）
- 熊貓衛士網際網路安全 2009
  Panda Security（西班牙）
- Quick Heal Total Security 2009
  Quick Heal Technologies (P) Ltd.（印度）
- 趨勢科技網路安全專家 2009
  趨勢科技（中國）有限公司
- TrustPort PC Security 2009
  TrustPort, a.s.(捷克)
- 費爾托斯特安全
  費爾安全實驗室（中國）

實驗室動態及最新看點

- 來自德國的 GDATA 宣佈加入 PCSL 全方位安全軟體測試並首次參加公開測試
- 授權 PC 安全實驗室對其安全軟體進行公開測試的廠商達到 15 家，並有 3 家廠商正在進行內測
- PC 安全實驗室成功邀請到太平洋電腦網作為實驗室繼電腦之家（PChome）和中關村線上（ZOL）之後的第三家合作報導媒體

測試方法及評分細則

- 本期測試基於 2008 年 12 月版的 PC 安全實驗室手冊，升級時間統一為 2009 年 3 月 12 日 21：00 GMT+8，所有掃描和測試都在擁有網路連接的情況下進行。
- 本期測試使用 2009 年 01 月的 Malware-List 流行樣本包，一共包含 2059 個樣本



- 評分公式=（A+B）/C*100-lg(D+1)

  A=靜態測試偵測數

  B=動態測試偵測數

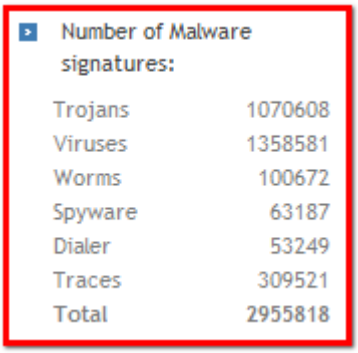
  C=惡意樣本總數

  D=誤報樣本數
- 最終得分在 95.00-100.00 將得到 5 星優秀月度認證
- 最終得分在 90.00-94.99 將得到 4 星標準月度認證

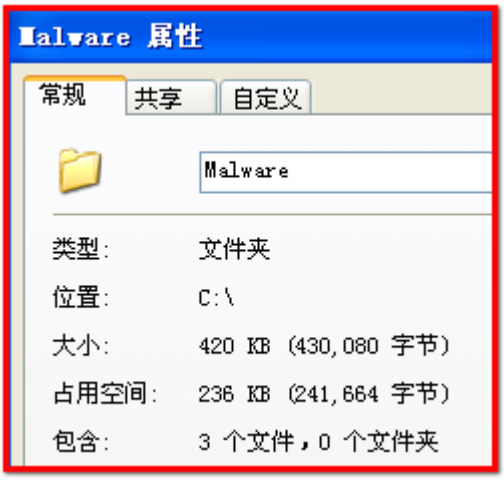
各產品詳細測試結果

※ a-squared Anti-Malware 4.0 以下簡稱 a2 ※

- 廠商：Emsi Software GmbH（奧地利）
- 產品詳細資訊：



- 靜態測試：選擇刪除所有偵測到的樣本，去除重複後 **a2** 共偵測樣本數=2059-3=2056



- 動態測試：運行剩餘樣本，**a2** 共偵測樣本數為 0

◆ 誤報測試：**a2** 共有 10 個誤報

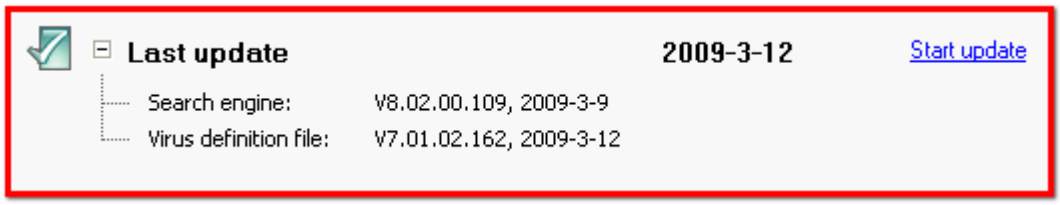
09344655 Virus.Win32.Trojan
0f708ae7 Backdoor.Win32.GrayBird.EJ
337965a9 Trojan-Downloader.Win32.Dadobra
4f893c42 Virus.Win32.Trojan
5480ba8c Trojan.Win32.Agent
6d0717d5 Virus.Win32.Trojan
a3c31a97 Virus.Win32.Crypt.COK
b049ff9e Trojan-Downloader.Win32.VB.abu
f3441c43 Virus.Win32.Agent.RZV
f97a9997 Trojan-Spy.Win32.Qeds.A

◆ 結果統計

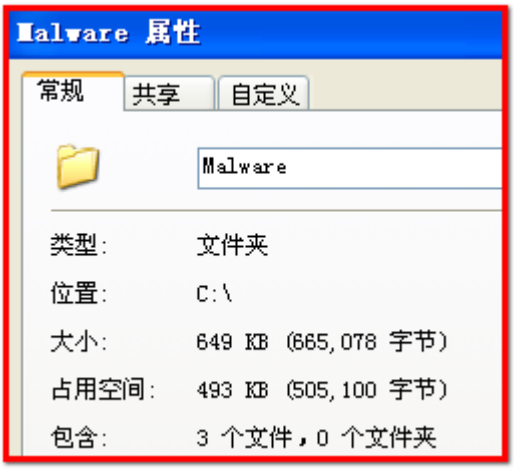
a-squared Anti-Malware 4.0 在本次測試中
靜態測試中偵測樣本數 A=2056
動態測試中偵測樣本數 B=0
樣本包樣本總數 C=2059
誤報測試中誤報樣本數 D=10
則最後總分=（A+B）/C*100-lg(D+1)=（2056+0）/2059*100-lg(10+1)=98.81

※ Avira Premium Security Suite 8 以下簡稱 Avira ※

- 廠商：Avira GmbH（德國）
- 產品詳細資訊：



- 靜態測試：選擇刪除所有偵測到的樣本，去除重複後 **Avira** 共偵測樣本數=2059-3=2056



◆ 動態測試：運行剩餘樣本，**Avira** 共偵測樣本數為 0

◆ 誤報測試：**Avira** 共有 3 個誤報

09344655 ADSPY/Agent.50688 adware or spyware

79ad6d4b TR/Starter.263 Trojan

b049ff9e TR/Agent.33792.H Trojan

◆ **結果統計**

Avira Premium Security Suite 8 在本次測試中

靜態測試中偵測樣本數 A=2056

動態測試中偵測樣本數 B=0

樣本包樣本總數 C=2059

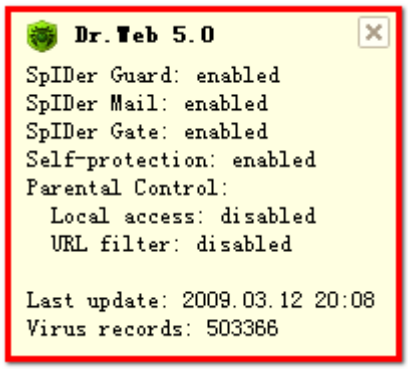
誤報測試中誤報樣本數 D=3

則最後總分=（A+B）/C*100-lg(D+1)=（2056+0）/2059*100-lg(3+1)=99.25

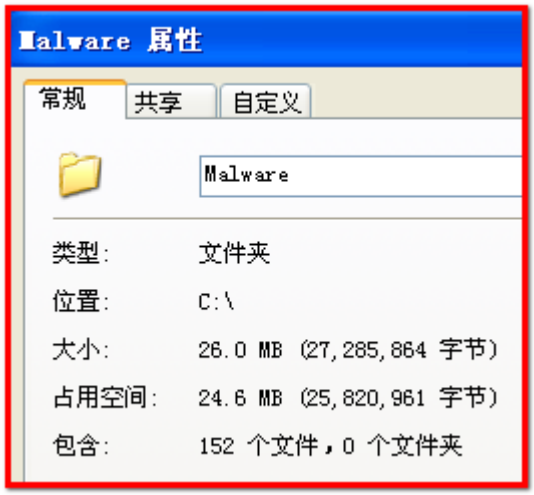
※ Dr.Web® Security Space 以下簡稱 Dr.Web ※

- 廠商：Doctor Web, Ltd. (俄羅斯)

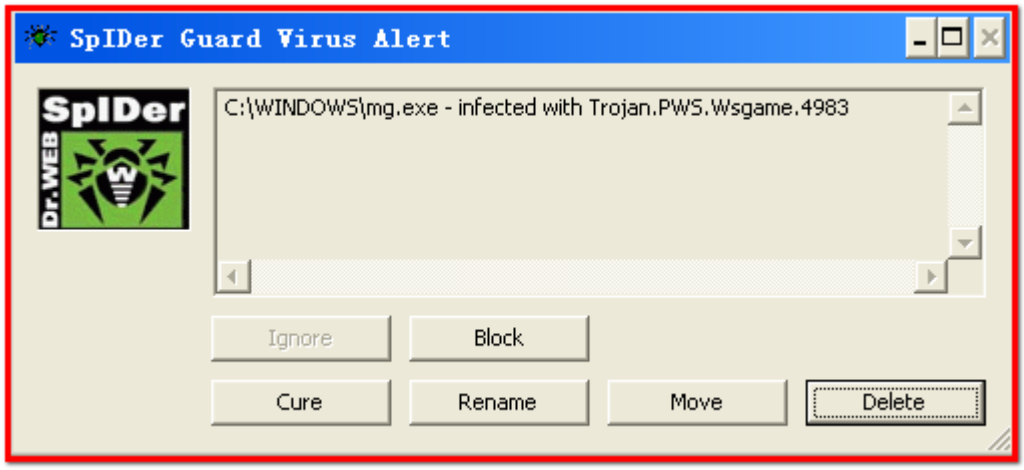
- 產品詳細資訊：



- 靜態測試：選擇刪除所有偵測到的樣本，去除重複後 **Dr.Web** 共偵測樣本數 =2059-152=1907



◆ 動態測試：運行剩餘樣本，**Dr.Web** 共偵測樣本數為 49



◆ 誤報測試：**Dr.Web** 共有 2 個誤報

5480ba8c　Win32.HLLW.Gavir.75

79ad6d4b　Archive contains infected objects

◆ **結果統計**

Dr.Web® Security Space 在本次測試中

靜態測試中偵測樣本數　A=1907

動態測試中偵測樣本數　B=49

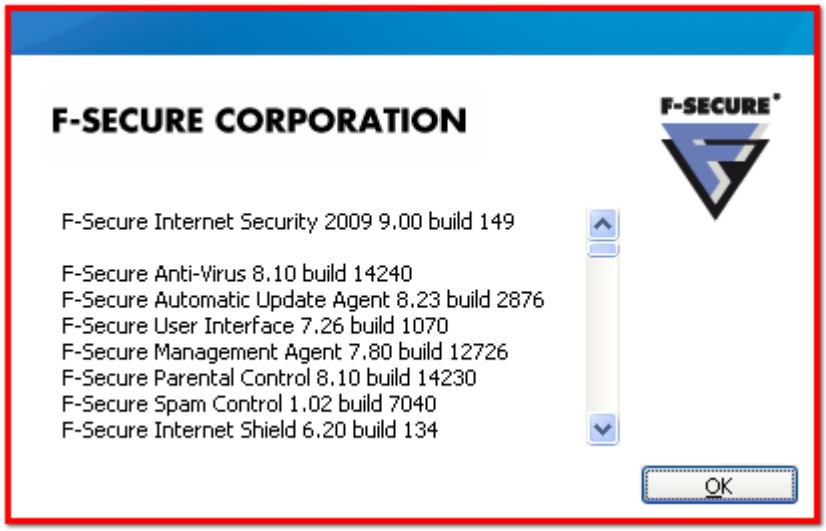
樣本包樣本總數　　C=2059

誤報測試中誤報樣本數　D=2

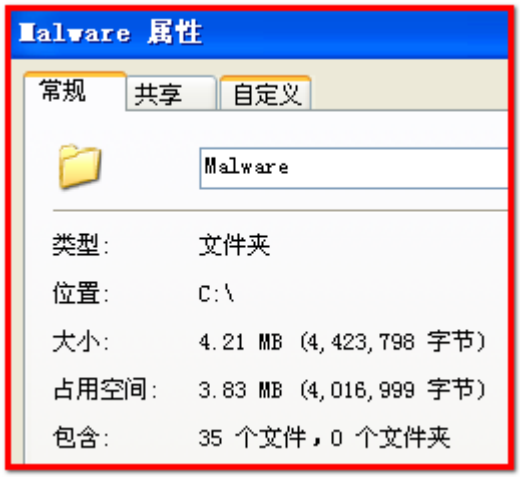
則最後總分=（A+B）/C*100-lg(D+1)=（1907+49）/2059*100-lg(2+1)=94.52

※ F-Secure Internet Security 2009 以下簡稱 F-Secure ※

- 廠商：F-Secure Corporation（芬蘭）
- 產品詳細資訊：



- 靜態測試：選擇刪除所有偵測到的樣本，去除重複後 **F-Secure** 共偵測樣本數 =2059-35=2024



◆ 動態測試：運行剩餘樣本，**F-Secure** 共偵測樣本數為 25

◆ 誤報測試：**F-Secure** 共有 1 個誤報

0f708ae7　　Trojan.Win32.Genome.ceb

◆ **結果統計**

F-Secure Internet Security 2009 在本次測試中

靜態測試中偵測樣本數　A=2024

動態測試中偵測樣本數　B=25

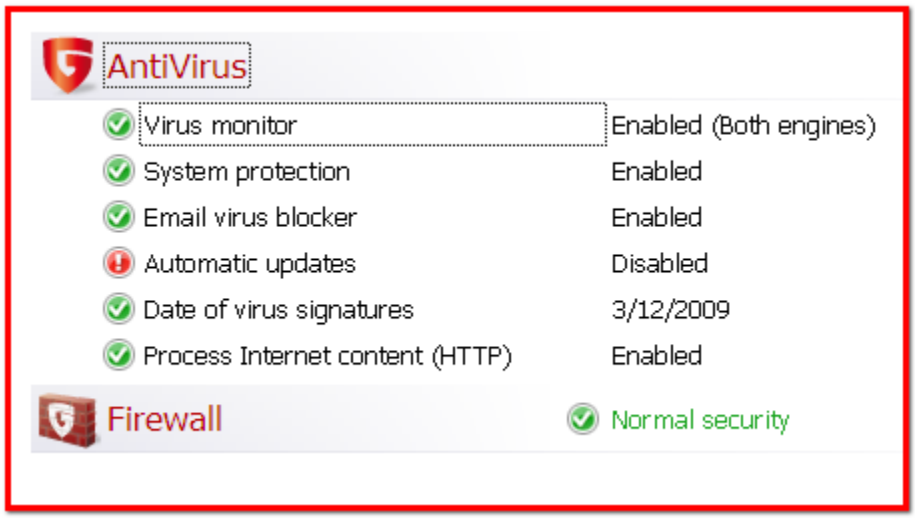
樣本包樣本總數　　C=2059

誤報測試中誤報樣本數　D=1

則最後總分=（A+B）/C*100-lg(D+1)=（2024+25）/2059*100-lg(1+1)=99.21

※ G DATA InternetSecurity 2009 以下簡稱 G DATA ※

- 廠商：G DATA Software AG.（德國）
- 產品詳細資訊：



- 靜態測試:選擇刪除所有偵測到的樣本,去除重複後 **G DATA** 共偵測樣本數=2059-2=2057

◆ 動態測試：運行剩餘樣本，**G DATA** 共偵測樣本數為 2

◆ 誤報測試：**G DATA** 共有 5 個誤報

Trojan.Generic.536485 (Engine A)	09344655
Trojan.Generic.179994 (Engine A)	0f708ae7
Win32:Trojan-gen {Other} (Engine B)	4f893c42
Win32.Worm.Viking.LQ (Engine A)	5480ba8c
Backdoor.Hupigon.130581 (Engine A)	61f0d510

◆ **結果統計**

G DATA InternetSecurity 2009 在本次測試中

靜態測試中偵測樣本數 A=2057

動態測試中偵測樣本數 B=2

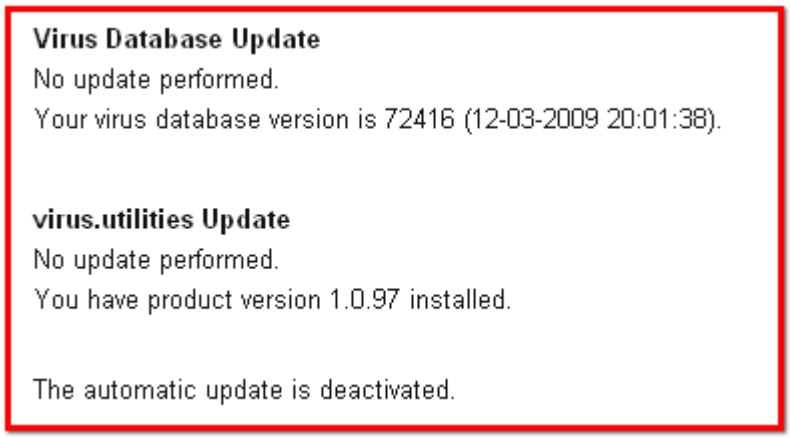
樣本包樣本總數 C=2059

誤報測試中誤報樣本數 D=5

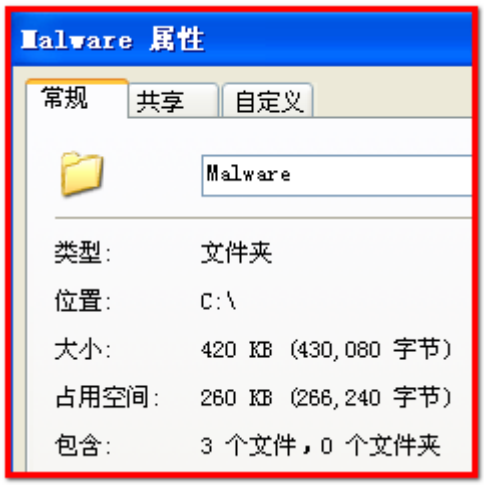
則最後總分=（A+B）/C*100-lg(D+1)=（2057+2）/2059*100-lg(5+1)=99.22

※ IKARUS virus utilities T3 以下簡稱 IKARUS ※

- 廠商：IKARUS Security Software GmbH（奧地利）
- 產品詳細資訊：



- 靜態測試:選擇刪除所有偵測到的樣本,去除重複後**IKARUS**共偵測樣本數=2059-3=2056



- 動態測試：運行剩餘樣本，**IKARUS** 共偵測樣本數為 0

◆ 誤報測試：**IKARUS** 共有 10 個誤報

09344655 Virus.Win32.Trojan
0f708ae7 Backdoor.Win32.GrayBird.EJ
337965a9 Trojan-Downloader.Win32.Dadobra
4f893c42 Virus.Win32.Trojan
5480ba8c Trojan.Win32.Agent
6d0717d5 Virus.Win32.Trojan
a3c31a97 Virus.Win32.Crypt.COK
b049ff9e Trojan-Downloader.Win32.VB.abu
f3441c43 Virus.Win32.Agent.RZV
f97a9997 Trojan-Spy.Win32.Qeds.A

◆ **結果統計**

IKARUS virus utilities T3 在本次測試中

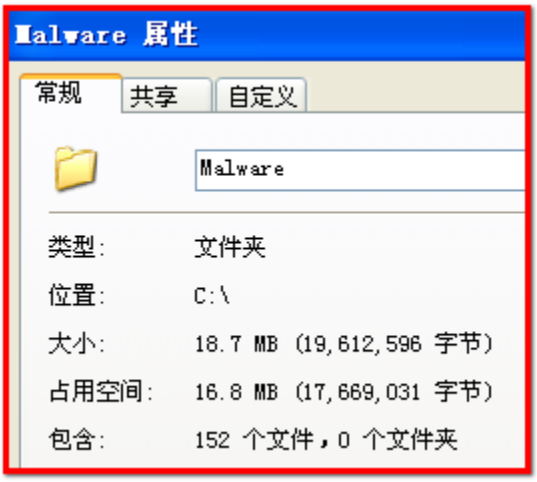
靜態測試中偵測樣本數 A=2056
動態測試中偵測樣本數 B=0
樣本包樣本總數 C=2059
誤報測試中誤報樣本數 D=10
則最後總分=（A+B）/C*100-lg(D+1)=（2056+0）/2059*100-lg(10+1)=98.81

※ 江民殺毒軟體 KV2009 以下簡稱 Jiangmin ※

- 廠商：江民新科技術有限公司

- 產品詳細資訊：

- 靜態測試：選擇刪除所有偵測到的樣本，去除重複後 **Jiangmin** 共偵測樣本數 =2059-152=1907



◆ 動態測試：運行剩餘樣本，**Jiangmin** 共偵測樣本數為 133

◆ 誤報測試：**Jiangmin** 共有 2 個誤報

E:\Clean\0f708ae7	Backdoor/Hupigon.be
E:\Clean\f97a9997	Trojan/PSW.GamePass...

◆ **結果統計**

江民殺毒軟體網路版 KV2009 在本次測試中

靜態測試中偵測樣本數 A=1907

動態測試中偵測樣本數 B=133

樣本包樣本總數 C=2059

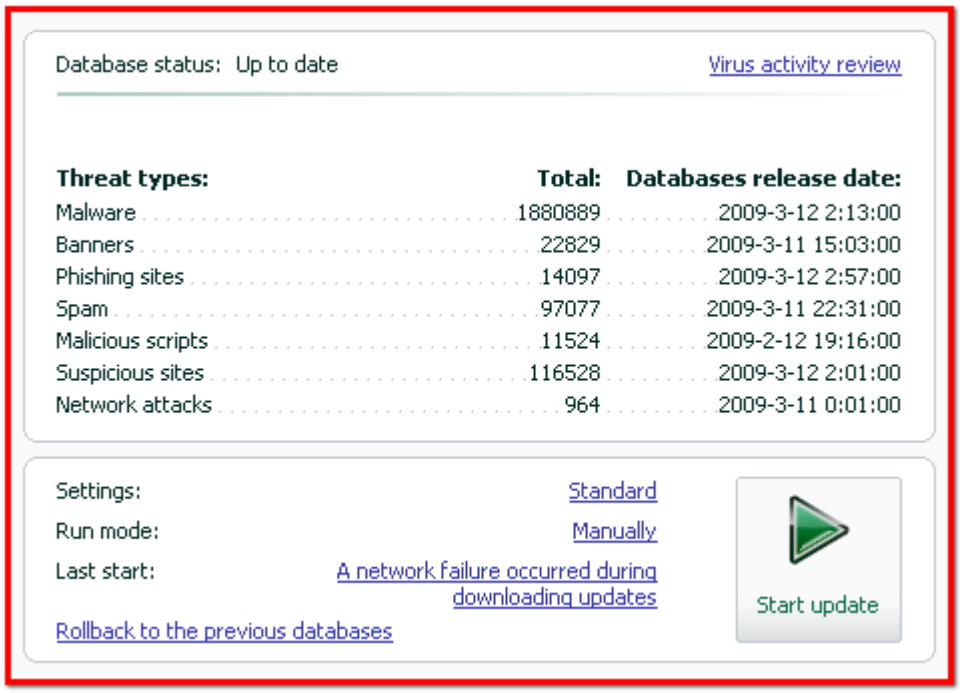
誤報測試中誤報樣本數 D=2

則最後總分=（A+B）/C*100-lg(D+1)=（1907+133）/2059*100-lg(2+1)=98.60

※ 卡巴斯基網路安全套裝 2009 以下簡稱 卡巴斯基 ※

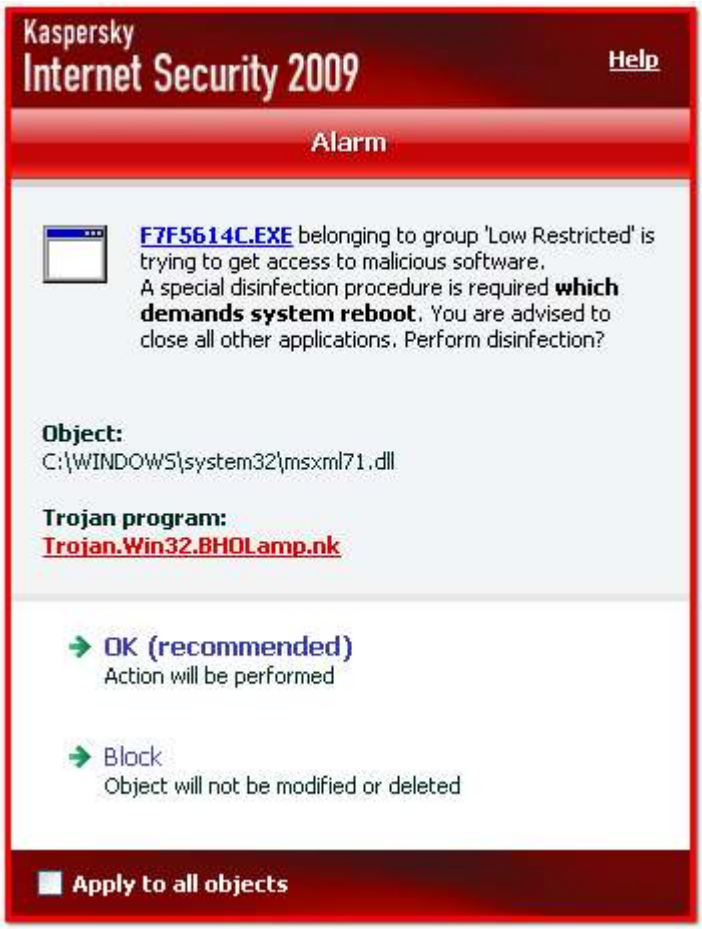
- 廠商：Kaspersky Lab

- 產品詳細資訊：



- 靜態測試：選擇刪除所有偵測到的樣本，去除重複後**卡巴斯基**共偵測樣本數 =2059-28=2031

◆ 動態測試：運行剩餘樣本，**卡巴斯基**共偵測樣本數為 24



◆ 誤報測試：**卡巴斯基**共有 1 個誤報

0f708ae7　　Trojan.Win32.Genome.ceb

◆ **結果統計**

卡巴斯基全功能安全軟體 2009 在本次測試中

靜態測試中偵測樣本數　A=2031

動態測試中偵測樣本數　B=24

樣本包樣本總數　　C=2059

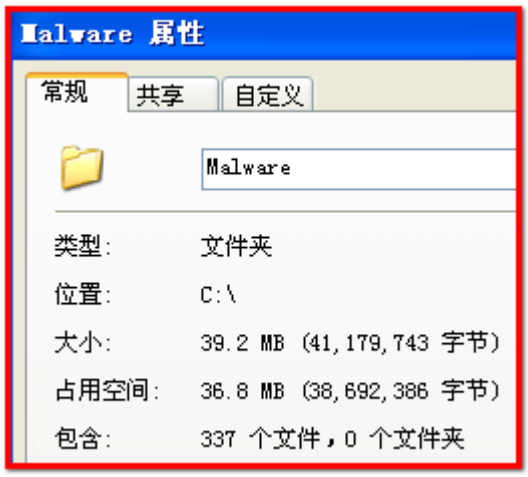
誤報測試中誤報樣本數　D=1

則最後總分=（A+B）/C*100-lg(D+1)=（2031+24）/2059*100-lg(1+1)=99.50

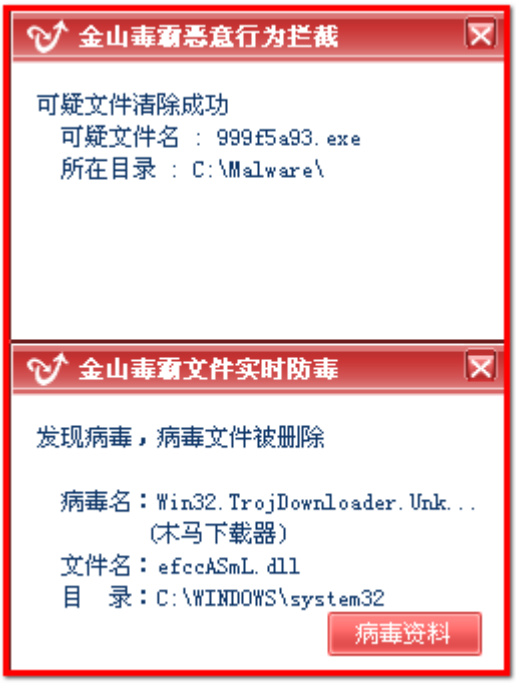
※ 金山毒霸 2009 殺毒軟體套裝 以下簡稱 金山 ※

- 廠商：金山軟體有限公司
- 產品詳細資訊：

- 靜態測試：選擇刪除所有偵測到的樣本，去除重複後**金山**共偵測樣本數=2059-337=1722



◆ 動態測試：運行剩餘樣本，**金山**共偵測樣本數為 165



◆ 誤報測試：**金山**共有 0 個誤報

◆ **結果統計**

金山毒霸 2009 殺毒軟體套裝 在本次測試中

靜態測試中偵測樣本數 A=1722

動態測試中偵測樣本數 B=165

樣本包樣本總數 C=2059

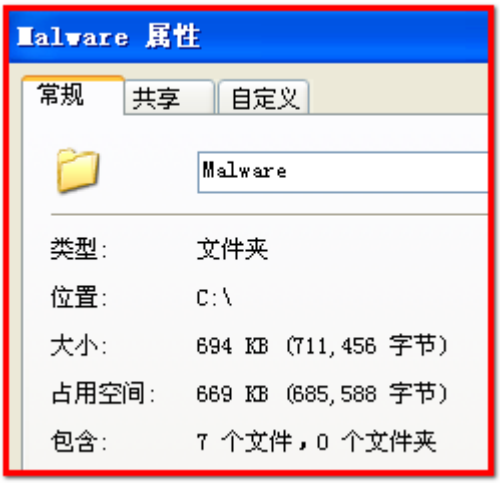
誤報測試中誤報樣本數 D=0

則最後總分=（A+B）/C*100-lg(D+1)=（1722+165）/2059*100-lg(0+1)=91.65

※ 熊貓衛士網際網路安全 2009 以下簡稱 熊貓 ※

- 廠商：Panda Security（西班牙）
- 產品資訊：

- 靜態測試：選擇刪除所有偵測到的樣本，去除重複後**熊貓**共偵測樣本數=2059-7=2052



- 動態測試：運行剩餘樣本，**熊貓**共偵測樣本數為 1

◆ 誤報測試：**熊貓**共有 1 個誤報

◆ **結果統計**

熊貓衛士網際網路安全 2009 在本次測試中

靜態測試中偵測樣本數 A=2052

動態測試中偵測樣本數 B=1

樣本包樣本總數 C=2059

誤報測試中誤報樣本數 D=1

則最後總分=（A+B）/C*100-lg(D+1)=（2052+1）/2059*100-lg(1+1)=99.41

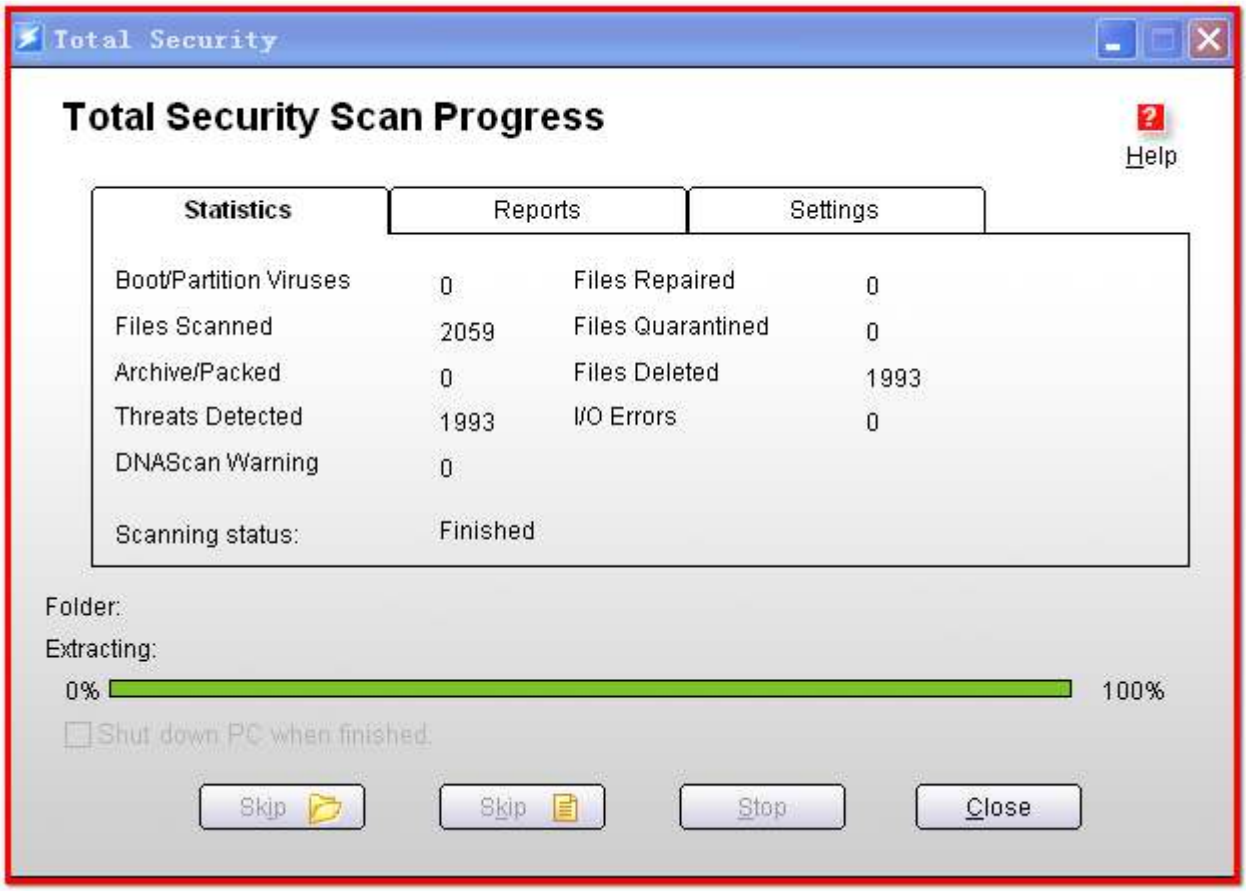
※ Quick Heal Total Security 2009 以下簡稱 Quick Heal ※

Quick Heal®

- 廠商：Quick Heal Technologies (P) Ltd.

- 產品資訊：

- 靜態測試：選擇刪除所有偵測到的樣本，去除重複後 **Quick Heal** 共偵測樣本數 =2059-66=1993



◆ 動態測試：運行剩餘樣本，**Quick Heal** 共偵測樣本數為 36

◆ 誤報測試：**Quick Heal** 共有 4 個誤報

of708ae7 Win32.Virtool.DelfInject.Gen!X.5
5480ba8c Trojan.Agent.IRC
a3c31a97 Trojan.Agent.IRC
f3441c43 Trojan.Agent.ATV

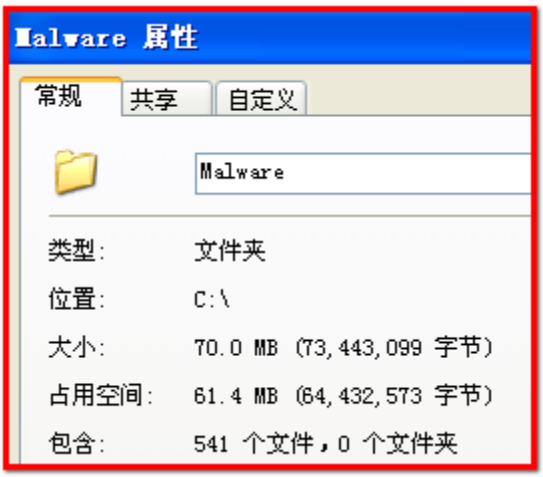
◆ **結果統計**

Quick Heal Total Security 2009 在本次測試中
靜態測試中偵測樣本數 A=1993
動態測試中偵測樣本數 B=36
樣本包樣本總數 C=2059
誤報測試中誤報樣本數 D=4
則最後總分=（A+B）/C*100-lg(D+1)=（1993+36）/2059*100-lg(4+1)=97.84

※ 趨勢科技網路安全專家 2009 以下簡稱 趨勢 ※

- 廠商：趨勢科技（中國）有限公司
- 產品資訊：

- 靜態測試：選擇刪除所有偵測到的樣本，去除重複後**趨勢**共偵測樣本數=2059-541=1518



◆ 動態測試：運行剩餘樣本，**趨勢**共偵測樣本數為 345

◆ 誤報測試：**趨勢**共有 2 個誤報

09344655 TROJ_GENERIC.APC

283a763c PACKER-GEN.101

◆ **結果統計**

趨勢科技網路安全專家 2008 在本次測試中

靜態測試中偵測樣本數 A=1518

動態測試中偵測樣本數 B=345

樣本包樣本總數 C=2059

誤報測試中誤報樣本數 D=2

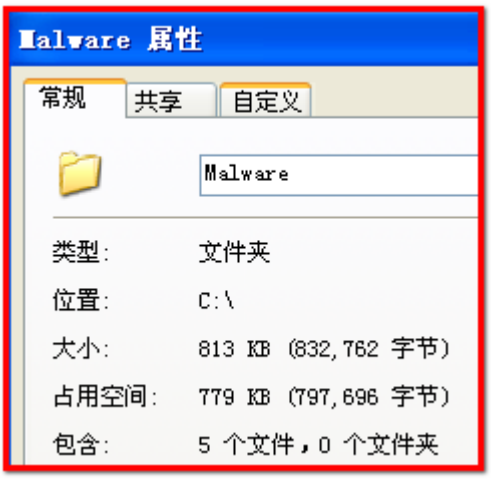
則最後總分=（A+B）/C*100-lg(D+1)=（1518+345）/2059*100-lg(2+1)=90.00

※ TrustPort PC Security 2009 以下簡稱 TrustPort ※

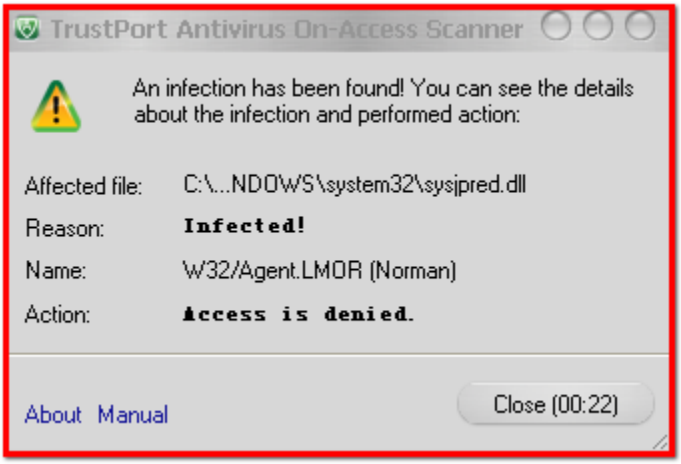
- 廠商：TrustPort, a.s.

- 產品資訊：

- 靜態測試：選擇刪除所有偵測到的樣本，去除重複後 **TrustPort** 共偵測樣本數 =2059-5=2054



- 動態測試：運行剩餘樣本，**TrustPort** 共偵測樣本數為 1



◆ 誤報測試：**TrustPort** 共有 9 個誤報

09344655 Clicker.DQK(Avg)
0f708ae7 W32/Packed_NsPack.I(Norman)
3be77210 VB.FEK(Avg)
4f893c42 SHeur.BAAI(Avg)
5480ba8c Worm/Delf.CKI(Avg)
9bd01461 W32/Malware.FBEF(Norman)
f2f988e1 BScope.Trojan-PSW.OnlineGames(VirusBlokAda)
f3441c43 W32/GrayBird.VAL(Norman)
f97a9997 Worm.Win32.Otwycal.g(VirusBlokAda)

◆ **結果統計**

TrustPort PC Security 2009 在本次測試中

靜態測試中偵測樣本數 A=2054
動態測試中偵測樣本數 B=1
樣本包樣本總數 C=2059
誤報測試中誤報樣本數 D=9
則最後總分=（A+B）/C*100-lg(D+1)=（2054+1）/2059*100-lg(9+1)=98.81

※ 費爾托斯特安全 以下簡稱 費爾 ※

- 廠商：費爾安全實驗室

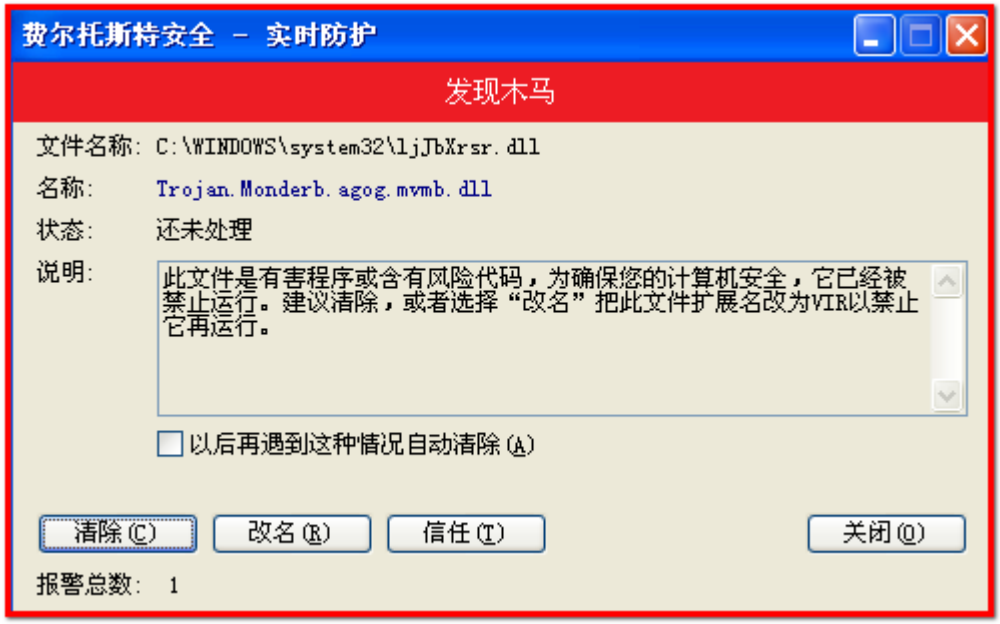
- 產品資訊：

2009/03/12 19:57 (9). 费尔托斯特安全病毒库升级到 **v9.120.47215 (2009.03.12.19:57)**，新增72个新木马和病毒。本日第9次更新，日累计新增600。病毒库总数：1258517。

默認設置並不開啟殼偵測

- 靜態測試：選擇刪除所有偵測到的樣本，去除重複後**費爾**共偵測樣本數=2059-398=1661

- 動態測試：運行剩餘樣本，**費爾**共偵測樣本數為 373



- 誤報測試：**費爾**共有 0 個誤報
- **結果統計**

費爾托斯特安全在本次測試中

靜態測試中偵測樣本數 A=1661

動態測試中偵測樣本數 B=373

樣本包樣本總數 C=2059

誤報測試中誤報樣本數 D=0

則最後總分=（A+B）/C*100-lg(D+1)=（1661+373）/2059*100-lg(0+1)=98.79

測試總結

廠 商		靜態測試	動態測試	偵測總數	偵測率	誤報	得分
AVIRA	Avira	2056	0	2056	99.85%	3	99.25
Dr.WEB	Dr.Web	1907	49	1956	95.00%	2	94.52
A-SQUARED ANTI-MALWARE EMSI SOFTWARE	Emsisoft	2056	0	2056	99.85%	10	98.81
Filseclab Securing Your PC!!	Filseclab	1661	373	2034	98.79%	0	98.79
F-SECURE	F-Secure	2024	25	2049	99.51%	1	99.21
G DATA	G DATA	2057	2	2059	100.0%	5	99.22
IKARUS security software	IKARUS	2056	0	2056	99.85%	10	98.81
江民杀毒软件	Jiangmin	1907	133	2040	99.08%	2	98.60
KASPERSKY	Kaspersky	2031	24	2055	99.81%	1	99.50
	Kingsoft	1722	165	1887	91.65%	0	91.65
PANDA SECURITY	Panda	2052	1	2053	99.71%	1	99.41
Quick Heal	Quick Heal	1993	36	2029	98.54%	4	97.84
TREND MICRO	Trend Micro	1518	345	1863	90.48%	2	90.00
TrustPort	TrustPort	2054	1	2055	99.81%	9	98.81

月份認證結果

廠 商 名 稱	獲 得 認 證 標 識
KASPERSKY lab	2009 NO.03 Excellent ★★★★★ PC Security Labs
PANDA SECURITY	2009 NO.03 Excellent ★★★★★ PC Security Labs
AVIRA	2009 NO.03 Excellent ★★★★★ PC Security Labs
GDATA	2009 NO.03 Excellent ★★★★★ PC Security Labs
F-SECURE	2009 NO.03 Excellent ★★★★★ PC Security Labs
A-SQUARED ANTI-MALWARE EMSI SOFTWARE	2009 NO.03 Excellent ★★★★★ PC Security Labs
IKARUS security software	2009 NO.03 Excellent ★★★★★ PC Security Labs

廠 商 名 稱	獲 得 認 證 標 識
TrustPort	2009 NO.03 Excellent ★★★★★ PC Security Labs
Filseclab Securing Your PC!!	2009 NO.03 Excellent ★★★★★ PC Security Labs
江民杀毒软件	2009 NO.03 Excellent ★★★★★ PC Security Labs
Quick Heal®	2009 NO.03 Excellent ★★★★★ PC Security Labs
Dr.WEB	2009 NO.03 Standard ★★★★ PC Security Labs
	2009 NO.03 Standard ★★★★ PC Security Labs
TREND MICRO™	2009 NO.03 Standard ★★★★ PC Security Labs

免責聲明

It is not allowed to take parts of our testing result into own tests or to use the data ulterior without a written permission of PC Security Labs. We cannot be made liable for any damage or loss which might occur as a result of, or in connection with the use of the information provided on our website or testing reports. We try our best to ensure the correctness of the testing result, but we do not provide any guaranty for the correctness, completeness, etc. of both the information on our website and our testing reports at any time. You are allowed to download, view, print and copy the material from our site on the hard disk of your computer and to use it for your own personal, non-commercial purposes as a personal information resource in good faith only. It is forbidden to transmit or re-circulate any material obtained from PC Security Labs (including from the email delivered by PC Security Labs) to any third party without the written agreement of PC Security Labs. We focus on computer security and we try our best to protect the PC security. All the samples are from the Internet and we are not responsible for the malware samples. The research is taken in an internal network environment and we all remove the samples' extension in order to prevent incorrect manipulation by the user. We are not responsible for the damage caused by incorrect manipulation. In addition, we are also not responsible for the behavior taken by the outlaws. The testing report from PCSL is for reference only and the copyright of the testing report belongs to PC Security Labs. Any commercial activity wants to cite our report result please contact Jeffrey through his email address (jeffrey@pcsecuritylabs.net). For the monthly award logo, its use on the Internet, marketing materials and user documents by the antivirus vendor is free of charge. The annual certification logo is free of charge to be used on the Internet, marketing materials, user documents and the product packaging. For more detailed information about annual certification, please contact Jeffrey Wu via email: jeffrey@pcsecuritylabs.net. We have the right to withdrawn the license of monthly award and annual certification due to the improper use of the antivirus vendor.

All related issues about the testing, monthly award, logo, certification, legal notes, disclaimer, copyright, etc will be based on the latest PC Security Labs Manual. The copyright of this report belongs to Jeffrey Wu, PC Security Labs.