Anti-Virus Comparative

# Malware Removal Test

Language: English
October 2012
Last Revision: 11th November 2012

**www.av-comparatives.org**

# Table of Contents

# Tested Products

- avast! Free Antivirus 7.0
- AVG Anti-Virus 2013
- AVIRA Antivirus Premium 2013
- Bitdefender Anti-Virus Plus 2013
- BullGuard Antivirus 2013
- ESET NOD32 Antivirus 5.2
- F-Secure Anti-Virus 2013
- Fortinet FortiClient Lite 4.3
- G DATA AntiVirus 2013
- GFI Vipre Antivirus 2013
- Kaspersky Anti-Virus 2013
- Panda Cloud Antivirus Free 2.0.1
- PC Tools Spyware Doctor with AV 9.0

## Introduction

This test focuses only on the malware removal/cleaning capabilities, therefore all selected/used samples were samples that the tested Anti-Virus products were able to detect. It has nothing to do with detection rates or protection capabilities. Of course, if an Anti-Virus is not able to detect the malware, it is also not able to remove it. The main question was if the products are able to successfully remove malware from an already infected/compromised system. The test report is aimed to normal/typical home users and not Administrators or advanced users that may have the knowledge for advanced/manual malware removal/repair procedures. Most often users come with infected PC's with no (or outdated AV-software) to computer repair stores. The used methodology considers this situation: an already infected system that needs to be cleaned.

The test was performed in October 2012 under Microsoft Windows 7 Professional SP1 64 Bit. Only products available in English language whose vendors subscribed for the full 2012 public test-series are included in the malware removal test.

## Test-Procedure

- Thorough malware analysis to know what to look for
- Infect native machine with one threat, reboot and make sure that threat is fully running
- Install and update the Anti-Virus product
- *If not possible, reboot in safe mode; if safe mode is not possible and in case a rescue disk of the corresponding AV-Product is available, use it for a full system scan before installing*
- Run thorough/full system scan and follow instructions of the Anti-Virus product to remove the malware like a typical home user would do
- Reboot machine
- Manual inspection/analysis of the PC for malware removal and leftovers

## Malware selection

The samples have been selected by following criteria:

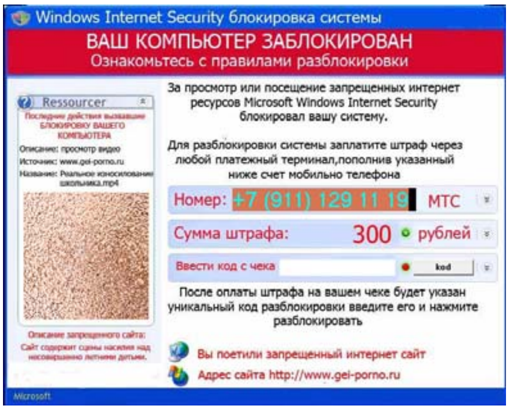
- All Anti-Virus products must be able to detect the used malware dropper on-demand/on-access
- The sample must have been prevalent (according to metadata on exact hashes) and/or seen in the field on at least two PC's of our local customers.
- The malware must be non-destructive (in other words, it should be possible for an Anti-Virus product to "repair/clean" the system without the need of replacing windows system files etc.) and show common malware behaviors (in order to represent also behaviors observed by many other malware samples). Due to that, the selected malware is representative of a very large amount of other samples that show similar behavior and system changes.
- We randomly took 11 malware samples from the pool of samples matching the above criteria. Additionally, we took three samples that have been used already last year, to see if there was an improvement and/or if the removal capabilities under Windows 7 are different.

## Used samples

Below is a list of the used samples[1]. Please do not wonder about the IDs in parenthesis, we mention them only as a reference for the tested AV vendors to identify them based on the samples they received from us after this test.

To avoid providing information to malware authors who could be potentially useful for them to improve their creations, this public report contains only general information about the malware/leftovers, without any technical instructions/details.

**Sample 1 (74b2f9):** This sample is a widespread ransom trojan horse. The user can circumvent the blocked screen by e.g. inserting and installing the AV product from a portable device.



Windows Internet Security блокировка системы

ВАШ КОМПЬЮТЕР ЗАБЛОКИРОВАН

Ознакомьтесь с правилами разблокировки

Последние действия вызвавшие БЛОКИРОВКУ ВАШЕГО КОМПЬЮТЕРА

Описание: просмотр видео

Источник: www.gei-porno.ru

Название: Реальное изнасилование школьника.mp4

Описание запрещенного сайта: Сайт содержит сцены насилия над несовершенно летними детьми.

За просмотр или посещение запрещенных интернет ресурсов Microsoft Windows Internet Security блокировал вашу систему.

Для разблокировки системы заплатите штраф через любой платежный терминал,пополнив указанный ниже счет мобильно телефона

Номер: +7 (911) 129 11 19 МТС

Сумма штрафа: 300 рублей

Ввести код с чека

После оплаты штрафа на вашем чеке будет указан уникальный код разблокировки введите его и нажмите разблокировать

Вы поетили запрещенный интернет сайт

Адрес сайта http://www.gei-porno.ru

**Sample 2 (5be0c6):** This sample is a widespread trojan horse.

**Sample 3 (aa8899):** This sample is a very widespread rootkit/bootkit which infects the MBR.

**Sample 4 (325d04):** This sample is a very widespread Autorun worm.

**Sample 5 (2895d5):** This sample is a very widespread backdoor.

**Sample 6 (88821e):** This sample is a widespread trojan horse.

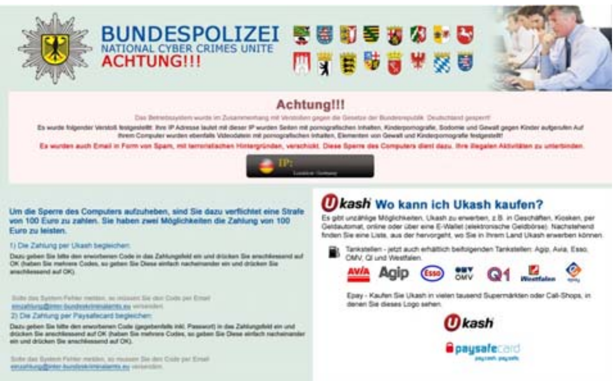
**Sample 7 (fd3bf7):** This sample is a widespread trojan horse.

**Sample 8 (e9bd7b):** This sample is a very widespread trojan horse.

**Sample 9 (902abd):** This sample is a widespread trojan horse.

[1] Initially we had some few more samples, but we removed/replaced them with other samples, as e.g. their malware behaviour was too similar with already included samples, which required a rescue disk. The samples/results included in this report were verified by the vendors after the test. One sample that showed different behaviour and could no longer be proved/confirmed by us and by several vendors was removed.

**Sample 10 (f8052c):** This sample is a common ransom trojan horse from the BKA-Trojaner or Ukash-ransomware family.



BUNDESPOLIZEI
NATIONAL CYBER CRIMES UNITE
ACHTUNG!!!

Achtung!!!

Das Betriebssystem wurde im Zusammenhang mit Verstößen gegen die Gesetze der Bundesrepublik Deutschland gesperrt!

Es wurde folgender Verstoß festgestellt: Ihre IP Adresse lautet mit dieser IP wurden Seiten mit pornografischen Inhalten, Kinderpornografie, Sodomie und Gewalt gegen Kinder aufgerufen Auf Ihrem Computer wurden ebenfalls Videodaten mit pornografischen Inhalten, Elementen von Gewalt und Kinderpornografie festgestellt!

Es wurden auch Email in Form von Spam, mit terroristischen Hintergründen, verschickt. Diese Sperre des Computers dient dazu, Ihre illegalen Aktivitäten zu unterbinden.

IP:

Um die Sperre des Computers aufzuheben, sind Sie dazu verflichtet eine Strafe von 100 Euro zu zahlen. Sie haben zwei Möglichkeiten die Zahlung von 100 Euro zu leisten.

1) Die Zahlung per Ukash begleichen:

Dazu geben Sie bitte den erworbenen Code in das Zahlungsfeld ein und drücken Sie anschliessend auf OK (haben Sie mehrere Codes, so geben Sie Diese einfach nacheinander ein und drücken Sie anschliessend auf OK)

Sollte das System Fehler melden, so müssen Sie den Code per Email einzahlung@inter-bundeskriminalamts.eu versenden.

2) Die Zahlung per Paysafecard begleichen:

Dazu geben Sie bitte den erworbenen Code (gegebenfalls inkl. Passwort) in das Zahlungsfeld ein und drücken Sie anschliessend auf OK (haben Sie mehrere Codes, so geben Sie Diese einfach nacheinander ein und drücken Sie anschliessend auf OK).

Sollte das System Fehler melden, so müssen Sie den Code per Email einzahlung@inter-bundeskriminalamts.eu versenden.

Ukash Wo kann ich Ukash kaufen?

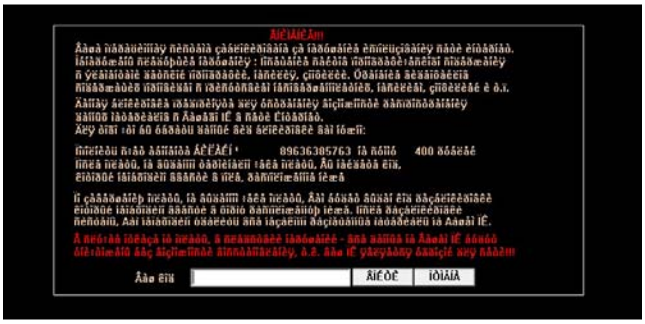
Es gibt unzählige Möglichkeiten, Ukash zu erwerben, z.B. in Geschäften, Kiosken, per Geldautomat, online oder über eine E-Wallet (elektronische Geldbörse). Nachstehend finden Sie eine Liste, aus der hervorgeht, wo Sie in Ihrem Land Ukash erwerben können.

Tankstellen - jetzt auch erhältlich beifolgenden Tankstellen: Agip, Avia, Esso, OMV, Q1 und Westfalen.

Epay - Kaufen Sie Ukash in vielen tausend Supermärkten oder Call-Shops, in denen Sie dieses Logo sehen.

**Sample 11 (1114df):** This sample is a widespread worm.

**Sample 12 (96a126):** This sample is a very widespread ransom trojan horse. This sample is a typical widespread ransom Trojan that takes the system as hostage. This common malware shows the importance of rescue disks for home users. Rescue disks, which only delete the file but do not fix the registry, will not solve the problem, as in that case Windows Explorer will not load.



[illegible]

[illegible] 89636385763 [illegible] 400 [illegible]

[illegible]

**Sample 13 (ccf34e6):** This sample is an extremely widespread worm.

**Sample 14 (1d88a7):** This sample is a widespread trojan horse.

## Ratings

We allowed certain negligible/unimportant traces to be left behind, mainly because a perfect score can't be reached due to the behaviour / system modifications done by some of the used malware samples. The "removal of malware" and "removal of leftovers" are combined into one dimension and we took into consideration also the "convenience". The ratings are given as follows:

a) Removal of malware / traces

- Malware removed, only negligible traces left (A)
- Malware removed, but some executable files, MBR and/or registry changes (e.g. loading points, etc.) remaining (B)
- Malware removed, but annoying or potentially dangerous problems (e.g. error messages, compromised hosts file, disabled task manager, disabled folder options, disabled registry editor, detection loop, etc.) remaining (C)
- Only the malware dropper has been neutralized and/or most other dropped malicious files/changes were not removed or system is no longer normally usable / Removal failed (D)

b) Convenience:

- Removal could be done in normal mode (A)
- Removal requires booting in safe-mode or other build-in utilities and manual actions (B)
- Removal requires Rescue Disk (C)
- Removal or install requires contacting support or similar / Removal failed (D)

## Award system

The following award / scoring system has been used:

AA = 100
AB = 90
AC = 80
BA = 70
BB = 60
BC = 50
CA = 40
CB = 30
CC = 20
DD = 0

The awards are then given based on the reached rounded mean value:

86-100 points: ADVANCED+
71-85 points: ADVANCED
56-70 points: STANDARD
Lower than 56 points: TESTED

## Results

Based on the above scoring system, we get the following summary results:

| | Sample | | | | | | | | | | | | | | Points |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | ∅ |
| **Avast** | AA | BA | BA | BA | AA | BA | AA | DD | BA | DD | DD | BA | DD | AA | 59 |
| **AVG** | AA | BA | BC | BA | BA | BA | AA | BA | BA | BC | BC | BA | DD | AA | 67 |
| **AVIRA** | AA | AA | CC | AA | AA | AA | AA | DD | AA | BC | DD | AC | AA | AA | 75 |
| **Bitdefender** | AA | AA | AA | AA | AA | AA | AA | BA | AA | BC | AA | AA | AA | AA | 94 |
| **BullGuard** | AB | AA | BA | AA | BA | AA | AA | BA | AA | DD | DD | AA | AA | AA | 79 |
| **ESET** | AA | AA | BC | AA | AA | AA | AA | AA | AA | BC | BC | CC | DD | AA | 76 |
| **F-Secure** | AA | BA | BC | AA | AA | AA | BA | AA | AA | BC | BC | BA | DD | AA | 76 |
| **Fortinet** | AA | BA | BA | AA | BA | AA | BA | BA | AA | DD | BA | CA | AA | AA | 76 |
| **G DATA** | BA | AA | BC | AA | BA | BA | BA | BA | AA | BC | BC | BA | BA | BA | 72 |
| **GFI Vipre** | AA | AA | BA | AA | AA | AA | BA | BA | AA | DD | DD | CA | AA | AA | 75 |
| **Kaspersky** | AA | AA | AA | AA | AA | AA | AA | AA | AA | BC | BA | AA | AA | AA | 94 |
| **Panda** | AA | AA | BC | AA | BA | AA | BA | AA | AA | BC | BA | AA | AA | AA | 86 |
| **PC Tools** | AA | AA | BA | AA | AA | DD | AA | AA | DD | AB | BC | AA | AA | AA | 79 |

Good malware detection is very important to find existing malware that is already on a system. However, a high protection or detection rate of a product does not necessarily mean that a product has good removal abilities. On the other hand, a product with low detection rate may not even find the infection and therefore not be able to remove it.

Some users may wrongly assume that Anti-Virus products just delete binary files (probably because most Anti-Virus products usually list only infected files in their logs) and do not fix anything else, like e.g. the registry etc. This report is also intended as a little informational document to explain that professional Anti-Virus products do much more than just deleting malicious files.

We advise users to do regular backups of their important data and to use e.g. image restoring software.

Most AV vendors have by now already addressed and fixed/improved the next releases of their products based on our findings in this report.

## Additional Free Malware Removal Services/Utilities offered by the vendors

| | Boot-Disk[2] available | Free Removal-Tools |
|---|---|---|
| **Avast** | - | - |
| **AVG** | YES | http://www.avg.com/virus-removal |
| **AVIRA** | YES | http://www.avira.com/en/downloads#tools |
| **Bitdefender** | YES | http://www.bitdefender.com/free-virus-removal/ |
| **BullGuard** | - | - |
| **ESET** | YES | http://kb.eset.com/esetkb/index?page=content&id=SOLN2372 |
| **F-Secure** | YES | http://www.f-secure.com/en/web/labs_global/removal/easy-clean |
| **Fortinet**[3] | - | http://www.fortiguard.com/antivirus/malware_removal.html |
| **G DATA** | YES | http://www.gdata.de/support/downloads/tools.html |
| **GFI Vipre** | YES | http://live.vipreantivirus.com/ |
| **Kaspersky** | YES | http://support.kaspersky.com/viruses |
| **Panda** | YES | http://www.pandasecurity.com/homeusers/downloads/repair-utilities/ |
| **PC Tools** | YES | - |

The customer support of AV vendors may help the users in the malware removal process. In most cases, such support services are nowadays charged separately, but several vendors may provide to their customers malware removal help for free (i.e. service included in the charged product fee). We suggest to users with a valid license to try contacting in any case the AV vendor support by email if they have problems in removing certain malware or issues while installing the product.

How some AV vendors could improve the help provided for home users with an infected system:

- provide/include a rescue disk in the product package (or point to links where to download it)
- provide up-to-date offline-installers (e.g. if malware blocks access to the vendors website)
- do not require the user to login into accounts to install products or to activate the cleaning features (as malware could intercept passwords etc.) and provide cleaning abilities also in trial mode (for infections which do not allow to register the product / to enter the license keys)
- check for active malware before attempting installation
- point to standalone tools if installation fails or if malware could not be successfully removed
- include tools/features inside the product to fix/reset certain registry entries / system changes
- promote more prominently the availability of additional provided free malware removal utilities and free malware removal procedures/support on the website, manuals, inside the product or when an active infection is found

[2] Included in the standard package without extra charging (and without the need to contact/request it from the vendor support personnel).
[3] Fortinet is a corporate product.

## Awards reached in this test

The following awards / certification levels have been reached by the various products in this specific test:

| AWARDS | PRODUCTS |
|---|---|
| AV comparatives ADVANCED+ ★★★ MALWARE REMOVAL NOV 2012 | Bitdefender<br>Kaspersky<br>Panda |
| AV comparatives ADVANCED ★★ MALWARE REMOVAL NOV 2012 | BullGuard<br>PC Tools<br>ESET<br>F-Secure<br>Fortinet<br>AVIRA<br>GFI Vipre<br>G DATA |
| AV comparatives STANDARD ★ MALWARE REMOVAL NOV 2012 | AVG<br>Avast |
| AV comparatives TESTED MALWARE REMOVAL NOV 2012 | - |

## Copyright and Disclaimer

AV-Comparatives e.V. and its testers cannot be held liable for any damage or loss, which might occur as result of, or in connection with, the use of the information provided in this paper. We take every possible care to ensure the correctness of the basic data, but a liability for the correctness of the test results cannot be taken by any representative of AV-Comparatives e.V. We do not give any guarantee of the correctness, completeness, or suitability for a specific purpose of any of the information/content provided at any given time. No one else involved in creating, producing or delivering test results shall be liable for any indirect, special or consequential damage, or loss of profits, arising out of, or related to, the use or inability to use, the services provided by the website, test documents or any related data. AV-Comparatives e.V. is a registered Austrian Non-Profit-Organization.

For more information about AV-Comparatives and the testing methodologies, please visit our website.

AV-Comparatives e.V. (November 2012)