

Avira Web Protection

(Detections)

HowTo

Table of contents

1. Introduction	3
2. Example detections	4
3. Other detections	5
4. Test options - testing Web Protection	5
5. Possible questions and answers	6

1. Introduction

This quick tutorial examines the various Web Protection detection types.

A detection in the Avira Web Protection can have various causes. A detection can be caused by:

- Calling infected files on the Internet
- Visiting a website which distributes malware or carries out phishing
- Pages which are filtered by the Proventia Web Filter (Cobion)

In these cases the Web Protection draws on the following sources:

- **Virus definition file (VDF) and engine**

The VDF only reports a detection if an entry exists for an infected file. The engine uses a generic and a heuristic detection system.

- **Webcat database**

The Webcat contains a database of different websites in the following categories: Malware, Phishing, Spam, and Fraud and Detection

- **IBM Proventia Web Filter (Cobion)**

The Proventia Web Filter expands the database with real-time requests and other categories.

Please note that the Proventia Web Filter is only available with the following products:

- Avira Internet Security 2012
- Avira WebProtector (für KEN!)
- Avira WebGate Suite

2. Example detections

```
[EVALUATION] [860] The URL (http://www.site.com/) has been evaluated as Fraud/Deception(c). It has been blocked
```

This detection is a Webcat event and is therefore identified with a (c).

```
[EVALUATION] [964] The URL (http://www.site.com/test_61.html) has been evaluated as Malware(p). It has been blocked
```

This detection is a Cobion event. In this case the “Malware” category is active. The detection event marker is the (p). This stands for the IBM Proventia Web Filter.

```
[EVALUATION] [907] The URL (http://www.site.com/malware-test.html) has been evaluated as Malware(c). It has been blocked
```

This detection is a Webcat event within the Malware category and is therefore identified with a (c). Categories can be defined in the configuration under *Web Protection > Search > Blocked access > Web-Filter*.

```
[INFO] [856] The URL (http://www.site.com/) has been evaluated as Illegal Activities. It has been blocked
```

This detection is an IBM Proventia Web Filter event and this category is therefore not available in WebCat.

```
[INFO] [959] The URL (http://www.site.com/index.php) has been evaluated as Pornography. It has been blocked
```

This detection is part of the IBM Proventia Web Filter, as this category is not available in WebCat.

```
[INFO] [968] The URL (http://www.site.com/) has been found in the Block List. It has been blocked
```

In this case, there is no detection in Webcat or in the Proventia Web Filter. This page has been manually blocked via parental controls.

3. Other detections

Detection through heuristics (HEUR/)

```
[EVALUATION] Malware found.  
URL: http://www.site.com/ort.html?id=2b9-12764  
contains suspicious code: HEUR/HTML.Malware
```

Detection through the Engine (Gen)

```
[DETERMINATION] Malware found.  
URL: http://www.site.com/  
contains virus patterns of the HTML script virus HTML/Infected.  
WebPage.Gen
```

Detection through the Virus Definition File (TR/, W32/, BDS/...)

```
[EVALUATION] Malware found.  
URL: http://www.site.com/17.exe  
is the Trojan horse TR/Spy.Veetle.
```

4. Test options - testing Web Protection

You can check whether WebCat is functioning via the following pages:

- **Malware:** [Avira Malware URL Test Page](#)
- **Phishing:** [Phishing Test Page](#)

Further test options, in particular for the IBM Proventia Web Filter, are available in the following products:

- Avira Internet Security 2012
- Avira WebProtector (für KEN!)
- Avira WebGate Suite

In these cases, various test pages are available (please note that not all categories are available in Avira Internet Security 2012):

[IBM Security Systems Support Resources](#)

If you want to know explicitly whether a specific page is listed in Cobion, you can access this information at:

[Test-a-Site](#)

5. Possible questions and answers

Question: Why is the same URL blocked twice?

```
[INFO] [969] Requested URL: http://www.site.com/  
[INFO] [969] The URL (http://www.site.com/) has been found in  
the Block  
List. It has been blocked  
[INFO] [970] Requested URL: http://www.site.com/favicon.ico  
[INFO] [970] The URL (http://www.site.com/favicon.ico) has been  
found in  
the Block List. It has been blocked
```

Answer: In this case the browser attempts to download “Favicon” separately and creates a separate access.

Question: Why, depending on the database, is a (c) or a (p) appended for the “Malware” category, but not for “Illegal Activities” or “Weapons/Military Items”?

Answer: (c) or (p) is only appended when this category exists in both databases.

Question: What do the numbers in the square brackets stand for?

Answer: The numbers describe the connection number in Web Protection. These are reset after each Web Protection restart.

Question: Are requests cached by the Proventia Web Filter servers?

Answer: Requests are not cached. For your security, a new request is carried out for each call event.

Question: What happens if the Proventia Web Filter server cannot be accessed?

Answer: If the Proventia Web Filter server cannot be reached, access to the website is permitted. The IBM infrastructure can also process a high volume of requests within a specified period.

This manual was created with great care. However, errors in design and contents cannot be excluded. The reproduction of this publication or parts thereof in any form is prohibited without previous written consent from Avira Operations GmbH & Co. KG.

Issued Q2-2012

Brand and product names are trademarks or registered trademarks of their respective owners. Protected trademarks are not marked as such in this manual. However, this does not mean that they may be used freely.



live free.™