Avira Protection Labs

Fast Facts

1. Where are Avira's Protection Labs located and why were those sites chosen?

The Avira Protection Labs are located in Tettnang (Germany) and Bucharest (Romania). These two sites allow the Avira Protection Labs to offer uninterrupted, 24-hour availability. In addition, Avira has a Response Team which can respond at any time to a current threat.

2. What types of malware are there?

There are different categories of malware, which is an umbrella term for "malicious software". For an overview of the different categories and a brief description, visit
http://www.avira.com/en/support-about-malware

3. Where does Avira get the latest malware from?

The Avira Protection Labs use honeypots at multiple locations to capture new, as-of-yet unknown malware. A global system monitors malicious URLs which are already known about, and immediately analyzes the appearance of new malware files. In addition to these sources, customers and independent security researchers regularly send Avira new malware files.

4. How do I send infected files to Avira?

Avira customers can upload or email infected files directly from the product (quarantine) to http://analysis.avira.com/samples or virus@avira.com. An additional address, virus_malware@avira.com, emails the Avira Support Team directly. These queries are forwarded directly to the Avira Protection Labs. Customers receive a response to all queries together with Avira Protection Labs' analysis result.

5. What methods does Avira use to detect malware?

Avira employs various technologies to detect malware. In all products with Web Protection, Internet data traffic is analyzed for malware, and access to known malware and phishing websites (URLs) is blocked. Every program is monitored in real-time on the user's system. When they are run, Avira Protection Cloud analyzes the suspicious files
http://www.avira.com/en/avira-protection-cloud.

Furthermore, all Avira products include traditional malware detection routines, such as signature search as well as heuristic and generic detection, in the engine and virus definition file (VDF).

Avira Operations GmbH & Co. KG
Kaplaneiweg 1
88069 Tettnang
Germany
Phone: +49 (0) 7542-500 0
www.avira.com

live *free.*™

Avira Protection Labs

Fast Facts

6. How many infected files are added to the detection system each day?

Avira Protection Labs receive an average of 200,000 – 250,000 new malware files every day. Depending on the threat level and malware used, on average 9,000 to 10,000 new detections are added to Avira's signature database each day.
A signature often detects more than one file, and is able to detect millions of malware files.

7. What are whitelisted files?

Avira products stop reporting files if, for instance, they have been detected heuristically or generically by the engine and have been whitelisted, meaning added to the exceptions list, via the detection pattern database. This technique is used to eliminate false positives without needing to update the engine each time one is detected.

8. How is quality assurance performed?

Avira Protection Labs have their own quality-assurance department: Protection QA. Prior to each detection pattern database update, several million files are scanned and analyzed to determine they contain no false positives. These files relate to widely used software such as Microsoft Office and Microsoft Windows, etc.

Several employees are hard at work every day incorporating new software into our test environment.

9. When malware is detected, how long does it take on average until a VDF update is issued?

Avira usually responds to new malware in well under an hour. This includes the analysis, development of antivirus updates (signatures), and extensive quality assurance.

10. Where do most attacks originate from?

The majority of infections are caused by drive-by downloads. These exploit the system's various security loopholes (besides those in Windows, there are also loopholes in third-party vendors' solutions such as Java, PDF, and Flash). Drive-by downloads are predominantly hidden in webpages. When the webpage is accessed, the download happens in the background, without the user's awareness, and the PC is infected. Another very widespread method is infection through the sending of spam. Here, the virus is sent with an email as an attachment or a link to a URL. To ensure the attachment is opened the user is often tricked into doing so, believing the attachment to be an invoice or photo.

Avira Operations GmbH & Co. KG
Kaplaneiweg 1
88069 Tettnang
Germany
Phone: +49 (0) 7542-500 0
www.avira.com