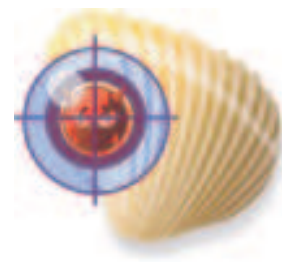


What's New

ClamAV 0.94



Sourcefire is pleased to announce ClamAV 0.94. The purpose of this document is to describe the new and improved capabilities of this product update that provide features to enhance protection against viruses and malware.

The following are the key features of this release:

- Logical signatures
- Anti-Phishing Technology
- Disassembly engine
- Improved scanning of scripts
- Data Loss Prevention (DLP)
- PUA Detection
- IPv6 support
- More flexibility when scanning remote file systems
- Improved QA and unit testing

The remainder of this document will explore the benefits of each key new feature.

Logical Signatures

New! Enhanced Detection Engine

Description: ClamAV now supports logical signatures. The logical signature technology uses operators such as AND, OR and NOT to allow the combination of more than one signature into one entry in the signature database resulting in more detailed and flexible pattern matching. This helps ClamAV catch modern ever-evolving scripting and complex malware.

Benefit: The enhanced ClamAV signature accuracy increases the detection of more complex malware and scripts.

Anti-Phishing Technology

Improved!

Description: Users can now change the priority and reporting of ClamAV's heuristic anti-phishing scanner within the detection engine process. They can choose whether, when scanning a suspicious file, ClamAV should stop scanning and report the phish, or continue to scan the file for other malware.

We have improved the flexibility in the way the regular expression parser handles URLs.

Benefit: By tuning the precedence of scanning, systems administrators can increase the scanning speed of ClamAV. Upon finding a match, the scanning engine stops, thus improving the efficiency of ClamAV.

This regular expression enhancement improves ClamAV's detection of malware where writers regularly change their subdomains, a common technique of phishing sites.

Disassembly Engine

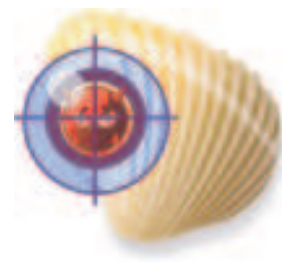
New!

Description: The bytes of a virus can now be examined more rigorously, improving the detection of encrypted malware. The disassembly engine improves detection of complex malware by disassembling and examining executable code at certain positions.

Benefit: The disassembly engine allows signature writers to create more reliable signatures.

What's New

ClamAV 0.94



Improved Scanning of Scripts

Improved!

Description: We have improved the normalization of scripts, in particular JavaScript programs. ClamAV 0.93 included normalization of text and HTML; 0.94 extends the module to cover JavaScript.

Benefit: Increasingly we find that malware writers obfuscate their script-based malware. The improved normalization will cause many obfuscation techniques currently employed by malware writers to evade detection to fail, resulting in improved detection rates.

Data Loss Prevention (DLP)

New!

Description: We have written a new module that, when enabled, scans data for the inclusion of U.S. formatted Social Security Numbers, credit card numbers and other personally identifying information.

Benefit: Identity theft is an increasing concern among both IT specialists and the public. This fully configurable module scans incoming and outgoing data for signs of Trojans that transmit private data. ClamAV, coupled with Snort, detects attempted data thefts.

PUA Detection

Improved!

Description: We improved the detection of PUAs (potentially unwanted applications) and now allow users to decide which signatures should be loaded by changes to clamd.conf.

Benefit: Users gain from an improved level of configurability in ClamAV's PUA feature. While ClamAV 0.93, required the entire feature to be on or off, 0.94 permits a user to block some signatures, for example jokes, while allowing others. We maintain a list of available PUA categories on www.clamav.net.

IPv6 Support

Improved!

Description: We have added IPv6 support to freshclam.

Benefit: IPv6 is increasingly used in intranets, and is a requirement for Japan because of its extensive adoption there.

More Flexibility when Scanning Remote File Systems on a File Server

Improved!

Description: We added an option to clamd to prevent the scanning of specific directories. This option was previously only available in clamscan

Benefit: File servers' systems administrators often wish to have per directory scanning configurability for remote file systems such as NFS and Samba. With this feature, system administrators can specify which directories to include in scans.

Improved QA and Unit Testing

Improved! Unit Tests

Description: The improved ClamAV's QA process now includes automated regression testing using white and black box methodologies. In addition to added API testing, we now create and distribute a library of files in various formats that are tested on a wide variety of systems.

Benefit: The continued support of different architectures and operating systems is ensured with better support and testing. Sourcefire is committed to supporting the widest possible combinations of platforms in use, including legacy systems.