Lavasoft's Innovative Detection Technologies

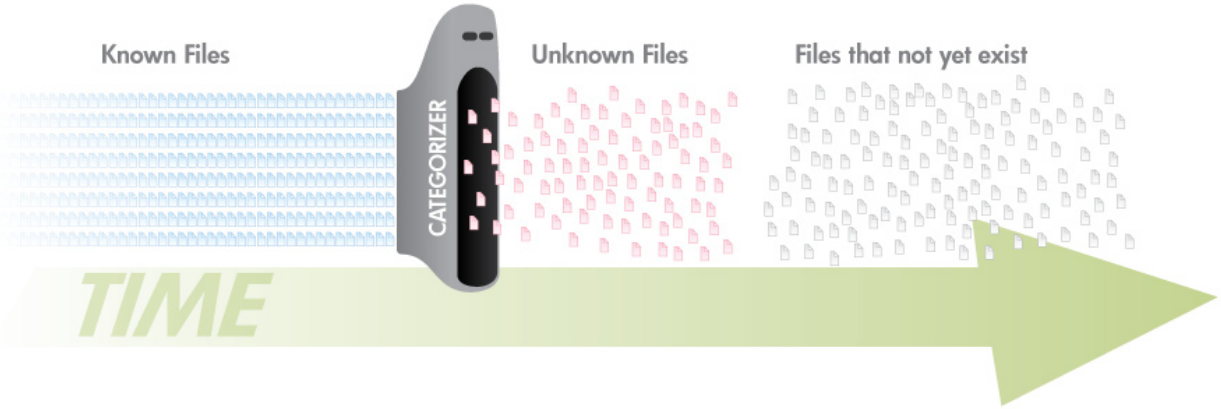
This version of Ad-Aware includes new anti-malware technologies, designed to give you maximum protection against the ever-evolving threats of today – and tomorrow. By focusing on new innovative solutions, we are able to increase the protection level for all Ad-Aware users.

Below is a brief overview of Lavasoft's new detection technologies: what they are, how they work, and the features that guarantee the best protection against today's sophisticated and constantly morphing cyber threats, as well as those threats that have not yet been created.

The Problem with Reactive Detection

The classic method for detecting malware is reactive, and quite simple. Most security companies have teams that analyze incoming malware samples. If a file is deemed to be malicious, it is added to the detection database.

The weakness of the reactive method is that only files that are known, i.e. files that exist in the database, will be detected by the scanner. The quality of the protection for the end user hinges on two things: the speed with which new files are added to the database, and that the user has the latest version of the database.



You can try to alleviate this problem by throwing more resources at the addition of new files, and issue new definition database updates more frequently, but the reality of it is this that at any given time, there are malicious files in the wild that are unknown to the scanner, simply because they are too new.

Polymorphism

To make matters worse, malware distributors—well aware of the weaknesses of reactive detection—are doing what they can to avoid detection by the security software vendors. They have come up with ways of changing the appearance of the files, while retaining their functionality, a phenomenon called polymorphism. The morphing of the files can take place both server-side, before they are distributed, or by letting the files change themselves as they replicate and spread.

This way, a single malware family may have hundreds of thousands of individual files. This makes the traditional, "one signature–one file" way of detecting malware increasingly unfeasible, since it is nearly impossible to find all permutations of a file. The massive amounts of files also make the signature databases grow incredibly large over time.

The Solution

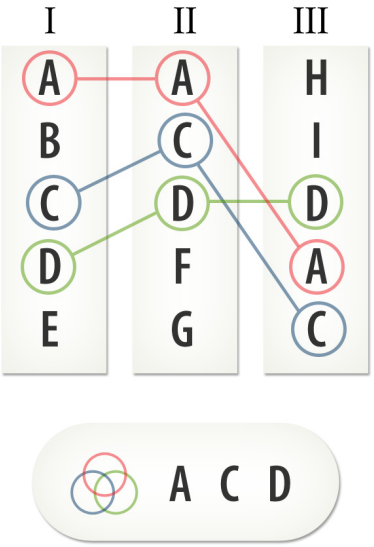
The solution is to create signatures based on generic traits of entire malware families, rather than the individual files. Family signatures are vastly more complex than file signatures, and take a lot more time and effort to create. The upside is that one family signature can detect thousands of files, including those that are yet to be seen, or even ones that that are yet to be created. This means that they provide proactive protection for the customers.

When creating family signatures, there is typically a correlation between how complex a signature is and how effective it is. In order to cover as much of the broad malware spectrum as possible, Ad-Aware employs proactive detection technologies that use signatures of varying complexity, which look at different aspects of the malware files. These technologies are described below.

Genocode

Lavasoft first added proactive detection to Ad-Aware with Genocode, in version 8.1. Genocode is a heuristics-based detection technology that uses family signatures, employing a system for cross-referencing properties in current threat samples. These properties are tracked across a set of collections, and are then cross-referenced in order to uncover and rate relationships.

For example, in the image on the right, columns I, II, and III each represent a known threat in Ad-Aware's Detection Database, and the varying properties (shown by A, B, C, etc) that make up its specific threat signature. The final column shows the signature created for the new threat variant resulting from the three malware samples.



Genocode processes and evaluates the three current threat samples – identifying the most prevalent and unique properties – and essentially captures the core of the threat variant. By cross-referencing properties using Genocode, Ad-Aware is able to assess and discover the strongest possible combined signature that best represents the new threat variant. Herein lies the power of Genocode – enabling proactive protection against evolving versions of threats that have not yet been created.

Introducing Dedicated Detection

In Ad-Aware 9, Lavasoft introduces a new proactive detection method, called Dedicated Detection (DD), a technology that looks inside files and analyzes the code. Based on this code analysis, a loosely defined pattern that detects families of malware is created. It is designed specifically to detect polymorphic and obfuscated files, and it operates on the processor (CPU) instruction level.

The resulting signatures are extremely powerful, with a single DD signature being able to detect hundreds of thousands of files. The examples below show the numbers for the two most efficient DD signatures.

Win32.Worm.Allaple

255,848 samples detected using one signature. The signature has detected 100% of new samples encountered since its creation.

Win32.Worm.Vbna

245,949 samples detected using one signature. The signature has detected 100% of new samples encountered since its creation.

At the time of writing, 16.8% of a target library of over 5 million files were detected using only 30 DD signatures, and the numbers only continue to improve as more signatures are added.

Introducing MagmaShield

In parallel to Dedicated Detection, our research team has also developed MagmaShield, a technology that searches for suspicious operations at certain points in a program, a pattern frequently found in malware. More specifically, MagmaShield emulates processor instructions, looking for operations that are valid on the processor (CPU) level, but undefined in the application layer.

This technology does not rely on patterns or signatures to detect, which makes it completely proactive. MagmaShield is able to flag objects as potential malware instantly, which makes it an excellent complement to the other proactive detection methods.

Below, we walk you through the technical and not-so-technical meaning behind the highlights of Ad-Aware's proactive detection technologies.

What our developers say…	What that means for you…
Genocode uses heuristics to detect evolving versions of threats.	Ad-Aware is able to find and detect newly emerging threats based on Genocode's analysis of the properties of existing threats, allowing you to be protected from threats that have not yet been created.
Ad-Aware proactively detects and blocks threats.	Not only can we find and detect threats on your system using our proactive detection methods, we're also able to block the potential threats that we have identified as malicious, *before* they load on your PC.
Genocode uses one-pass scanning, allowing for unmatched scalability.	A unique property of Genocode's scanning method—setting it apart from traditional anti-malware scanners—is its use of one-pass scanning. With traditional signature scanning, two threat signatures require two passes by the scanner, while 100 threat signatures require 100 passes, and so on. With the new Genocode technology, millions of threat signatures are scanned in just one pass. Regardless of whether two or two million signatures are scanned, the speed won't slow down. The end result for you: scanning is always quick and efficient.
Ad-Aware proactively detects rogues.	Rogue security programs (also called scareware), applications that masquerade as legitimate security software—often to install malware or steal personal information—are one of today's fastest growing threats to consumers. Ad-Aware uses its proactive technologies to detect and alert you to rogue installations.
Dedicated Detection is resistant to false positives.	One main problem with heuristics in other security products is that detection is often prone to false positives. Dedicated Detection is resistant to false positives, due to the way threats are compared against multiple threat signatures, ultimately meaning better accuracy in what is detected as a threat.