

Quick Guide to Ad-Aware's Genocode Detection System

Ad-Aware now includes new anti-malware technology, called Genocode, to keep you safe from the ever-evolving threats to your online privacy and security. Below is your quick guide to understanding Genocode: what it is, how it works, and the features which guarantee the best protection against the threats of today... and tomorrow.

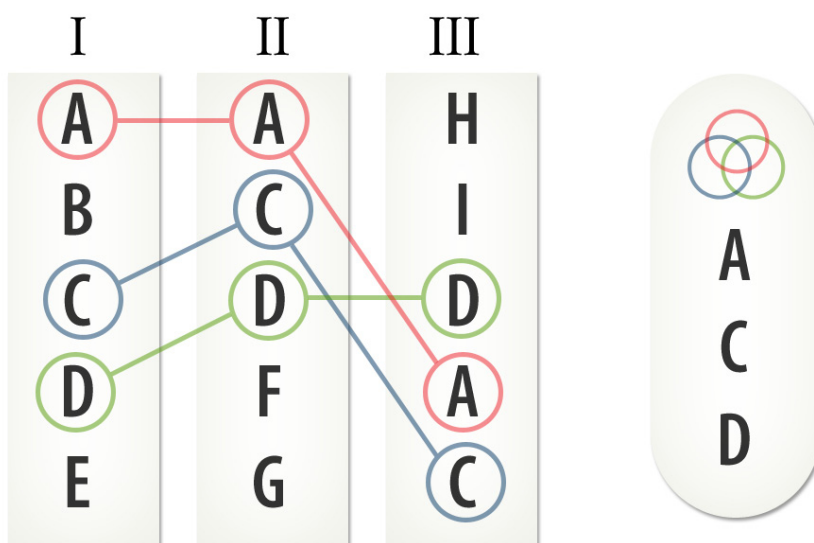
What is Genocode?

Genocode is a completely new malware detection system, based on heuristics, which is included in Ad-Aware Internet Security and Ad-Aware Total Security. Among the many advantages of this newly-developed Lavasoft technology, Genocode gives Ad-Aware the ability to find and proactively protect users from threats that have not yet been created, ultimately meaning you stay safer and more secure online.

How does Genocode work?

With traditional scanners, detection of threats is reactive, meaning that threats can only be found and removed once added into detection. With Genocode, Ad-Aware is able to proactively detect newly emerging threats by using 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 below, 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.

How does Genocode improve Ad-Aware's detection?

By using heuristics, the Genocode detection system allows Ad-Aware to stay a step ahead of the programs that pose a threat to your online privacy and security, meaning improved protection against today's sophisticated and morphing threats.

Below, we walk you through the technical and not-so-technical meaning behind the highlights of Genocode.

WHAT OUR DEVELOPERS SAY...

Genocode uses heuristics to detect evolving versions of threats.

Genocode proactively detects and blocks threats.

Genocode uses one-pass scanning, allowing for unmatched scalability.

Genocode proactively detects rogues.

Genocode is resistant to false positives.

WHAT THAT MEANS FOR YOU...

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.

Not only can we find and detect threats on your system using Genocode, we're also able to block the potential threats that we've identified as malicious, before they load on your PC.

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, in order to scan two threat signatures, two passes must be made by the scanner; in order to scan 100 threat signatures, 100 passes must be made by the scanner. With the new Genocode technology, millions of threat signatures are scanned, in just one pass. Regardless of whether Ad-Aware is scanning two or two million signatures, the speed of the scan won't slow down. The end result for you: scanning is always quick and efficient.

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. Through the Genocode technology, Ad-Aware is able to proactively detect and alert you to rogue installations.

One main problem with heuristics in other security products is that detection is often prone to false positives. Genocode 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.

CONTACT INFORMATION



www.lavasoft.com



+46.(0)31.777 77 50



+46.(0)31.15 69 10



Lavasoft AB
Odinsgatan 10
411 03 Gothenburg
Sweden