



Leveraging community intelligence to combat malware

INTRODUCTION

With a membership of around a hundred million people worldwide, the avast! community provides a powerful tool to both strengthen the community's security and to enhance the performance of avast! itself.

This white paper explains how AVAST Software harnesses community intelligence for the benefit of its users.

HOW COMMUNITY INTELLIGENCE CAN HELP IN THE FIGHT AGAINST MALWARE

With malware evolving at an unprecedented rate and social media enabling rapid propagation, it has become increasingly critical that security vendors are able to quickly respond to new and emerging threats. All versions of avast! antivirus include multiple sensors that continuously monitor key areas of the user's computer for any signs of activity that may be malware-related. Monitored areas include:

- The registry
- The file system
- The network (HTTP-based communication)

Should any suspicious actions be detected, avast! can automatically block those actions, copy the suspicious files and send these copies, together with relevant contextual information, to the avast! Virus Lab for detailed analysis.

There are two primary categories of data collected by avast!:

- Contextual information on viruses – includes the virus name, when the virus appeared, and information on associated files. While the AVAST database already contains copies of most viruses in circulation, this additional information helps us track how a specific virus is spreading.
- Data on suspicious behavior - suspicious behavior is identified by avast! sensors and data on the

suspect files is submitted to the Virus Lab for more detailed analysis. These samples can be used to create new virus definitions which are then distributed to all avast! users around the globe in the form of a virus definitions update.

In the past, users had to manually submit samples that they considered suspicious to the avast! Virus Lab. This was a process that was both slow and unreliable – it relied on users recognizing potentially malware-related behavior, deciding to submit the suspicious files and then working out which files needed to be submitted. In the current version of avast!, the entire process is completely automated and, therefore, substantially faster.

The enormous avast! user-base also contributes to the speed with which new threats are identified and neutralized. Because of the sheer size of the user community, there is a high probability that whenever a new threat emerges, it will be quickly encountered by an avast! user and information about the new threat

sent to the avast! Virus Lab. This enables a very quick reaction to new threats so that the time between when a new threat is identified and a virus definitions update released is very small. In this way, every user contributes to the protection of the entire community.

USING COMMUNITY INTELLIGENCE TO BOOST PERFORMANCE

Information gathered from the community enables AVAST to make avast! even more user-friendly. For example, less experienced users often find the prompts and alerts generated by firewalls to be thoroughly confusing (“Do you want XYZ to be able to act as a server and to connect to the internet on port 444?”).

By gathering data from its users, AVAST is gaining a clearer insight into their most commonly used applications and can build additional rules into the

firewall which will result in fewer alerts while providing the exact same level of security. This additional automation not only makes life easier for users by removing some of the decision making, but also lessens the chances of errors which could otherwise compromise their computer security.

PROTECTING USERS’ PRIVACY

Participation in the avast! community is – and will continue to be – entirely voluntary as AVAST provides users with easy opt-in or opt-out mechanisms. User data is submitted anonymously and without links to specific individuals or computers. The data is also not warehoused and is not used for marketing purposes. By cooperatively working with our community of users, we are able to collect all the data needed to keep the protection provided by avast! at the highest level.

ABOUT AVAST SOFTWARE

Based in the Czech Republic, AVAST Software a.s (formerly ALWIL Software a.s.) has been producing industry-leading security solutions since 1991 and is the developer of the award-winning avast! product line. As a global company, AVAST has partners all around the world who contribute to the continuous development and improvement of their products and provide technical support to clients in their native language.

AVAST’s mission is to provide both home users and businesses with solutions that are easy-to-use, affordable and exceptionally effective.

To find out more about AVAST Software and the avast! product line, please visit www.avast.com.