# Anti-Virus: Little More Than a Team Player

28 March 2014
**Ryan W Smith**

While anti-virus plays an important role in complete security architecture, gone are the days when it's acceptable to simply install anti-virus and consider oneself secure.

Imagine that the FBI* is conducting a nationwide manhunt looking for a suspect and they've sent out every image they can find from Facebook, Instagram, TwitPic and even printed pictures found in the suspect's house. Trying to sneak through the border, the victim concocts a disguise by cutting and dyeing their hair red, wearing green contacts, inserting lifts into their shoes, and adding fake facial hair. Using this new look that doesn't exist in any of the previous pictures, the suspect is allowed to pass by the FBI without objection.

While the FBI is far more capable than to be duped by such a basic disguise, most of the anti-virus systems are regularly fooled by this type of trickery every day. This is because most anti-virus still heavily relies on 'static signatures' or characteristics of a file or program that match various malware they've seen before. This makes the traditional anti-virus defense brittle, letting through malware that has never been encountered, or has been tweaked slightly to bypass any checks.

Now imagine the FBI stops the suspect for questioning at the border because they noticed the suspect had driven over 1,000 miles in one day to get to the border, was talking frantically, and was carrying over $10,000 in cash. They recognize that even though the person doesn't exactly match the description, there are enough behavioral indicators that something may be wrong. Considering both the suspect's appearance, as well as their behavior, law enforcement is able to successfully identify their target.

Similarly, a complete security solution should have the ability to detect malware based on observed behavior, even if it's disguised or not otherwise recognized. For example, by monitoring all network communications, a security solution would be able to identify and block connections to known 'bad addresses', both preventing the action and identifying the new malware. In many cases, the decision may not be black and white. For instance, on mobile devices, personal information is frequently accessed and transmitted by legitimate applications.

Although these applications are not malware, their activities may nonetheless present business risks to users. In these cases the binary question (Is it malware?) is insufficient, and instead the user should be able to block applications based on their level of risk tolerance.

To achieve the best level of protection, one should deploy a security system that provides a layered approach. The first layer of security would be to detect malware previously seen, or with obvious red flags. This initial layer is what's provided by most traditional anti-virus systems. The second layer one should look for is the ability to identify malware based on its behavior. This may be provided by monitoring your system to catch it in the act, or by running it in a sandbox, usually provided by uploading the application to a cloud service. By closely monitoring application behavior, the security system is able to flag and potentially block patterns that are considered high risk or malicious.

The third stage is integration with network-level security tools. This allows the security system to work in unison with network border protection to both prevent malware from leaking sensitive data, as well as updating the malware threat detection to better identify that type of malware in the future. Finally, for certain types of applications (such as mobile applications), the system should provide detailed analysis about the types of data the application has access to, and what is done with that information. Using this detailed data, the user would then be able to decide which applications present a high risk and block them, even if they're not malware.

Although a traditional anti-virus system is still recommended, it's only the first step and insufficient by itself. By deploying a layered, integrated threat defense system, one will have the best protection against both existing and unknown threats.

http://www.infosecurity-magazine.com/the-magazine/ 3449 п.з.

*FBI (Federal Bureau of Investigation) - ФБР, Федеральное бюро расследований (США)