WHAT IS YOUR ANTI-MALWARE DOING?

BY JAY BORDEN

Anti-malware applications are an essential ingredient in staying safe. To perform that task they need to have access to all your information. Some of that information is sent back to the main servers to compare against their collected information to identify malware.

Very understandable. However, do we ever consider what information is collected? Is it all needed for our protection? What is done with it besides working to protect us?

What data is necessary to collect is not a simple question. Certainly, your machine identifier and your device user name so it knows that you are a customer. Is the device user name your full name?

It also needs the version number of the anti-malware package purchased. A credit card number is needed to process the sale. The expiration date is used to validate the card. Your email address is used to send renewal notices. Most, if not all of that is certainly private information. What else is collected?

If the anti-malware looks at software vulnerabilities, it will have to examine all installed software packages and version numbers.

If it offers phishing protection, then it will send the URLs of all the sites you visit to its servers to see if any are on their list of compromised sites.

What else does it collect and what does it do with that information?

The EULA, End User License Agreement, or privacy policy should specify what information is collected and what is done with it. Is it used solely to protect you? Is it sold? If so, to whom is it sold? And for what purpose?

WHAT IS YOUR ANTI-MALWARE DOING?

CONTINUED

Is the data kept? Where is it kept? If a 3rd party cloud service is used how well do they protect your data? Are any other 3rd parties involved and for what purpose? How well do they protect your data?

We know that supply chain attacks are growing in popularity by attackers. The company should disclose their 3rd parties and examine their protections. Your relationship is with the anti-malware company, not 3rd parties.

You may be able to opt out of any data collection that isn't necessary to protect you in the anti-malware's settings.

While all this is important, it is good to remember that anti-malware program data collection is not your biggest risk. Phishing rates very high on the list as does human error. But all steps to protect your data are beneficial.

This Insight focused on anti-malware software because they need to capture information to protect you. But other software packages also collect information. I can't say every one of them because all haven't been examined. However, many collect data about you beyond what is needed to deliver the service or application you want. Many sell the data to third parties for their own benefit.

Social media companies are a prime example. There is no charge for their service, but they make billions of dollars a year by selling advertising. The more information they have about you the more targeted the advertising, and the more they can charge for it. They usually provide a way to opt out of some data collection but not all of it.

For any application or service you use, look at what is collected. This may be in the EULA or in the privacy policy. Opt out of everything you can that isn't needed. Remember no company is safe from attackers. The more information they have about people that hackers can use, the bigger a target they are.

Protect your private information and stay safer.

Visit our site, onebrightlycyber.com to learn all the ways we help keep you safer.

Welcome to peace of mind.