N·P·S NONPROFIT SERVICES Powered By VIENER4GATES

November 2018

We know firsthand from customer sites that malware attacks are on the rise. More importantly, *successful* attacks are rising. A virus is bad, but a trojan or zero-day attack is worse. It is easier to remove a virus than these more pervasive and malicious attacks.

These attacks can shut your business down for an unacceptable length of time. Maybe just for a few hours if you're fortunate, but perhaps several days or longer. Sometimes data is lost permanently. It's not a good scene. What is the difference between a malware attack and a virus? Actually, they are one and the same. Let's take a look:

"Malware is the collective name used to refer to malicious software or intent. These include Worms, Trojans, Ransomware, Spyware, Adware and, you guessed it, Viruses. So essentially, a virus is a type of malware. It works by executing into a user's machine unbeknownst to the user before proceeding to replicate and infect other programs and files in the computer. From there it moves onto other computers on the network.

New malware spreads more easily than viruses due to the way they operate, these are a great source of revenue to the bad guys." – Kevin Arrows

Attacks have evolved and eventually they will target you. It is just the law of averages. With all the threats out there, a common anti-virus might not be enough to protect you. You need a smarter anti-virus, plus anti-malware and some good common sense to stay as clean as possible.

The Evolution of Malware

Viruses have become harder to spread, so what do attackers do? They come up with new types of malware. You may also hear them being referred to as zero-day or zero-hour malware. These are new threats without a security patch.

- Cryptolocker Trojan – One good example of malware that was able to remain undetected by conventional antivirus programs is the Cryptolocker Trojan of 2013. This ransomware, considered to be one of the most dangerous of all time, used military-grade encryption to lock users out of their systems and stored the key in a remote server rendering it inaccessible. The creators then demanded payment via Bitcoin which, as you know, is untraceable. This same encrypting ransomware was used again in 2017 in the WannaCry Ransomware that hit over 150 countries and over 100,000 organizations.

Dealing with Malware Attacks

Ransomware detections have been more frequent in countries with larger internet-connected populations. The United States ranks highest with 18.2 percent of all ransomware attacks. Ransomware damage costs will rise to $11.5 billion in 2019 and a business or consumer will fall victim to a ransomware attack every 14 seconds at that time. (Cybersecurity Ventures).

Having antivirus alone is not enough. You need the extra protection of an anti-malware. I will use my favorite anti-malware software, Malwarebytes, to better explain how anti-viruses and anti-malware differ in protection methodologies and how they complement each other in fighting malware threats. Ask any cyber-security expert and they will probably tell you that Malwarebytes is the best anti-malware software right now.

Unlike the traditional antivirus software, Malwarebytes is able to flag and stop new threats that have not occurred in the past before they can turn into a disaster, whether they arrive through infected websites, suspicious emails, malicious links, browser extensions, or unwanted programs (PUP).

Malwarebytes uses what is called anomaly detection technology to match the behavior patterns of potential threats to existing threats, which is why it can detect malware even when there are no prior reported cases of similar infections. But when it comes to the older, more established threats, an antivirus is your best bet.

Protection against the older threats is thus left to the antivirus vendors who specialize in protecting the user against the older known threats, while antimalware protects the user against emerging threats. Take a look at this video link to see how Malwarebytes defends your PC and network against attack.