

Upgrade your anti-virus software

The world of viruses took another turn for the worse in September 2014. The CryptoLocker virus initially appeared in October 2013 and was the first to actually encrypt all of the data on your computer and demand a hefty ransom for its return.

Fast forward to September 2014 as the newer variant, Cryptowall 2.0 (since replaced by Cryptowall 3.0), began using Crypters to evade traditional anti-virus software. Crypters are new tools that change the signature of a virus payload. Traditional anti-virus software products use “signatures” to identify a threat about to attack your computer. Crypters are now readily available on the internet, and the Cryptowall authors are using Crypters to change their payload signatures more frequently than the anti-virus companies can keep up. Because of this, the traditional anti-virus products are not stopping Cryptowall.

To make matters worse, the Cryptowall authors also began purchasing banner ads in September to spread their virus. Using Flash and Java vulnerabilities, Cryptowall began infecting computers that simply visited web sites like yahoo.com, aol.com, and match.com (no clicks required). Basically, this means that visiting any legitimate web site containing banner ads can cause your computer to become infected. Again, you do not have to click on anything. Simply visiting a site is enough to spread the virus.

The bottom line is, we all need another layer of protection to combat Cryptowall, and the copycat viruses that are sure to follow. The best product to help keep computers and data safe is offered by a company called OpenDNS. The best OpenDNS product for home users is “Prosumer” (go to www.opendns.com, click on “For Personal” Tab, scroll to the bottom of the page, click “Check it Out” and review “Want a package for 1 to 5 Users?”). This product adds vital protection against the newest, most dangerous viruses.

OpenDNS uses internet traffic patterns to differentiate between normal good internet traffic, and internet traffic used to infect computers. When it detects bad traffic, it blocks it to keep your computer safe. Additionally, OpenDNS understands the internet traffic used to communicate with the Cryptowall encryption servers, and it blocks that traffic. So even if your computer gets infected, there is a good chance your data will not be encrypted.

In addition, I am now using Umbrella for all my clients, and we use Umbrella to block banner ads as an additional protective step.

Traditional anti-virus software is no longer capable of stopping the newest and most dangerous viruses. Updated tools such as OpenDNS Umbrella, should be used for all home computers as an added layer of protection against the newest, most dangerous, viruses.

Excerpted from Biondo Perspectives 4th Q 2014

Article by Greg Miller, President of CMIT Solutions, in Goshen, NY. He provides IT services to The Biondo Group, and serves as our company’s Chief Information Officer in conjunction with our Cybersecurity efforts.