The topics of this column include a situation in which anti-malware software rendered a computer useless; new cell-phone and other case designs from OtterBox; software that views, edits, and converts many different types of files; a hidden charge associated with using toll roads when driving rental cars; and a setting you may wish to change in the Firefox browser.

WHEN YOUR ANTI-MALWARE SOFTWARE BECOMES MALWARE

I’ve written several times about Malwarebytes’ Anti-Malware Premium software, most recently in the April 2018 and February 2016 issues of IEEE Antennas and Propagation Magazine. I’ve always found this software to do an excellent job of protecting against root kits and malicious Web sites. The various releases under Version 2 and earlier were intended to work with other publishers’ anti-malware software. Version 3, which was released about a year and a half ago, could also be used as a full-featured stand-alone product.

Like most anti-malware products, Anti-Malware Premium automatically updates itself (this includes updating both the databases it uses as well as the program code). On Saturday, 27 January 2018, Malwarebytes issued an update to their software that caused two very significant problems: it caused machines running their software to block a large range of Internet Protocol (IP) addresses, and it caused excessive RAM usage. From a practical standpoint, within 10–20 s of completing the booting process, the response of my machine to any input would slow down to the point of being basically unusable. Malwarebytes claimed that they detected the problem and posted a fixed update that when downloaded by the software should have immediately fixed the problem within three hours of when the original bad update was posted. The difficulty was that the problem would overwhelm the machine before the fixed update could be detected, downloaded, and installed. In short, a very large number of people’s machines (including mine) became unusable with no mechanism for fixing them.

The situation was so bad that even booting the machine in Windows’ Safe Mode and using System Restore to try to restore to an earlier “known-good” state wouldn’t work. I can’t say for sure that the problem with this approach was due to the Malwarebytes issue, but the problem went away after the Malwarebytes issue was resolved. Others whose systems were affected also noted that System Restore wouldn’t work. You know something really bad has happened when System Restore won’t work!

In spite of many hours of effort, my machine remained unusable for almost two days. That cost me a great deal of time, money, and frustration. I finally found mention of the cause of the problem on a forum on the Web. With that knowledge, I was able to use a combination of Safe Mode and forcing Anti-Malware Premium to immediately update itself upon booting to solve the problem.

In my opinion, what made this whole situation much, much worse than it should have been was that Malwarebytes made little attempt to publicize the problem, let alone the solution. As noted above, Malwarebytes claimed they had the problem fixed within three hours. They apparently posted a notice about the fix on their forum but, notably, did not e-mail their customers about it, and they did not issue a press release that would have resulted in out-of-channel information being passed on to those affected by the problem. That would have been very helpful to all of those who couldn’t use their computers to receive e-mail or visit the Malwarebytes forum because of what the Malwarebytes software had done to their machine! From the posts on the Malwarebytes forum, many, many...
customers lost huge amounts of time and money because they were not promptly informed of the cause of the problem and how to fix it.

As far as I can tell, Malwarebytes has never apologized for the problem. As far as I can tell, they have never acknowledged that there were other side effects besides the blocking of IP addresses and high RAM usage. As far as I can tell, they have never admitted that posting a fixed update might not have been sufficient to fix the problem with many users’ machines.

It is easy for an experience such as this to cause you to lose faith in a software company. That was reinforced when a subsequent update to Anti-Malware Premium did not properly install. That left Anti-Malware Premium removed from my machine. I didn't bother trying to reinstall it. My machine now boots noticeably more quickly. I had written before that, on the few occasions when my computer has been attacked by malware, it was Anti-Malware Premium that first detected and neutralized the threat in almost every instance. Unfortunately, Anti-Malware Premium has now become a bigger threat than the malware against which it protects. I no longer recommend it, and I won’t put it on my machines.

NEW CASE DESIGNS AND OTHER ITEMS FROM OTTERBOX

I’ve written several times before about the incredible protection OtterBox (www.otterbox.com) cases and their companion cover-glass products give cell phones. My daughter’s phone in an OtterBox case has survived being dropped from a horse. More recently, one of her cell phones in an OtterBox case with Alpha Glass survived being stepped on by a horse!

The real news here is that OtterBox has added a very wide and interesting variety of theme designs to its Symmetry line of cases. These include classic Disney themes (think Mickey, Minnie, and friends), modern Disney, Marvel, Star Wars, NFL, Call of Duty, and what they call Studio Collections. These are miniature works of art on cell-phone cases. The Symmetry case is about as thin as a case can be and still provide robust protection. The new designs make it much more interesting and/or beautiful.

OtterBox makes a protective glass for cell phones and tablets they call Alpha Glass. I’ve used this on several cell phones, and it does an excellent job of protecting the cell-phone screen from scratches and breakage without having any effect on visibility or touchscreen operation. It is also very easy to install. They have Alpha Glass for tablets, as well.

OtterBox makes cases for tablets. They also just introduced a line of portable hard- and soft-sided drink coolers in a variety of sizes. What distinguishes these is that they have the same reputation for ruggedness as the cell-phone cases, and they keep items cold for a very long time. The soft-sided coolers are supposed to keep ice frozen for up to three days. The hard-sided coolers are supposed to keep ice frozen for up to ten days, and some are certified bear resistant!

A FILE VIEWER THAT DOES FAR MORE THAN VIEW FILES

File Viewer Plus 2 (www.fileviewer-plus.com) is a small Windows utility that does far more than its name implies. It will open and allow viewing of files in more than 300 formats. This includes all of the formats associated with Microsoft Office, PDFs, most all image and graphic formats, HTML, most music-file formats, and most video formats. It allows you to edit Microsoft Word documents, spreadsheets, and image files, and to save the edited versions (without having to have the actual associated application on your computer). Perhaps, most importantly, it allows converting files from one format to another and saving the results. As just one example, I’ve found that File Viewer Plus 2 does a better job of converting Word .docx files to .doc format than the Microsoft Office Compatibility Pack. Documents that the Compatibility Pack scrambled came out perfectly when converted using File Viewer Plus 2.

A complete list of what formats File Viewer Plus 2 will handle and which of these formats it can edit and convert is given on the Web site. A free trial is available. The full version is US$39.95. The software runs under Windows XP and all later versions of Windows.

A SUBSTANTIAL HIDDEN RENTAL-CAR TOLL-USAGE CHARGE

I recently rented a car from Hertz. I knew that I wanted to use a toll road on the way from the airport to my destination. I asked the Hertz attendant and was told that the car had an electronic toll device that would cause the amount of the road tolls to automatically be billed to me through Hertz after my rental. I also asked if there was any additional charge for the tolls associated with this. I was told there wasn’t.

I was therefore rather upset when I received a bill for US$24.75 in addition to the tolls from PlatePass (www.platepass.com). After a lot of research (that really means, after a lot of being passed from one person to another at both Hertz and PlatePass), what I considered to be a rather nasty story emerged.

Supposedly, buried in the copy of the contract I received from Hertz (I no longer have a copy of the contract, and I’m not sure I ever received one), and contrary to what I was explicitly told by the Hertz attendant, there are administrative charges added to any use of a toll road. In the case I experienced (which is apparently typical for a rental in the United States), these amounted to US$4.95/day. This amount is added per day once you use a toll road for the duration of your rental, no matter whether you use another toll road, up to a maximum amount per month (the maximum in this case was US$24.75; you are only charged for months in which you use a toll road if you rent for
more than a month). In my case, the administrative charges were approximately double the tolls I paid. This was, in part, because I only used the toll road for two days (going from and returning to the airport), while I was charged the administrative charge for the full week of my rental.

PlatePass is a separate company from Hertz, and it appears that many other rental-car companies in the United States also use it. My attempts to get an explanation for the charges resulted in repeated instances of Hertz putting responsibility on PlatePass and PlatePass putting responsibility on Hertz. Representatives from both treated me in a manner that made me think they must really hate my business.

What is insidious about this is that more and more U.S. toll roads are eliminating the option of paying cash for their use. This means that if you rent a car and want to use a toll road (which, in many instances, is the only practical option), you are going to be stuck with a much higher effective “toll” than you may expect. In the future, I plan to avoid using toll roads in rental cars where I can.

A SETTING YOU MAY NEED TO CHANGE IN FIREFOX

Internationalized domain names have been supported on the Web for some time. This allows the use of non-Latin-alphabet characters in domain names for Web sites. Since some characters in other alphabets are visually the same as some Latin characters (e.g., “c” in the Latin alphabet looks the same as the letter “s” in the Ukrainian and Russian alphabets), domain names can be crafted that appear to mimic well-known names but are made up of characters that have different Unicode values. This makes it possible to register look-alike domain names.

To protect against confusion and people being inappropriately redirected to Web sites for malicious purposes, most Web browsers convert an address in their address bars into what is called punycode. This provides a unique representation of characters from non-Latin alphabets. The Chrome, Safari, and recent versions of Internet Explorer and Edge browsers do this. Mozilla’s Firefox does not. Mozilla has some justifications for this. However, if you want Firefox to show the punycode in its address bar so that you can recognize when a “look-alike” domain name is being used, you can change a setting.

To do this, type “about:config” (without quotes) in the Firefox address bar. Agree to accept the risk, and then type “punycode” (without quotes) in the search box. Locate the value “network.IDN_show_punycode.” The default setting of this is false. It needs to be set to true, which can be done by double clicking it.

The information for this item came from a post on the www.krebsonsecurity.com blog.

ERRATA

In the February 2017 issue of IEEE Antennas and Propagation Magazine, there were errors in (1) of [1]. Equation (1) is missing the minus sign from the first two terms in the denominator. Moreover, these two terms should be within the square root. The correct equation is

\[
G = \frac{4\pi r}{\lambda} \frac{1 - \Gamma_\delta \Gamma_L}{1 - \Gamma_\delta \Gamma_C} \sqrt{\frac{P_t}{P(1 - \Gamma_\delta^2)(1 - \Gamma_C^2)}} \tag{1}
\]

These errors were caused partly by the authors’ oversight and partly during the production process. It is noted that the reflection coefficient terms under the square root do not significantly affect the gain and uncertainty values reported in [1]. We sincerely apologize for the error and any confusion it may have caused.

REFERENCE