COMPUTER NEWS from the

DECEMBER 2014 Volume 2 NO.12

As found on the web and other sources

I got your mobile phone and you can't do anything about it!

Well maybe not. Read on and find all about how to be safer on your mobile equipment.

New Mobile Malware Threat

Category: Mobile from "askbobrankin.com".

A well-known predator named "Koler" has ramped up its game from "drive-by download" to "self-replicating virus," accelerating the spread of this ransomware from one smartphone to all its owner's contacts. Read on to learn about a secret feature that will zap this and other mobile malware apps...

Got Koler Mobile Ransomware? Don't Panic!

Regular readers of this site may remember my article about Cryptolocker, a desktop malware menace that locks your computer, scrambles your files, and demands payment to restore access.

Likewise, Koler is mobile malware targeting Android smartphones and tablets, which extorts ransom from its victims, telling them their data has been encrypted and the key will cost money.

But don’t panic. Koler is mostly bluff, a serious nuisance, but one that’s essentially toothless and easily banished if you know a little “secret” about Android that even I wasn’t aware of until recently. (Be sure to see my rant below about "unknown sources" too...)

Koler has been known to security researchers since May, 2014. In its original form it seized control of an infected Android device, freezing everything and displaying a screen that demanded payment for unlocking the device. Koler infected Android devices by the classic “Trojan horse” ploy, masquerading as a benign app available for free download on numerous Web sites. But now it’s self-replicating, and that changes the game dramatically.

When the new Koler infects a device it still does its “stand and deliver” ransomware thing. A scary-looking image blocks your screen, pretends to be a message from the FBI, accuses you of viewing and/or storing vile materials on your phone, and demands payment in lieu of prosecution.

But also, it’s busy in the background sending text messages to all of the contacts stored on the infected device. It tells your friends, family, and associates that you have posted photos of them online and provides a link to the page where they can view themselves. That page, of course, has no photos but only a link that will trigger the downloading and execution of Koler on the new victims’ devices.

Time to Panic?

Denis Maslennikov, a security analyst with AdaptiveMobile, told TechNewsWorld, "This is the first time we've seen self-replicating ransomware on Android." Time to panic, right?

First, Koler (and almost ALL other Android malware that I'm aware of) can be installed ONLY if the user has modified their settings to specifically allow software to be installed from "unknown sources," which means sources other than the official Google Play Store. Click on Settings, then Security on your device. (On my Samsung Galaxy, I have to tap "More" to find the Security option under Settings.)

The factory setting for "Unknown sources" is OFF, and it should stay that way, unless you absolutely must install a trusted app from a third-party source. In such a case, remember to turn this setting back to OFF after allowing the install. **It irritates me to no end that tech writers, researchers and security analysts (who should know better) almost NEVER mention this very important fact.**

Here's a second reason not to panic. Even if you do take the bait, your data is not encrypted; that's a bluff. It won't be wiped out forever if you don't pay the ransom. You can access all of your data as usual and eradicate Koler if you know about Android's semi-secret "reboot to safe mode" feature. I've been using Android phones for years, and I didn't learn about this until recently.

Most tablet and smartphone users don't know about safe mode. They assume the only way to get rid of Koler is to do a factory reset, which wipes out all user data entered since the phone was activated. But in safe mode, all third-party apps are temporarily disabled, including Koler. Then you can use Android's built-in uninstall tool to remove "Photoviewer" -- the alias used by Koler. When you reboot again in normal mode, Koler will be gone.

To uninstall an app on your Android device, first open Settings, then Apps or Application Manager. (You may have to click the More tab to find it.) Tap the app you'd like to uninstall, then tap the Uninstall button. And poof, the stain's gone in the first wash!

How to Use Android's Safe Mode

If your device is ON: Press and hold the power button until the menu appears. Next, tap AND HOLD the Power Off button for a second or so, until the "Restart in Safe Mode" menu appears. Tap the "Turn On Safe Mode" button.

If your device is OFF: Press and hold the power-on button. As soon as the first screen or logo appears, press and hold the volume-down button simultaneously when restarting. On some devices, you'll need to press and hold BOTH the volume-up and volume-down buttons at once. On others, you need to press and hold the menu button. If that doesn't do the trick, search online for device-specific instructions on rebooting in safe mode.

When your device starts up in Safe Mode, you'll see "Safe Mode" in the lower left corner of the display. No third-party apps will be loaded when you start up in Safe Mode, nor will they appear on your Home screens. Restarting your phone normally will get you out of Safe Mode.

So Koler, the latest Android malware scare, is nothing to worry about if you follow my tip about not installing apps from unknown sources. And even if you or a friend does fall for this or a similar trick, now you know what to do.

What happened to Windows 9

Or here comes Windows 10: More Features Announced

By John Lister in “infopsckets.com”.

Microsoft has unveiled additional features for Windows 10, as well as making previously-announced features available for testing. Most of the changes are aimed at **mobile computer** users, but there will be a few extra improvements for **desktop users**.

Windows 10 Testing being done in Batches

Microsoft is taking a very deliberate approach with its **public testing program** for the new Windows 10 operating system. Rather than throw out a semi-completed version of Windows 10 for testing and deal with all the feedback at once, Microsoft is slowly adding new features to the test edition of the operating system, known as a **technical preview**. That should allow it to concentrate on a few elements at a time and fix any problems in batches, rather than all at once.

Among the changes is increased support for **touchpads**, which are finger-operated keyboard accessories that remove the need for a mouse. Touchpads are typically found on laptops, but are also sold as separate and **larger sized units for desktop PCs**. It's been said that Windows 10 will work with more gestures on touchpads, a move analysts suggest may have been inspired by features found on portable Mac computers.

Touchpad Triple Finger Gestures

The added touchpad support will mean users can use multiple fingers to perform a wider range of controls, similar to how a touchscreen operates on **tablet computers**. For example, putting three fingers on a touchpad and dragging them down at once will minimize all windows to expose the desktop, while dragging three fingers up will bring all open windows back to view.

Similarly, dragging three fingers left or right will cycle through open windows, duplicating the existing Alt + Tab command on a keyboard. The idea is that once users learn the controls, they'll be able to work more efficiently with less need to use a mouse. (Source: **pcworld.com**)

Windows 10 will also fix a limitation with the Snap feature, which automatically resizes an open window to fill exactly half the screen. Snap is typically used when working with multiple applications at once; for example: when using a web browser to research information while writing a Word document. The new Snap system will also be easier to use if you are running multiple monitors.

Smartphone Features Come To Windows

Two more changes will be particularly useful for **laptop** and **tablet users**. The DataSense feature keeps track of how much **WiFi** or mobile data you've consumed and will let you set controls to limit unexpected data use. This is especially useful for users on a limited mobile data plan and will help to avoid penalties for over-usage.

Meanwhile, the Battery Saver feature will replicate similar features on smartphones that limit unnecessary "behind-the-scenes" **CPU processing** activity when the system is running on battery, rather than main power. This will help to prolong the life of the battery between charges.

Desktop Mode for Apps

Finally, Microsoft is going to make life a little easier for people who prefer the old-style **desktop PC mode**, but still want to use some of the apps from the Windows store.

In Windows 10, users will be able to create a desktop shortcut to any app downloaded from the store, rather than having to switch to the modern interface just to launch it. This was a huge complaint for **Windows 8** desktop users, and as such, this feature will save a lot of 'back and forth' between interfaces. That said, it's not clear as to whether or not all apps will be compatible with the desktop interface, or if users will be forced to switch over to the modern interface once the app has launched. (Source: **makeuseof.com**)

Internet Explorer: The LEAST Secure Browser?

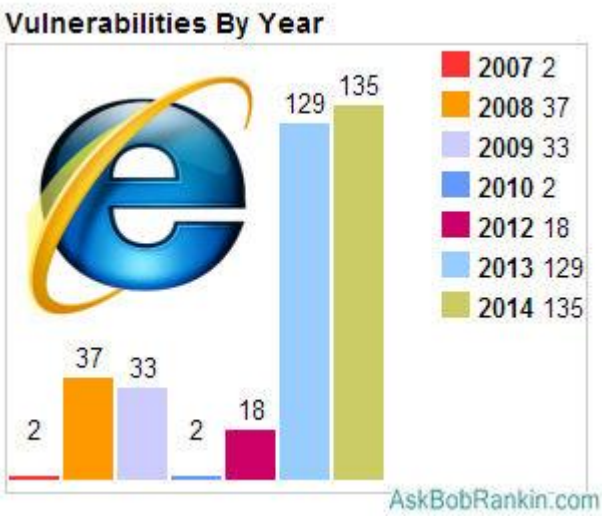
Category: Browsers From “askbobrankin.com”.

One website is reporting that a record number of security vulnerabilities were discovered in Internet Explorer during the first half of 2014, far more than in Google Chrome or Mozilla Firefox. Should alarms be sounded across the land? Should you tell Mom to switch browsers? Let's find out...

Is Internet Explorer Unsafe at Any Speed?

"We really recommend that you not use Internet Explorer," I overheard a librarian telling a patron in the local Public Library recently. Chrome and Firefox are available on every terminal available at all library branches. I wonder why they don't simply disable IE to make it disappear, but I understand why they discourage its use: the pundits that everyone heeds miss no opportunity to make IE look bad.

Most recently, Techworld trumpeted that a disturbing number of security vulnerabilities were discovered in Internet Explorer during the first half of 2014, far more than in any other popular program. That's according to an analysis of U.S. National Vulnerability Database (NVD) figures. Researchers found 133 NVD records of IE vulnerabilities so far in 2014, compared to 130 for all of 2013. By contrast, the competing browsers Chrome and Firefox each logged about 75 vulnerabilities during the first six months of 2014.



But wait; Chrome had 175 vulnerabilities discovered during 2013 while Firefox achieved 150. So over a full year, IE actually had the least vulnerabilities of the three major browsers! Confused yet? What Techworld didn't mention is that those numbers don't take into account the severity of the software bugs. Severity is measured on a scale of 0 - 10, with a higher score indicating a more serious problem. Digging a bit deeper, I found that the average severity for vulnerabilities discovered in 2014 tell a story that's a bit more illuminating:

Internet Explorer: Average severity 9.8, with 93% in the 9-10 (most severe) range

Firefox: Average severity 8.0, with 49% in the 9-10 (most severe) range

Chrome: Average severity 7.5, with under 3% in the 9-10 (most severe) range

Okay, Internet Explorer seems to look worst when it comes to both raw numbers of vulnerabilities discovered, and the seriousness of those vulnerabilities. But keep in mind that a vulnerability means only that a security researcher found a software bug that COULD POSSIBLY be exploited by hackers, crackers and other cybervillians.

Nobody Expects the Spanish Inquisition!

And of course, nobody expects that they'll fall prey to a security flaw in their favored browser. So how many of those vulnerabilities were actually exploited? Firefox and Chrome have had ZERO exploits since 2010. For IE, there were only 3 in the past year. That's not so bad, considering that these exploits require the user to be tricked into viewing a specially crafted web page in order to be affected. And in each case, Microsoft responded to the flaws with timely fixes.

Personally, I found the NVD website rather heavily laden with acronyms and jargon, hard to search, and nearly incomprehensible. I discovered that the NVD is fed by another site called CVE Details that lets you search, browse and drill down into security vulnerability data in a much friendlier format.

Microsoft released version 11 of IE last October. Like all new major versions of any software, it contains numerous bugs. The company issued its first security patch for IE 11 just five days after the update hit the Web, compared to more than 80 days lag time back in 2007 to 2011.

So no, IE is not the runaway winner of the Most Dangerous Software of All Time. A deeper look at the details of the software flaws discovered, their relative severities, the number of actual exploits, and the difficulty of carrying out an exploit, reveals that IE, Firefox and Chrome are all very safe vehicles on the information superhighway. The latter two automatically update themselves, and IE will do likewise if Windows Update is run with the default (automatic) settings. And as in the physical world, the driver is the cause of more accidents than the car.

You Want Danger? I'll Show You Danger...

A lot of techies give the Most Dangerous Software title to Java, which is found in more places than IE and has a horrible history of security vulnerabilities and exploits. (See my article, Time to Boycott Java? Apparently, a lot of people have been boycotting Java of late, encouraging bad guys to seek other victims.

In related news, Firefox 31.0 was released in July with a new anti-malware feature. The browser will now check the Google Safe Browsing reputations of individual files as they are downloaded,

as well as checking Web sites' reputations to warn users away from known phishing and malware sites.

Mozilla announced that Firefox 32.0, due in September, will add a new and more efficient file-checking feature. Before contacting the Google Safe Browsing database, Firefox will check a file for a valid digital signature that confirms the author is known and safe. Only if no signature is found will Firefox refer to the Google Safe Browsing database. If the user has added a software publisher to his/her local list of "known good guys," Firefox will skip these tests.

The bottom line is that vulnerabilities logged in the National Vulnerability Database are down this year overall. At least temporarily, the good guys seem to be winning. But the pendulum can swing at any time, so keep your local defenses and good computing sense on the alert.

Your thoughts on this topic are welcome. Post your comment or question below...

Read more:
http://askbobrankin.com/internet_explorer_the_least_secure_browser.html#ixzz38rrgfczL

Now a little health information,

Button batteries that won't burn babies' mouths and digestive tracts have been invented at MIT. A special coating allows the battery to conduct electricity when it is compressed between circuit contacts, but prevents current flow if the battery is swallowed. From "askbobrankin.com".

Lawyers believe that a man is innocent until proven broke.

~ Robin Hall

Till next month

Bob