How to protect yourself from ransomware attacks (Excerpts)

By Kelli Uhrich, Komando.com, May 17, 2017

On Friday, May 12, the largest ransomware attack ever recorded began breaking headlines. What started with one unwitting computer user in Europe soon spread to more than 200,000 machines worldwide - ultimately affecting Windows computers in over 150 countries, including South Korea, Germany, China, Japan and Britain.
This new strain of ransomware, called WannaCry or WanaCrypt0r 2.0, was unlike anything seen before. By convincing someone to open an email attachment with a compressed zip folder, hackers were able to unleash WannaCry to the world. And stopping it seemed nearly impossible. Were it not for a random kill switch discovered in the code, the results of WannaCry would have been even more devastating. In less than 24 hours, WannaCry was able to exploit a security loophole in Windows computers called "EternalBlue" that allowed it to scramble hard drives at banks, oil companies, hospitals, automakers and even high-profile companies such as FedEx. What allowed WannaCry to spread so quickly was that the code deployed a worm that crawled through the network and spread itself from one vulnerable computer to the next.

ANOTHER ATTACK IS COMING

Hearing about all the damage WannaCry successfully caused makes what we're about to tell you even more frightening: That is, researchers now believe the WannaCry ransomware attack was created by amateurs. Or, at least that it was launched accidentally, prior to perfecting the code.
A plethora of inexplicable errors have been baffling the cybersecurity community ever since the kill switch was found. In fact, the kill switch in itself, as well as broken code that complicated or restricted ransom payments, prove just how likely it is that WannaCry was not released by cybercriminal professionals.
All blunders aside, WannaCry successfully earned over $55,000 from those who payed the ransom. But the possibility of another attack now has everyone worried. New versions of WannaCry are already popping up, and if the right hacker were to improve the code, the next attack will be even stronger.

FIGHT BACK AGAINST RANSOMWARE

Although WannaCry primarily impacted large-scale corporations, it's important to point out that it started by infecting a single computer. When the next wave strikes, you don't want to be the one who falls victim. Whether you just own a few computers, or run a small business, you need to follow these steps to make ensure you're protected.

1. Install Microsoft's patch and system updates

Microsoft knew of the EternalBlue vulnerability months ago and sent a patch for it in a Security Update back in March. Since EternalBlue is the flaw being exploited by WannaCry ransomware, it is *CRITICAL* to make sure your Windows operating system is up to date. The specific update you're looking for is MS17-010. To get this patch, simply run a software update on your PC.

To update Windows 10 follow these steps:

1. On Windows 10, click Start (Windows logo).
2. Choose Settings.
3. Select Update & Security.
4. Then on the Windows Update section, click on Advanced Options. (Note: the "Windows Update" section is also handy for showing you updates that are currently being downloaded or applied.)
   Under Advanced Options, just make sure the drop down box is set to Automatic. (automatic is the only option in Home version)
   Note: Be sure to check the box to get updates to all of your Microsoft products

To update Windows 7 follow these steps:

1. Click the Start menu button.
2. Click All Programs.
3. Scroll through the list and click Windows Update. The Windows Update window will open.
4. Click Check for Updates.
5. Click Install Updates.

To update other versions of Windows:
Unfortunately, some older versions of Windows operating systems are no longer supported and cannot install this critical Security Update. But, the good news is, Microsoft released an emergency patch specifically for WannaCry since the virus is so wide-spreading. This means, if you are running Windows XP, Windows 8 or Windows Server 2003, you'll need a different patch. Go to this link to download the available Security Update for these older Windows versions. (http://www.catalog.update.microsoft.com/Search.aspx?q=KB4012598)

2. Install antivirus software and Backup your data
Typically, we'd recommend that you install a strong antivirus software on your computer. But, the truth is, in instances such as this, many antivirus programs fail to catch the virus.
It's still best if you have an antivirus installed, however, you also need to backup all of the data on each of your devices. This way, if ransomware hits, you're protected no matter what! Plus, with WannaCry ransomware, experts are saying even if you do pay the ransom there is very little chance you will get your data back which makes back up that much more important.
Note: When backing up to an external drive, it is best to disconnect it after backing up. Ransomware can encrypt all drives connected to a PC, even USB connected drives

---------- Added by Tom ----------
3. Create a system recovery drive (You will need a 16GB Flash (thumb) drive)
1. In Windows 10, click on Cortana and type “create a recovery drive”
2. Click on the Create a recovery drive (Control Panel)
3. Follow the instructions (Make sure “Backup system files to the recovery drive” is checked
4. This creates a bootable drive you can use to restore your PC to its original status.

You can also do this in Windows 8 and something similar in windows 7. Do a search for “create a recovery drive in windows X” where X is 7 or 8. The process for 8 is similar to 10. Windows 7 has a more complicated process.
---

4. Watch out for phishing scams
Scammers are constantly improving their techniques and coming up with new ways to trick innocent computer users. Phishing is commonly an email scam, but it can also happen through social media, text messages and regular old phone calls.

To spot these scams, you should follow these general tips:
- Be cautious with links - If you get an email or notification from a site that you find suspicious, don't click on its links. It's better to type the website's address directly into a browser than clicking on a link. Before you ever click on a link, hover over it with your mouse to see where it is going to take you. If the destination isn't what the link claims, do not click on it.
- Double check the URL spelling - When typing a URL into your browser, take the time to verify you're spelling it correctly. With typosquatting, misspelling a URL could lead to a phishing scam.
- Watch for typos - Phishing scams are infamous for having typos. If you receive an email or notification from a reputable company, it should not contain typos. Before clicking on a link, hover over it and check for spelling. The safest move is to type the URL into your browser, with the correct spelling of course.
- Use multi-level authentication - When available, you should be using multi-level authentication. This is when you have at least two forms of verification, such as a password and a security question before you log into any sensitive accounts.

What to do if already infected
If your device has already been infected with ransomware like WannaCry, the most important thing to do is disconnect it from the internet. This will prevent the virus from spreading to other machines on your network.
Once you've disconnected your computer, it's important that you do not pay the ransom! Giving in to the hacker's demands only rewards the behavior and keeps the scam going.If you've taken the steps mentioned above, you can wipe your gadget and restore it back to the factory settings. This should remove the malware installed on it; however, it will

also delete all your files. But, if you've backed up your devices, you can easily recover all of your files, photos and documents, and install them on your wiped (or new) device.
This is why we say backing up your gadgets is so important.

Excerpts from: **How to remove ransomware like WannaCry: Use this battle plan to fight back**
By Mark Hachman, Senior Editor, PCWorld | MAY 13, 2017

What to do if you're infected by ransomware

If you are infected, ransomware may allow you to see exactly which files it's holding hostage via File Explorer. One clue may be ordinary .DOC or .DOCX files with strange extensions attached. Ondrej Vlcek, the chief technical officer of Avast, offered an unintuitive piece of advice: If the ransomware isn't time-locked, and you don't need the files right away, consider leaving them alone. (Work on another PC, though.) It's possible that your antivirus solution may be able to unlock them later as it develops countermeasures.
Backup isn't foolproof, however. For one thing, you may need to research how to back up saved games and other files that don't fit neatly into "Documents" or "Photos." Ditto for utilities and other custom apps.

Don't panic. Your first move should be to contact the authorities, including the police and the FBI's Internet Crime Complaint Center. Then ascertain the scope of the problem, by going through your directories and determining which of your user files is infected. (If you do find your documents now have odd extension names, try changing them back—some ransomware uses "fake" encryption, merely changing the file names without actually encrypting them.)
The next step? Identification and removal. If you have a paid antimalware solution, scan your hard drive and try contacting your vendor's tech support and help forums. Another excellent resource is NoMoreRansom.com's Crypto-Sheriff, a collection of resources and ransomware uninstallers from Intel, Interpol, and Kaspersky Lab that can help you identify and begin eradicating the ransomware from your system with free removal tools.

The front page of NoMoreRansom.org's Crypto-Sheriff site includes an easy tool to discover what kind of ransomware may be affecting your PC.

If all else fails

Unfortunately, experts say that the key question—should we pay up, or risk losing everything?—is often answered by pulling out one's wallet. If you can't remove the ransomware, you'll be forced to consider how much your data is worth, and how quickly you need it. Datto's 2016 survey showed that 42 percent of those small businesses hit by ransomware paid up.

Keep in mind that there's a *person* on the other end of that piece of malware that's ruining your life. If there's a way to message the ransomware authors, experts recommend that you try it. Don't expect to be able to persuade them to unencrypt your files for free. But as crooked as they are, ransomware writers are businessmen, and you can always try asking for more time or negotiating a lower ransom. If nothing else, Grossman said there's no harm in asking for a so-called "proof of life"—what guarantee can the criminal offer that you'll actually get your data back? (Of the companies that Datto surveyed, about a quarter *didn't* get their data back.)
Remember, though, that the point of the prevention, duplication, and backup steps are to give you options. If you have pristine copies of your data saved elsewhere, all you may need to do is reset your PC, reinstall your apps, and restore your data from the backup.