FAQs about the WannaCry (or WannaCrypt) RansomWare Attack

As you may have learned over the weekend from national news coverage, a cyberattack using the ransomware known as **WannaCry** (or **WannaCrypt**) has impacted organizations and individuals on a worldwide scale. According to the latest reports, the attack was discovered on Friday, May 12 and quickly spread to at least 150 countries including the United States, United Kingdom, Russia, France and Japan.

What is WannaCry?

WannaCry is the name of a serious strain of ransomware that hit Windows PCs worldwide, starting last Friday and it had spread to an estimated 57,000 computers in more than 150 different countries around the world by the end of the day. European countries were hit the hardest, and business ground to a halt at several large companies and organizations, including banks, hospitals, and government agencies. Those who were infected found their computers locked, with hackers demanding a $300 ransom to unlock the device and its files.

What exactly does WannaCry do?

RansomWare like WannaCry works by encrypting most or even all of the files on a user's computer. Then, the software demands that a ransom be paid in order to have the files decrypted. In the case of WannaCry specifically, the software demands that the victim pays a ransom of $300 in bitcoins at the time of infection. If the user doesn't pay the ransom without three days, the amount doubles to $600. After seven days without payment, WannaCry will delete all of the encrypted files and all data will be lost.

FAQs about the WannaCry (or WannaCrypt) RansomWare

This is a screenshot from a computer infected with the WannaCry RansomWare:

FAQs about the WannaCry (or WannaCrypt) RansomWare

How were people infected?

Like many malware infections, it appears that human error is to blame. According to The Financial Times, someone in Europe downloaded a compressed zip file that was attached to an email, releasing WannaCry onto that person's PC. Many others did the same, and when all was said and done, at least 300,000 devices were affected globally.

That's unfortunate, but it's their problem, right?

Not exactly. Among the affected PCs were those used by the UK's National Health System (NHS). With computers locked, staff were unable to access patient records and other basic services. Appointments and surgeries were cancelled and medical facilities were shut down as NHS tried to stop the spread of WannaCry. Also affected: Germany's rail system, Renault and Nissan factories, FedEx, Spanish telecom Telefonica, and even Russia's central bank. These are examples of how devastating and dangerous this software can be.

During a Monday press briefing, Homeland Security Advisor Tom Bossert said WannaCry had not hit any US government systems.

Is the attack over?

Unfortunately, no, it is not.

What can I do if my computer is infected with WannaCry?

Sadly, there is no confirmed fix for WannaCry available at this time. Antivirus companies and cybersecurity experts are hard at work looking for ways to decrypt files on infected computers, but no means of third-party decryption are available right now. Hopefully affected users have backups of their data available, because the only other option right now that is known to work is to follow the instructions offered in the software to pay the ransom and even that will not guarantee the return of access to their files.

Is my PC at risk?

If you are running Windows 10 you are safe,
as WannaCry does not target Microsoft's newest OS.

FAQs about the WannaCry (or WannaCrypt) RansomWare

If you're running other, supported versions of Windows (Vista, Server 2008, Windows 7, Windows Server 2008 R2, Windows 8.1, Windows Server 2012, Windows Server 2012 R2, Windows Server 2016), a patch that Microsoft released in March addressed the vulnerability that WannaCry targets. So hopefully you or your office's IT department installed that update.

There are some people, however, who are still running aging versions of Windows; 7 percent still run Windows XP despite the fact that Redmond no longer issues security updates for it. So Microsoft took the unusual step of releasing a WannaCry patch for old versions of Windows it no longer supports, including Windows XP, Windows 8, and Windows Server 2003.

Regardless of which version of Windows you have, make sure you're up to date with your security patches!!!!

Ransomware isn't new; why is this such a big deal?

WannaCry uses an exploit known as EternalBlue developed by the US National Security Agency (NSA), which used it to go after targets of its own. Unfortunately, EternalBlue and other NSA hacking tools were leaked online last year by a group known as the Shadow Brokers, putting these powerful tools in the hands of anyone able to use them.

Is this still an issue?

Quite by accident, a UK researcher known as MalwareTech managed to hobble the spread of WannaCry over the weekend. He acquired a sample of the malware on Friday and ran it a virtual environment. He noticed it pinged an unregistered domain, so he registered it himself, as he often does in these types of situations. Lucky for him (and countless victims), WannaCry only locked PCs if it couldn't connect to the domain in question. Before MalwareTech registered the domain, it didn't exist, so WannaCry couldn't connect and systems were ransomed. With the domain set up, WannaCry connected and essentially died, protecting PCs.

FAQs about the WannaCry (or WannaCrypt) RansomWare

Great, so we're all good now, right?

Not so fast. Reports of new WannaCry variants are emerging, so stay alert and watch where you click.

What if my PC was ransomed?

While it appears that many people have paid the ransom demanded by the hackers, security experts warn against handing over your cash.

"As of this writing, the 3 bitcoin accounts associated with the WannaCry ransomware have accumulated more than $33,000 between them. Despite that, not a single case has been reported of anyone receiving their files back," Check Point warned in a Sunday blog post. "WannaCry doesn't seem to have a way of associating a payment to the person making it."

Bossert echoed that today, saying that **approximately $70,000 had been paid out since Friday, but there's no evidence of data recovery.**

If you've been hit, your best bet is to restore from backup; reputable security firms also have ransomware decryption tools. You can also use a tool like the FixMeStick; just insert the device, boot to its Linux-based environment, and let it take care of the problem. It won't restore files, but it will (hopefully) clean out the malware. When your PC is back up and running, make sure you have a robust antivirus program and the best ransomware protection.

How can we stop this from happening again?

Pay attention to emails with attachments or links!! Even if the message appears to be from someone you know, double-check the email address and be on the lookout for any odd wording or attachments you weren't expecting from that person. When in doubt, message the person separately to ask if they did indeed send you an email that requires you to download an attachment.

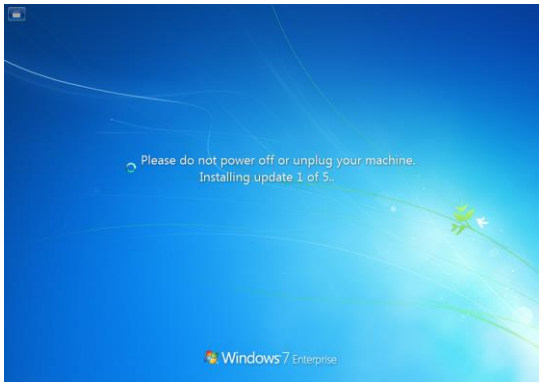
FAQs about the WannaCry (or WannaCrypt) RansomWare

Think before you click. Confirm the legitimacy of attachments, even if they come from a friend or known company. Take the extra few seconds to navigate directly to websites instead of clicking on a questionable link. And be suspicious of warnings or aggressive deadlines: Phishers will often try to push you into acting immediately, and may threaten consequences such as account suspension or additional fees if you don't respond right away.

Don't become a phishing victim.
Criminals frequently gain access to your computer by getting you to click on a link or an attachment within an email. Known as phishing, this technique can give criminals the opening they need to implant ransomware or other viruses.

Microsoft users: Update your system software!!
Microsoft released a patch in March, 2017 that addresses the WannaCry vulnerability. Making sure this patch is installed on your computer will help secure your systems from the threat. Again, Info Line's computers have the latest patches on the computers.

Here is a message from Microsoft concerning system updates:
While security updates are automatically applied in most computers, some users and enterprises may delay deployment of patches. Unfortunately, the ransomware, known as WannaCrypt appears to have affected computers that have not applied the patch for these vulnerabilities. While the attack is unfolding, we remind users to install MS17-010 update if they have not already done so. So, even though it is frustrating waiting for updates to load especially when they are still processing when you are ready to get to work, **please don't interfere with the process - the updates need to be completed to keep your PC safe!!**



FAQs about the WannaCry (or WannaCrypt) RansomWare

This is an excellent opportunity to back up your data on your computer to prevent possible loss from any occurrence, not just ransomware, whether you are at a home, work, or on a school computer. Use either a portable hard drive or any of the many cloud backup services that are currently available to back up your data automatically.

Again, **Think Before You Click!!** Confirm the legitimacy of attachments, even if they appear to come from a friend or known company. Take the extra few seconds to navigate directly to websites instead of clicking on a questionable link contained within an email. In reality, it is always a best practice to navigate directly to a website and ignore email links.

Lastly, be suspicious of ominous warnings and/or aggressive deadlines - Phishers will often try to use fear and intimidation to attempt to force you into acting immediately to provide your sensitive personal information and they may threaten serious and instant consequences such as account suspension or additional fees if you don't respond right away. These tactics should set off immediate red flags and alarms to you and should be ignored.

If you have any questions, please feel free to contact me at info@mc-akron.org.