About the ransomware WannaCrypt WannaCry WCry

Overview
A ransomware attack drew attention starting on Friday May 12. The malware is known by various names such as: WannaCrypt, WannaCry, WCry. The ransomware made the news because it quickly spread onto many computers, taking advantage of a vulnerability in Microsoft Windows that some computer owners did not patch.

The ransomware primarily spreads using a flaw in SMB (Windows filesharing). In March, Microsoft released a fix for the problem with SMB, so people who have run windows update since March should have good protection against the malware.

What does it do?
If the ransomware gets onto your computer, it encrypts files on your computer, making them unreadable. It then shows a message telling you to pay money to decrypt your files.

The current variant shows one price if you pay within 3 days, a higher price if you pay after 3, and threatens to delete the files if you do not pay after a week.

How can you protect your computer?
For best protection:
- **Keep current on operating system updates.** Run windows update, and when updates are available accept them promptly.
- **Have anti-virus on your computer.** In MIT’s case, we recommend both CrowdStrike Falcon and Sophos.
- **Have backups of your data.** At MIT, we recommend Code42. If your data is backed up, then you should be able to recover your data from backups if something causes you to lose your working data from your computer.

Specific protection vs WannaCry, checking to see if you are patched
Microsoft has put out patches for the SMB exploit that WannaCry uses. If you have accepted security patches from Windows Update since March, your computer will be safe.


Verifying that the update is applied to your computer is complicated, because Microsoft issues different “KB” patches for different operating systems. Below is a bit of PowerShell that takes 13 known hotfixes for this issue, gets a list of all hotfixes on the current computer, and checks to see if the installed hotfix IDs match one of the 13 fixes. It may require an administrative PowerShell prompt to run Get-Hotfix.

```
PS C:\WINDOWS\system32> $hotfixes = "KB4012598", "KB4018466", "KB4012217", "KB4015551", "KB4019216", "KB4012216", "KB4015550", "KB4019215", "KB4013429", "KB4019472", "KB4015217", "KB4015438", "KB4016635"
PS C:\WINDOWS\system32> Get-HotFix | Where-Object { $hotfixes -contains $_.HotFixID }
```


What should you do if your computer is infected with ransomware?
- **Disconnect the computer from the network.** Even if WannaCry has left your computer unusable, it is attempting to spread to other vulnerable computers on the network.
- **Find out if you can restore your data from backup.** If you can restore from backup, the ransomware is an inconvenience, but a manageable one.
You can contact MIT's IS&T Service Desk for help testing your backups. If you cannot restore from backup, you are in a difficult situation. We recommend NOT paying the ransom. Some ransomware is run very professionally, and swiftly unlocks your computer if you pay the ransom. It doesn’t feel right to reward the criminal for the crime, but people may do that if it is the only way to get data back. However, the current WannaCrypt variants are more amateur: reports say that ransom payments seem to require manual human verification, and can have long delays, and may not always work.

Assuming that you have verified that you have a working backup for your computer, you should

1. Save a copy of the encrypted data
2. Erase and re-install your computer
3. Take operating system updates, and install security software
4. Restore your data from the verified backup
5. Re-install your applications

The IS&T Service Desk can assist, if you want help.

The National Cybersecurity And Communications Integration Center has released a Fact Sheet on WannaCry=

**Additional reading**

- Talos blog (security group)
- Troy hunt blog (security researcher)
- Technical fact sheet

**Why all the names? Why can't people decide what to call this?**

The people who made the malware didn't tell us what it is named. Security researchers reading the malware code found interesting names in the code, and decided to name the malware based on these discovered names, such as: WannaCrypt, WannaCry, WCry.