BURR FORMAN LLP
results matter

# BURR ARTICLE

## WannaCry Ransomware - What You Need To Know

May 15, 2017

Starting on Friday, May 12th, computers in countries around the world have fallen victim to the latest ransomware attack. As of Monday morning, it is estimated that more than 150 countries have infected systems, totaling over 200,000 computers. The ransomware is known as WannaCry (or WannaCrypt), and as you might expect, it encrypts your computer and holds your files hostage, requiring you to pay a ransom to get your files back. The spread of this ransomware was enabled by a vulnerability in Windows, particularly for those running older versions of Windows. The patch for this vulnerability was made available earlier this year for currently supported versions of Windows, but Microsoft has now made patches available for older, unsupported versions of Windows.

Over the weekend, a British security researcher inadvertently managed to slow the spread of WannaCry, but experts do not believe the attack is over. In fact, there is evidence that new versions of the ransomware are now circulating that do not have the kill-switch activated by this researcher. If you have a Windows machine and have not yet been infected, you should immediately install the security update that Microsoft released on Friday.

The ransom demand for WannaCry stated that the ransom doubles 72 hours after the attack, and after seven days, files would be permanently locked. As of Monday morning, experts estimate the hackers have received roughly $50,000 in bitcoin ransom payments, which is minimal given the extent of the attack. At the same time, there are not yet any reports of victims recovering their files after paying the ransom.

Law enforcement and security experts around the world are currently recommending against paying the ransom, both because you are dealing with criminals and have no assurances of an honest transaction, but also because there is no evidence that the software includes a viable mechanism for decrypting files. In addition, unlike some ransomware attacks, it is not clear how or if the attackers are tying payments to a particular person or computer, which makes it less likely that paying the ransom will result in the release of your files. Private organizations around the world are currently working to develop a fix, but so far, there is no fix available from those efforts.

Even if you think you have escaped this attack, you should review your back-up procedures and your security measures and make sure everything is working as it should.

If you are one of those impacted, we are here to help. We can assist you with engaging the proper technical support, evaluating whether or not to pay the ransom, and protecting your organization from liability resulting from this attack. If you were not affected this time, but are concerned about protecting your organization in the event of future attacks, we will work with one of our trusted IT partners to help you establish and implement best practices for protecting your systems.

If you would like more information, please contact:

India Vincent in Birmingham at (205) 458-5284 or ivincent@burr.com
Josh Ehrenfeld in Nashville at (615) 724-3232 or jehrenfeld@burr.com
Ed Snow in Atlanta at (404) 685-4295 or esnow@burr.com
Ryan Corbett in Tampa at (813) 367-5740 or rcorbett@burr.com
or the Burr & Forman attorney with whom you regularly work.