the Availability Digest

www.availabilitydigest.com
@availabilitydig

WannaCry Ransomware Global Attack

June 2017

WannaCry is ransomware malware. If it infects your computer, it encrypts all your files and demands a ransom in order to get your files decrypted.

WannaCry began infecting computers on Friday, May 12, mainly in Europe. It then began expanding into China and Japan. Only a few systems in the U.S. were affected.

Fortunately, I escaped unaffected. I had updated my Windows operating system to Windows 10, a level that WannaCry could not infect. Furthermore, I backup my files in real time with an online service that would have allowed me to recover from a WannaCry infection.

What Is WannaCry?

When WannaCry infects a computer, it encrypts all the files stored in that computer. It then displays a message demanding a ransom payment in order to get the files released.

It asks for a payment of $300 in bitcoins. Bitcoins are a cryptocurrency that is not traceable.[1] If the ransom is not paid within three days, it is doubled to $600. If no ransom is paid within seven days, WannaCry threatens to delete all of the files. (However, no delete capability was found in the WannaCry code).

How Extensive Is It?

As of Monday, just four days after it first struck, WannaCry had locked over 300,000 computers in more than 150 countries. The most affected countries were Russia, Ukraine, India, and Taiwan. WannaCry supports over two dozen languages.

WannaCry reportedly caused disruptions at banks, hospitals, telecommunications services, train stations, and other mission-critical organizations in multiple countries, including the UK, Spain, Germany, and Turkey. FedEx, the UK government's National Health Service, and Spanish telecom Telefonica had all been hit.

According to Kaspersky Lab, 98% of the affected computers were running Windows 7. Windows 7 is still by far the most common version of Windows, with roughly four times as many computers running Windows 7 than are running Windows 10. Though Microsoft had issued a security patch for Windows 7 in March, 2017, that protected Windows 7 from WannaCry, many organizations had not yet installed it. Windows 10 was not vulnerable to the malware since Microsoft automatically applies updates to Windows 10 machines.

[1] Mt. Gox, Largest Bitcoin Exchange, Goes Belly Up, *Availability Digest*; March 2014.

© 2017 Sombers Associates, Inc., and W. H. Highleyman
www.availabilitydigest.com
For discussion, contact editor@availabilitydigest.com

How Did WannaCry Spread?

WannaCry was a network worm. It included a transport mechanism to automatically spread itself across corporate networks and the Internet.

WannaCry spread through a Windows 7 vulnerability named EternalBlue in the Microsoft SMB (Server Message Block) protocol. SMB is a file-sharing protocol. EternalBlue was discovered long ago by the U.S. NSA (National Security Agency), but the NSA chose to not disclose the vulnerability to Microsoft. Rather, it used the vulnerability to create an exploit for its own offensive work.

WannaCry did not use phishing emails or malicious websites to spread. Rather, it spread over networks by searching for systems with a vulnerable SMB protocol with the EternalBlue exploit. When it found such a system, it used the EternalBlue exploit to gain access and installed DoublePulsar, a backdoor implant tool. It used DoublePulsar to install and execute a copy of itself.

Microsoft to the Rescue

Microsoft learned of EternalBlue and issued a security patch to correct the vulnerability on March 14, 2017.

In April, a mysterious group calling themselves the 'Shadow Brokers' released the NSA exploit. The rapid outbreak of WannaCry infections in May attested to the fact that many companies had yet to install Microsoft's critical patch more than two months after it was released. Almost all the companies affected were running Windows 7.

How Successful Was It?

WannaCry demanded the payment be in untraceable Bitcoins. To facilitate this, it generated a unique Bitcoin wallet address for each infected computer so that it could trace who had made payments. However, these wallet addresses did not operate properly and were unusable by WannaCry.

As a consequence, WannaCry defaulted to three hard-codded Bitcoin addresses for payment, precluding their ability to determine the payers. However, the amount paid to the hackers could be determined from the Bitcoin block chain. Bitcoin addresses linked to the hackers showed a spike in payments to the hackers' account over the four day period from May 12th to May 15th. An analysis of the Bitcoin addresses indicated that fewer than 300 victims paid. The hackers netted about $101,000 from the ransomware attack.

The WannaCry Kill Switch

A security expert in England analyzed the WannaCry code and found a kill switch created by the hackers. The kill switch referenced a URL that, if successful, would shut down WannaCry. He created a website with this URL, and on May 15th the attack slowed. However, new versions quickly appeared that did not reference the kill switch.

How to Protect Yourself

Many users were protected from the ransomware attack by the Microsoft Windows 7 software patch that fixed the vulnerability. However, in China, many users were unable to take advantage of this fix because many Chinese run on pirated Microsoft operating systems.

WannaCry seems to have run its course. However, copycats abound; and there may well be further similar attacks by other hackers. Your best protection is to have current backups of all of your files. If a WannaCry look-alike should gain access to your computer and lock your files, you can wipe your

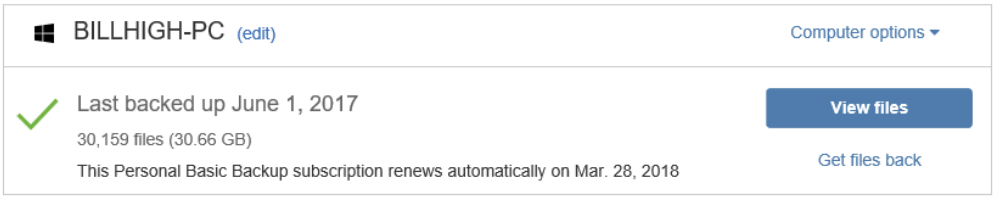
© 2017 Sombers Associates, Inc., and W. H. Highleyman
www.availabilitydigest.com
For discussion, contact editor@availabilitydigest.com

computer of these files and restore them from your backups. Be sure that your backups are saved on a hard drive that is not connected to your computer or are stored safely in a cloud.

How I Was Saved

Two actions saved me from the ravages of WannaCry. One was that I had switched to Windows 10 before WannaCry hit. So I was not even a candidate for the infection.

Even if I had been infected, I was safe. I use an online service that automatically backs up all of my active files as soon as they are changed. The service is Carbonite (www.carbonite.com), and it has saved me on many occasions when I have accidentally deleted or corrupted a file. Simply log on to Carbonite, search for the version of the file you have lost, and recover it.



Summary

WannaCry appears to have run its course. However, there is no assurance that it will not come back nor that other ransomware attacks will not occur. It is therefore imperative that you keep backup copies of all of your files so that you can restore them in the event of an attack. I highly recommend using an automatic online copying service such as Carbonite to perform this task for you. Other similar services include IDrive, CrashPlan, and OpenDrive.[2]

It is unknown who launched the attack. However, Symantic has identified the tools used by WannaCry as the same tools used by the Lazarus Group that carried out the 2014 attack on Sony after Sony released its film "The Interview" about an assassination attempt on the leader of North Korea, Kim Jong-un. The Lazarus Group is linked to North Korea.

Acknowledgements

Information for this article was taken from the following sources:

WannaCry Ransomware: What We Know Monday, *NPR*; May 15, 2017.
What you need to know about WannaCry Ransomware,*Symantic*; May 15, 2017.
WannaCry ransomware: Everything you need to know, *CNet*; May 19, 2017.
Almost all WannaCry victims were running Windows 7, *The Verge*; May 19, 2017.
WannaCry: Everything you still need to know because there were so many unanswered questions, *The infRegister*; May 20, 2017.
Inside the digital heist that terrorized the world – and only made $100K, *QZ*; May 21, 2107.
Windows 7 hardest hit by WannaCry worm, *BBC*; May 22, 2017.
WannaCry hackers still trying to revive attack says accidental hero, *The Guardian*; May 22, 2017.
Ransomware: WannaCry was basic, next time could be much worse, *ZDNet*; May 22, 2017.
WannaCry Ransomware; *Schneier on Security*; undated.
WannaCry ransomware attack, *Wikipedia*.

[2] The Best Online Backup Services of 2017, *PC Magazine*; May 5, 2017.

© 2017 Sombers Associates, Inc., and W. H. Highleyman
www.availabilitydigest.com
For discussion, contact editor@availabilitydigest.com