Wanna Cry

GBA-327-CA02

Dr. Regan

November 27, 2018

DeAndre King, Ashley Morris, Julian Taylor, Kalyah Walstad

Wanna Cry is a type of virus known as a crpytoworm and it is also on computers known as ransomware, which means that the virus will encrypt your files in your computer permanently unless you pay them in bitcoin. This started back in 2017 and it affected millions of Windows computers across the world. The reason it made worldwide news was that this ransomware attacked many high-profile computers around the world which included computers in the British National Health Services. The reason it was able to penetrate these British National Health Services computers were using a sixteen-year-old operating system and did not upgrade to a modern operating system. A major reason for not upgrading to a more modern operating system was that their MRI systems were designed to work with Windows XP, rather than a more updated version of Windows. This ransomware focused its attacks on Window's computers because it found an easy way into computers that the US National Security Agency discovered after these attacks began. These attacks were later found to be the product of a cybercrime organization called the Lazarus group, which could possibly be linked to the North Korean government. (Frulinger, 2018)

The Wanna Cry ransomware has different parts to it that make it very unique and hard to contain. When it first gets on a new computer it arrives as something called a dropper, which is a self-contain program that extracts other applications components which are embedded within itself. Inside of this includes an application that encrypts and decrypts data, files that contain encryption keys, and a copy of Tor. Tor is one of the largest known systems which allows you to be anonymous when contacting other people or computers. (Pascual, Shavitt, Uhlig, 2011) Once the virus gets into the computer it first tries to access a hard-coded URL, but if it cannot reach that then it starts looking for a variety of types of files such as Microsoft Office files and MP3 files which are on your computer. Once it is able to get in there the virus then demands for an

amount of bitcoin. One way to notice if your files have been hacked will be that the file extension will be changed to .WCRY and they will also use clickbait in file names to get you to pay them in order to get your files back. An example of a file name would be "! Please Read Me!.txt". (Symantec, 2017)

There are also many ways to prevent getting this ransomware virus in your computer. Microsoft released a patch back in March of 2017 which fixed all of the security flaws that were discovered by Wanna Cry. Microsoft now automatically updates its security system every time a new patch is made so that an issue like this is less likely to happen. If Windows had installed this patch when they originally received it two months prior to when the attack happened. (Cameron, 2017)

Here are some statistics about how vastly Wanna Cry hacked into computers globally. In a little over two weeks they had affected over 250,000 victims in 150 countries around the world. It is also considered one of the most aggressive and widespread attacks in all of history. The largest countries that were affected by this ransomware were the United States, the United Kingdom, Germany, Japan, Spain, France, Russia, and India. Over 176 different file types were encrypted during this attack on various types of computers. There were three different bitcoin addresses linked to the Wanna Cry ransomware that had balances of $50.14 thousand in bitcoin and they also asked for $133.3 thousand in currency from various computers that were attacked during their time. 46% of attacks on computers came from spam/phishing emails onto computers, 36% came from lack of employee training, 7% came from malicious websites/web advertisements, 1% came from a lack of security and 5% were from other various causes. Some of the types of security that this ransomware was able to get around to infect and hold hostage these files were anti-virus/anti-malware software (93%), email and spam filters (77%), patched

and updated apps (58%), ads and pop-up blockers (21%), and cyber-security training (14%). One reason people got hacked was because many people when they buy anti-virus software's they only want to pay for the software once and have that last for a lifetime. The problem with doing this is that if there needs to be an update you will not get the update unless you pay again for it, so some people would rather take the chance of getting hacked over buying more updates for the software.

The way that this ransomware was stopped was that a security researcher discovered an Achilles heel to the ransomware. He registered an obscure web address that was hard coded into the malware and due to this it was able to stop this malware infection from spreading more and more. After this, this only lasted for a few days, and by that time people had started creating new versions of the software that patched the original Achilles heel that the virus had had originally. The only way to really stop this virus is when users and IT professionals update their software on their computers to help eliminate the security flaws.

The Wanna Cry ransomware infected millions of Windows systems around numerous countries. The bad worm had also infiltrated many NHS systems across England halting their services as well. The Wikipedia entry for this attack contains more details on the affected organizations. Once a system was compromised by Wanna Cry and the data was encrypted, victims were asked to pay a fee of $300 in the form of bitcoins in a couple of days. If the ransom was not paid within seven days, the attacker threatened to delete the files altogether. The main thing that was reinforced by the speed, and success of the Wanna Cry ransomware attack is the importance of keeping systems up to date. If you're using outdated, vulnerable software, it is time to update it or replace it entirely. You should also uninstall or disable unnecessary services

and protocols if you really need to. Malware attacks often exploit these services and protocols as an attack vector.

The most important thing when it comes to ransomware is to back up your data no matter what. Always make sure you have a recent or current backup of your files on a system or in a cloud-based storage. However, you should never be forced to pay the ransom or risk losing your data. Even if your system is compromised by ransomware, you can just restore your backed-up data and resume normal operations. At the end of the day, the ransomware is an enemy and it will never be your friend.

References:

- Csoonline.com. (2018, August 30) What is WannaCry ransomware, how does it infect, and who was responsible?https://www.csoonline.com/article/3227906/ransomware/what-is-wannacry-ransomware-how-does-it-infect-and-who-was-responsible.html
- Symantec-Security. (2017, May 12). *Symantec Security Response*. Retrieved from https://www.symantec.com/security-center/writeup/2017-051310-3522-99#removal
-
- Domingo-Pascual, J., Shavitt, Y., & Uhlig, S. (2011). *Traffic Monitoring and Analysis Third International Workshop, TMA 2011, Vienna, Austria, April 27, 2011. Proceedings*. Berlin, Heidelberg: Springer Berlin Heidelberg.

- Gizmodo.com. (2017, May 13). *Today's Massive Ransomware Attack Was Mostly Preventable; Here's How To Avoid It* 9https://www.gizmodo.com.au/2017/05/todays-massive-ransomware-attack-was-mostly-preventable-heres-how-to-avoid-it/

- Bera, A. (2017, May 15). *MustTech News*. Retrieved from https://www.musttechnews.com/need-know-wanna-cry-virus/

- Hyden, M. E. (2017, May 15). *ABC News*. Retrieved from https://abcnews.go.com/US/timeline-wannacry-cyberattack/story?id=47416785