Logan Harris

MAT391 – Cryptology

**Research Assignment: WannaCry Ransomware**

As technology grows at an exponential rate, computerized systems become an increasingly essential component of our daily lives and the systems that power our global work force. New innovations provide a sense of confidence in our ability to assimilate to the challenges posed by the world around us, and they help make our lives easier at home and in the workplace. But with the advantages proposed by innovation comes dependence on the technology that is responsible for it, and a common fear is that the more humanity advances its technologies, the less individual information and capacity for knowledge we will possess overall. Today, we live in a modern time in which this fear is close to reality, and our dependence on computer systems to maintain the most vital functions of life means that the stability of the cyber-universe is largely reflective of the stability of our own world. Whereas previous attempts to disrupt peace came in the form of global acts of physical terrorism, those who seek to destabilize the world in modern times have begun to understand and take advantage of humanity’s dependence on technology. In the 21st century, we have entered a period of history in which terrorism – in addition to international wars/conflict as a whole – are fought on a digital battlefield. With less physical conflict and direct confrontation, we have been plunged into an “information war” in which national governments seek to combat their enemies by exploiting insecurities in their most important technological systems. This information war is largely fought by our country’s cryptanalysts and computer scientists employed by the National Security Agency, and with the proper amount of intel and tools at their disposal, NSA hackers can completely cripple an opposing nation’s government, military, and economy - indefinitely.

Due to the extremely volatile nature of world affairs politically, the cyber-security information war is an unending battle for supremacy. Every nation’s government is seeking new and better ways to expose the opposition, and even in times of relative peace we are actively trying out updated techniques and discovering new software exploits – this is where the controversy of interest arises. While the NSA is tasked with the defense of the cyber-security infrastructure of the U.S., they are of course also tasked with the opposition of foreign cyber-security entities. The issue is that, since more than 99% of the world’s computing devices utilize some form of the American-made Windows operating system, the same tools/techniques that are used to combat our enemies can be used against us. For many years, this double-edged sword was wielded by the NSA with great care, and to our general public knowledge there were no large-scale instances of computer systems being compromised in the U.S. It is important to note that there have been some minor attacks, but nothing of a magnitude that would require notifying the inhabitants of individual nations. This seemingly impeccable stability could not be maintained, and on May 12th, 2017, the largest worldwide cyberattack in recorded history affected more than 230,000 computers across more than 150 countries (Sherr) – and the NSA was mostly at fault.

The software behind the cyberattack – known as “WannaCry” – is a ransomware crypto-virus. A crypto-virus is a form of malware that is designed to use public-key cryptography to allow hackers to create a “one-way trapdoor” within a computer (Ernst & Young Global). The hacker does so by embedding a public key within a malware application, tricking the user to indirectly acquire this malware (the trap door), and then encrypting the victim user’s files by using a key pair of the public key and an additional private key that the attacker possesses. This is all done via operations that cannot be seen or undone by the victim user. The “ransomware” portion of the virus’ title simply means that the end goal of the malware is to collect on a financial ransom for illegal profit. Ransomware is commonly acquired via emails which trick the victim user into unknowingly corrupting their system by opening attachments that contain malware. This type of hacking strategy is also commonly used to secretly acquire user passwords or other important credentials, and the technique is known as “phishing.” (Graham)

In most cases, once a ransomware crypto-virus infects your computer, it uses system calls to access any and all files stored locally on the hard drive, encrypts them using a series of algorithms, and then prevents the victim user from undoing the encryption by utilizing the aforementioned one-way trapdoor methodology. This is exactly how WannaCry functioned, scrambling data on a local hard drive and only offering the decryption key after a ransom amount of $300 is paid. The first hours of the attack on May 12th showed that the initially-intended target was the United Kingdom’s National Health Service (NHS). More specifically, hospitals, emergency rooms, and other surgical facilities in England and Scotland were largely affected on the first day of the attack. Personal computers, medical instrumentation, and a myriad of other devices were affected by the WannaCry crypto-virus. Possibly the most important system that was affected by the virus was the telephone system, which completely disabled communication between hospitals and EMT dispatch units. This resulted in hospital staff members attempting to communicate via their own mobile phones and being forced to revert to traditional pen and paper documentation (Graham).

|  |
| --- |
|  |

**Figure 1: Message prompt provided by WannaCry cryptovirus**

Due to the chaotic situation, loss of access to medical instrumentation, and lack of organization during the emergency, many hospitals across the UK were forced to reject patients and cancel surgical appointments. Additional, civilians in the affected regions were told to only seek medical care in the case of an emergency. Needless to say, this held devastating consequences for the victims of the attack, and the NHS was aware that time was crucial factor in saving the lives of the individuals in need. Time was also an important factor due to the fact that the WannaCry crypto-virus increased the required ransom payment from $300 to $600 after three days, and also ensured its victims that their encrypted files would be permanently deleted after seven days. This is displayed in figure 1, which contains an image of the message prompt that appears to victim users affected by the WannaCry virus. An important note is that the only type of payment accepted by the WannaCry attackers is via the Bitcoin cryptocurrency. The crypto-infrastructure that the Bitcoin is built upon allows for a completely anonymous and encrypted currency transfer, meaning that this gave the attackers an easy way to hold out for ransom without any traceability.

Outside of the UK, other regions of the world that that were affected by WannaCry were Russia’s Interior Ministry, Spain telecommunications company Telefonica, Germany’s Deutsche Bahn railway, as well as Taiwan, Ukraine, and India. In a curious occurrence, FedEx Corporation was another major victim despite reports that the majority of American companies/services were unaffected by the attacks. (Graham) Additionally, sneaking suspicions that an Asian country was likely at fault for the crypto-virus were quelled as the Chinese media reported that more than 29,000 institutions across the country were infected with the WannaCry virus, and similar results were reported in Japan. For all intents and purposes there was no definitive location source for the attack, and certainly no leads on the identity of the specific parties involved with the development of the virus. So who exactly was responsible, and how did they create such an effective virus? The answer to that question was found on American soil.

Computer security companies including Avast, Proofpoint and Symantec all reported that WannaCry most likely spread via an exploit used by a collection of hackers known as the “Equation Group”– a group that has almost been proven without a shadow of a doubt to be tied to the NSA. Multinational cyber-security entity Kaspersky Labs’ expert analysts discovered that there are very keen similarities between the backend code utilized by the Equation Group and the NSA, such as the code words “STRAITACID” and “STRAITSHOOTER” (Woollaston). In addition, the timestamps embedded in malware associated with the Equation Group all suggest that the main labor hours put into the code fall between 9:00AM-5:00PM EST, which can obviously be found to correlate with the length of a normal work day on the East Coast in America. Based on Kaspersky analysts’ findings, the Equation Group is basically just a secretive extension of the NSA that is used to reduce liability in undesirable situations (such as the exact scenario that played out across the events of the WannaCry attack). Regardless of any doubt regarding direct affiliations between the Equation Group and the NSA, agents in the Equation Group are believed to all be American, and have developed malware/exploits that would not be possible without tools provided to them by the U.S. government.

The lifecycle of the WannaCry virus began when the Equation Group discovered a vulnerability in the Microsoft Windows operating system (OS) that allowed for unpermitted access to critical system areas. The vulnerability, entitled “MS17-010,” was used by the Equation Group to develop a piece of exploitation software called “Eternal Blue.” (Woollaston)This exploit was designed with intentions of being used to gain access to systems utilized by terrorist organizations and opposing nations. Although these were good intentions, any knowledge of the existence of an exploit in the world’s most commonly used OS necessitates that the developer of the OS be notified so that a patch can be made to fix the issue. This is due to the fact that there can be viral outbreaks of malicious viruses when government organizations begin stockpiling vulnerabilities without letting software developers know – the prime example being the WannaCry attacks. This is when the fault begins to shift towards the Equation Group and the NSA, who stockpiled the exploit and did not release any information to Microsoft or the general public that their systems could be compromised. This act of negligence was the catalyst for the creation of the WannaCry virus, as a secretive third-party organization known as the “Shadow Brokers” gained access to the Eternal Blue exploit.

The Shadow Brokers are an anonymous grouping of hackers who steal appealing hacking tools and data to be sold for profit in the cyber-security information war. Instead of using their skills to hold computer files for ransom, they instead hold onto national secrets and hacking techniques and sell them to the highest bidder. The bidder who pays the Shadow Brokers could range from a national government entity, a terrorist group, or some other private hacking group. In the 1-year period of time between the Shadow Brokers’ origin in 2016 and the month before the WannaCry attack in May of 2017, the group leaked a little over one gigabyte of software exploits that they reported were stolen from the NSA. This culminated in the acquisition and leak of Eternal Blue on April 14th, 2017, which gave an unknown multitude of criminal groups access to the exploit. Following this leak, experts believe that the developers of WannaCry first tested the vulnerability by gaining remote access to victim users’ computers, and then used the information collected by this test run in order to develop the full virus.

Cyber-security experts from Symantec and Kaspersky Labs found traces of code in some of the initial versions of WannaCry that also appeared in similar malware utilized by the Lazarus Group, another hacking group that has been largely tied with North Korea. Cyber-security entities in the U.S. were first exposed to the Lazarus Group during a cyberattack on Sony Pictures in 2014. (Graham) This attack was the result of the impending release of the controversial American film “The Interview,” that contained a depiction of the horrors of living in North Korea as well as dialogue with Kim Jong Un, and even goes as far as to showing him die in a fiery explosion as he is shot out of a helicopter by an American tank. For obvious reasons, the North Korean government did not want the citizens of North Korea exposed to this type of content, and the Lazarus Group was deployed as a preventative measure – one that the North Korea would deny its association with, of course. Similarly, North Korea denies any ties to the WannaCry outbreak and the Eternal Blue exploit auction conducted by the Shadow Brokers.

Prior to the WannaCry attack, Microsoft Corporation had implemented a series of OS updates, including an update that remedied the vulnerabilities exposed by Eternal Blue. The issue was that these security updates are often ignored or neglected by companies/services that utilize the Windows OS, and the updates also only apply to more recent versions of the OS. Following the WannaCry attack, Microsoft was forced to take immediate action in order to develop a fix for all systems affected by the virus. In order to do so, Microsoft developers did something that normally does not happen and issued a fix for versions of past versions of Windows that were considered to be deprecated, such as Windows XP. (Woollaston) This was extremely important, as Windows XP is a classic OS that is still widely used on many computers, most importantly of which being those used by health services and corporate entities around the world. Representatives from Microsoft also exposed the negligence exhibited by the NSA and other U.S. government agencies who attempt to hold on to secrets that compromise our national security.

Microsoft's president and CLO Brad Smith stated that the WannaCry attack "…provides yet another example of why the stockpiling of vulnerabilities by governments is such a problem." He went on to express the remainder of his concerns with a hint of anger/frustration, stating "We have seen vulnerabilities stored by the CIA show up on WikiLeaks, and now this vulnerability stolen from the NSA has affected customers around the world. Repeatedly, exploits in the hands of governments have leaked into the public domain and caused widespread damage. This most recent attack represents a completely unintended but disconcerting link between the two most serious forms of cybersecurity threats in the world today – nation-state action and organized criminal action." (Woollaston on Smith)

Other efforts to eliminate the spread of the WannaCry virus included those made by Marcus Hutchins, a younger cybersecurity researcher who accidentally stumbled upon a work-around that stopped the virus in its tracks. While analyzing the WannaCry code following the initial attack, Marcus discovered that there was a section of the backend code that displayed a URL address. He went on to discover that the executable malware code within the WannaCry virus seemed to periodically check this URL, and only continued its work if the URL was not a live, registered web address. After making this discovery, Marcus proceeded to register the web domain that was exposed in his findings and, much to his surprise, major cybersecurity firms around the world reported that the spread of the attack was ceasing.

This “kill switch” that Marcus found created a major roadblock for the WannaCry hackers, as they would need to revisit the code they developed in order to produce an updated version of the virus that would not be affected by Marcus’ discovery. "Thankfully some researchers are already registering the new domains as they identify them," Chris Doman, researcher at AlienVault says. "The cat-and-mouse will likely continue until [someone] makes a larger change to the malware, removing the kill-switch functionality completely. At that point, it will be harder to stop new variants" (Chappell). Analysts believe that the kill-switch was placed within the WannaCry virus by its developers so that they would have a way to manually stop it if they chose to do so. Experts also agree that the total damages that resulted from the WannaCry attack were greatly minimized by Marcus’ findings. Overall, despite the initial chaos and fear displayed by the victims of the WannaCry attack, the recovery effort was expedited by the combined intelligence of many cooperating cyber-security entities, and the economic loss associated with the attack is estimated to be about $4 billion (Ernst & Global), which is a relatively small amount of money based on the number of computing devices affected.

Despite the quick recovery time and the minimal cost associated with the attack, the WannaCry crypto-virus serves as a very intense wake-up call for security agencies, individual citizens, and the political bodies that govern them. It was one of the first large-scale accounts of a cyber-security attack resulting from a publicly-leaked vulnerability, and led to a great amount of change in how software development companies secure their applications around the world. Although the WannaCry attack is not the first time that the NSA and the U.S. Government have withheld information from its citizens, it is certainly the most pertinent occurrence regarding today’s expansive realm of technology. As we proceed towards a future that involves the continuous increase in our dependence on technology, we must always strive towards the complete and total security of the computer systems that we rely on.

**Works Cited**

Chappell, Bill. “WannaCry Ransomware: What We Know Monday.” NPR, NPR, 15 May 2017, www.npr.org/sections/thetwo-way/2017/05/15/528451534/wannacry-ransomware- what-we-know-monday.

Graham, Chris. “NHS Cyber Attack: Everything You Need to Know about 'Biggest Ransomware' Offensive in History.” The Telegraph, Telegraph Media Group, 13 May 2017, www.telegraph.co.uk/news/2017/05/13/nhs-cyber-attack-everything-need-know- biggest-ransomware-offensive/.

Sherr, Ian. “WannaCry Ransomware: Everything You Need to Know.” CNET, 19 May 2017, www.cnet.com/news/wannacry-wannacrypt-uiwix-ransomware-everything-you-need- to-know/.

“‘WannaCry’ Ransomware Attack.” Ernst & Young Global Ltd., 2017.

Woollaston, Victoria. “WannaCry Ransomware: What Is It and How to Protect Yourself.” WIRED, WIRED UK, 28 June 2017, www.wired.co.uk/article/wannacry-ransomware-virus-patch.