Research Note no. 26
August, 2017

CREOGN Research Note

WannaCry and the Diffusion of Zero Day Exploits.

Gendarmerie Nationale Officers College Research Center

What happened?

On Friday May 12th 2017, WannaCry began affecting computers worldwide. The infection started in Asia in the early morning and spread worldwide. Within a day, over 200,000 computers were reported to have been infected[1]. Sixteen British hospitals were unable to access their systems. Companies such as Renault, Deutsche Bahn and Telephonica were also affected. By May 14th, more than 150 countries had been hit.

The origin of the incident can be traced to the National Security Agency (NSA). The US agency tasked with signal intelligence had developed a tool, called EternalBlue, to take the advantage of a vulnerability in older versions of Microsoft's operating system which are no longer supported by the company but are still commonly used. For example, Windows XP, released in 2001, still runs on more than 5% of Windows computers. In essence, EternalBlue allows machines to receive files over network ports that are supposed to be blocked. This software can disable machines, collect intelligence and achieve multiple other objectives, exploiting undisclosed vulnerabilities collectively known as "zero day exploits".

Naturally, the tools were to remain confidential. However the NSA has experienced multiple leaks over the past few years. In 2016, the Federal Bureau of Investigation (FBI) arrested Harold Martin, a Booz Allen Hamilton employee who worked as a sub-contractor for the NSA, and charged him for the illegal possession of terabytes of data and computer code in his garage. In April 2017, the Shadow Brokers, a group with alleged links to Russian intelligence, put NSA tools online where anyone with a modicum of technical expertise could use it for their own purposes. In response, Microsoft developed a patch to plug the hole but this has been inconsistently applied by users. For example, some illegally obtained software is not able to download the update.

Other software such as Wannacry and Adylbuzz were then developed to take advantage of EternalBlue. WannaCry is a ransomware, a type of malicious software that blocks access to the victim's data until a ransom is paid, often in crypto-currencies such as bitcoins. On May 12, 2017, when WannaCry started affecting computers in Asia early in the morning, victims were asked to pay $300 within three days to recover data (the price increased to $600 afterwards). The malware then spread throughout the world. However, within a few hours, a British independent expert identified a critical weakness in the program : WannaCry had systematically tried to access a particular URL (that was hard coded in the malware) and disabled itself if it could not access it. This may have been designed as a security feature to prevent an examination of the software in sterile environments known as "sandboxes", where accessing the URL would have been impossible. By

[1] However, the estimation appears to have been reached by examining the number of machines that accessed a URL hard coded in WannaCry. This approach may have exaggerated the number of machines that were meaningfully affected.

not being able to access the URL, the software would have detected a sandbox environment and shut itself down to prevent examination. However, this led to a weakness in the malware. When the analyst bought the URL (for $11), he was able to considerably slow down the worldwide propagation of WannaCry. On March 14th, Microsoft released an emergency security patch that protected users of the XP version. By May 15th, the outbreak was essentially contained. By May 18th, three French researchers had identified a way to decrypt files infected by WannaCry in certain cases.

During the WannaCry episode, a separate program dubbed Adylkuzz was actively exploiting the EternalBlue vulnerability. The purpose of this second malware was different from WannaCry. Crypto currencies such as Bitcoin or Ether are digital assets that are created by decentralized communities through the implementation of algorithms on individual computers. This process (known as "mining") requires computer time and electricity, and as such is costly. Adylkuzz focused on the mining of Monero, a crypto-currency with enhanced privacy features whose market capitalization has been steadily increasing since 2014. However, Adylkuzz made sure that the benefits of the mining were captured by the hackers. Ironically, one of the features of Adylkuzz was to plug the vulnerability exploited by EternalBlue. In other words, Adylkuzz completely protected machines it infected from WannaCry.

What were some of the consequences of WannaCry?

WannaCry was the biggest ransomware attack in history. Its coverage was massive with estimates of computers in more than 150 countries were being infected within just 72 hours. Russia, Ukraine, and generally-speaking, countries from the Commonwealth of Independent States, were particularly affected. Computers in the interior ministries of Russia and China were infected. However, authorities had advised the public not to pay the ransom and the advice was largely followed. The bitcoin accounts set up by the hackers received slightly more than $100,000 and this amount has not been retrieved so far. If the motivation was financial, WannaCry was a failure.

Broader costs are difficult to estimate. No effect on critical infrastructure and no major lasting effects were reported. For example, British hospitals retrieved backed-up data and quickly resumed operations. Despite the breadth of the attack, its effects appear to be relatively immaterial for the worldwide economy and even the most affected countries.

In reaction to WannaCry and its exploitation of NSA assets, American lawmakers decided to review the policy regarding disclosure of "zero day exploits". The decision to publicly release a known vulnerability is currently based on an administrative framework known as the Vulnerability Equities Process (VEP), an approach based on a cost-benefit analysis. While keeping exploits secret provides a clear advantage to intelligence or even law enforcement agencies, maintaining confidentiality makes the cyber-ecosystem more vulnerable to criminals who are able to independently identify the vulnerabilities. These two considerations are traded off to decide if and when a known vulnerability is disclosed to software developers. On May 17th, just five days after the initial emergence of WannaCry, American lawmakers introduced the Patch Act to formalize the process and to have exploits reviewed by an independent board. If passed, the Patch Act would create a legal framework as opposed to an administrative one.

Who was behind WannaCry?

Attribution remains speculative at this point and is largely based on circumstantial evidence. WannaCry has two components, the network infection vector (the part that installs the malware in the computer) and the crypto-locker (the part that encrypts the files). The first component can be directly traced to the NSA leak. Various actors have noted similarities in the second part with codes that have been used by a group dubbed Lazarus. This group has been linked to North Korean intelligence and has received attribution for previous cyber-incidents. For example, Lazarus has been accused of executing different Distributed Denial of Service (DDoS) attacks targeting South Korean organizations as early as 2009. A DDoS attack is an attempt to make an online service unavailable by overwhelming it with traffic from multiple sources. The group has been accused of orchestrating the hack of Sony Pictures in 2014 that resulted in the leak of a large volume of confidential information and unreleased movies. In 2016, Lazarus was accused of orchestrating cyber-attacks on three financial institutions. In particular, a sophisticated and integrated attack on the central bank of Bangladesh nearly led to the theft of one billion dollars (payments were stopped after the first 80 million dollars disappeared).

However, in contrast to these events that have evidenced an increasing degree of sophistication in coding, intelligence and financial acumen, WannaCry was poorly executed with numerous programming errors that slowed down the progress of the attack and made payments difficult. This has led some commentators to suggest that the ultimate goal of the attack was to embarrass the NSA rather than to collect money. Another possibility is that individuals associated with Lazarus executed the attack without the full support of the organization. Linguistic analysis suggests that the ransom notes were written by individuals speaking a form of Southern Chinese (not Korean) but Macao has been rumored to be a base of operations for North Korean intelligence[2].

What can we learn from WannaCry?

WannaCry will probably not lead to many technical insights. The malware did not introduce any coding innovations and the threat of ransomware is nothing new. EternalBlue has also been used as a penetration vector by other malware although they have been more focused than WannaCry. However, we can make two observations.

First, affected machines were running older versions of the Windows operating system that are no longer supported by Microsoft. For example, British hospitals were identified as the most high profile victims of WannaCry. Indeed, media have reported that a study conducted by cyber-security firm Citrix found that 90% of British NHS hospitals were still running XP in 2016[3]. It may be tempting to attribute this reliance on outdated technology to incompetence and inadequate funding. However, it is important to realize that numerous medical devices run specialized software that may not easily migrate to more recent operating systems. This legacy issue is likely to increase with the development of connected objects that are part of complex systems. Many of the devices will not be designed with robust security features and will become unsupported by their manufacturer after a few years of service. Quickly identifying faulty system components

[2] https://www.flashpoint-intel.com/blog/linguistic-analysis-wannacry-ransomware/

[3] http://www.zdnet.com/article/windows-xp-why-hospitals-are-still-using-microsofts-antique-operating-system/

and patching vulnerabilities in real time without degrading their interoperability with other components is likely to be increasingly important but challenging.

Second, WannaCry made world headlines. News media ran titles such as “the Wannacry ransomware catastrophe, explained” or “How Soon Until the Next Ransomware Catastrophe?”. Actual damages were more limited than these headlines suggest. Stock prices of companies selling sophisticated cyber-security products increased significantly when technical solutions (e.g., patching, data backup) were relatively easy to implement[4]. The perceived impact of the incident was probably greater than it real effect. Cyber-security issues are often difficult to explain and can be a source of anxiety to the public. Firms selling cyber-security solutions naturally exacerbate this tendency by sending alarming messages after attention-grabbing cyber-incidents. This anxiety may be directly exploited in the future. Large nation states have the capability to inflict severe damage on critical foreign infrastructures, however, such attacks are likely to be met with similarly effective counter-strikes. In contrast, it would be difficult for democratic states to respond to a cyber-campaign that inflicts minimal physical but large symbolic damage, particularly if the attack is waged under a false signature. Examples include large scale attacks on media operations or on electronic billboards in transportation hubs coupled with limited attacks on high profile objectives (for example, targeting a small number of industrial control systems in chemical factories). In scenarios such as this one, the impact of rare but serious cases is likely to be amplified by benign but high profile ones. Foreign nations may estimate that such attacks remain under the threshold for escalation in spite of their significant political implications. In this context, effective communication from authorities is crucial to preventing irrational reactions from the public and to minimizing the psychological consequences of cyber-attacks.

[4] http://www.cnbc.com/2017/05/15/cybersecurity-stocks-surge-on-fears-wannacry-cyberattack-isnt-over.html

Author: Gilles Hilary,
Chaired Professor, Houston Term Professor,
Department of Accounting and Control, Georgetown University,
chercheur associé du Centre de recherche

de l’École des officiers de la gendarmerie nationale