Cyro Kamogawa

Professor Johnson

COMP 465W

14 November 2017

The WannaCry Virus and Ethical Software Engineering

The National Security Agency (NSA) regularly traces malware servers and retrieves data from them in order to identify potential threats[[1]](#footnote-1),[[2]](#footnote-2). In 2013, a previously little-known hacking group, known as the Shadow Brokers, hacked an NSA staging server and stole information regarding malware that the NSA had collected. The Shadow Brokers then, for reasons unknown, waited until the summer of 2016 to start leaking this information online, often trying to auction it off to tech companies or governments. Possibly in response to this, Microsoft issued an update in March of 2017 to their supported Windows operating systems to protect against ransomware[[3]](#footnote-3), a particularly nasty form of malware that holds user data hostage until a ransom is paid. After failing to auction off a particular set of Windows exploits, the Shadow Brokers dumped it online in April. These leaked exploits led to one of the most catastrophic cyber attacks in recent history: the WannaCry virus[[4]](#footnote-4). WannaCry was ransomware that spread less than one month after the Shadow Brokers released data about the Windows security holes. The attack held over 200,000 computers ransom across the globe, affecting hospitals, air traffic controls, and other major businesses[[5]](#footnote-5). The developers of WannaCry were never definitively identified, but security experts noticed striking similarities between the ransomware’s code and previously developed attacks by cyber-terrorists known as the Lazarus Group, who have ties to North Korea[[6]](#footnote-6). As we will see, all of the groups involved share some of the blame for this severely unethical use of software engineering and could have done more to prevent it.

First, the NSA stockpiles information about security holes in major networks, which could greatly help protect against cybersecurity threats, if they act on their discoveries. In this way, the NSA contributes to the good life of American citizens and minimizes harm and suffering. However, the agency usually does not report the risks that they identify in order to collect more data -- a practice that has earned them a great deal of ridicule[[7]](#footnote-7). In the case of the discovered Windows exploits, the NSA failed to warn Microsoft about their security holes and allowed their own research to be used against the public. By failing to prioritize the potential harm over research purposes, the agency has ethically failed in the realms of honesty and responsibility in software engineering. Whether or not the NSA is ethically obliged to report all of the risks they identify – I am not sure. The reward from the additional information gained from their secretive research could potentially outweigh the risks, in some cases. In the WannaCry case, however, the NSA’s silence has damaged not only the infected devices and their users, but also the agency’s relationship with top tech companies, like Microsoft, and their trust with the American people -- again.

Although they are largely victims in this attack, Microsoft is also guilty of bringing harm to the infected computers. Microsoft first failed to develop a fully secure Windows platform -- a task that is near-impossible to accomplish completely, but nonetheless, the blame for the security holes cannot fall on anyone else. Additionally, the tech giant failed to notice its own security risks until March of 2016, while the NSA had caught them by fall of 2013, at the latest. These software development mistakes are the unfortunate result of laziness on Microsoft’s part. Although Microsoft’s employees cannot be expected to constantly work tirelessly on security, recent events have shown that the corporation may not be doing enough. The company’s users, on the other hand, are definitely not doing enough to protect themselves. Reports showed that many of the infected computers were still running Windows XP -- an operating system that Microsoft no longer supports. It is the responsibility of computer users and company IT departments to keep their devices updated, not only to protect themselves, but to protect everyone else on the network too. After the attack, Microsoft showcased ethical practice by issuing a rare update to protect the unsupported Windows XP users from future ransomware attacks[[8]](#footnote-8).

Finally, the two or more criminal parties behind the WannaCry virus clearly deserve a share of the blame for the damage. The Shadow Brokers deliberately performed unethical acts when they hacked the NSA and released the information online. The hackers knew that the NSA was in possession of extremely sensitive data, and that the leaking of this data could bring great harm to the public. Nonetheless, the Shadow Brokers valued the money to be made from online auctions and the fame to be earned from hacking the NSA over the safety of computer users worldwide. The Shadow Brokers’ hack has damaged the public by costing many individuals hundreds of dollars or their precious data, temporarily shutting down critical systems, and tarnishing the public’s confidence in both the NSA to keep the nation safe and in Microsoft to develop secure software. The fact that all of this was done intentionally highlights the group’s terrible moral standards and the need for robust security. Similarly, the WannaCry developers themselves fully intended to profit off of the suffering of others. The creation and spread of malware is an extremely unethical act for software engineers as it completely disregards the concerns of others and prioritizes the self. Although the authors merely used the information that was made publicly available by the Shadow Brokers, and the software may have been developed by someone else eventually, the authors’ actions represent a monumental ethical failure. They have brought harm and embarrassment to all other parties involved, and in order to encourage ethical software engineering practices, the developers should be caught and punished.

The WannaCry virus caused significant damage during its short lifespan, and brought the dangers of software engineering ethical failures to the public’s attention. These failures, intentional or not, can have severe impacts that give the practice of software engineering a bad reputation. Software engineers must consistently be attentive, secure, and moral in their development practices in order to prevent attacks like the WannaCry virus. Individual developers and major corporations alike must be sure that their engineering practices are not tainted with unethical practices, and always prioritize the safety and well-being of their users.

1. Snowden, Edward: Twitter. <https://twitter.com/Snowden/status/765514477341143040> 16 August 2016 [↑](#footnote-ref-1)
2. Schneier, Bruce: “Computer Network Exploitation vs Computer Network Attack”. Schneier on Security. 10 March 2014 [↑](#footnote-ref-2)
3. Schneier, Bruce: “Who Are The Shadow Brokers?”. The Atlantic. 23 May 2017 [↑](#footnote-ref-3)
4. # Price, Rob: “The hackers that leaked NSA cyber-weapons say they will dump more data on a monthly basis” Business Insider. 17 May 2017

   [↑](#footnote-ref-4)
5. op. cit.: “Who Are The Shadow Brokers?” [↑](#footnote-ref-5)
6. Pearce, Matt: “Their code was used to hack Sony and create ‘WannaCry.’ Meet the ‘Lazarus Group,’ the armed robbers of the Internet”. LA Times. 18 May 2017 [↑](#footnote-ref-6)
7. Smith, Brad: “The need for urgent collective action to keep people safe online: Lessons from last week’s cyberattack”. Microsoft. 14 May 2017 [↑](#footnote-ref-7)
8. Sherr, Ian: “WannaCry ransomware: Everything you need to know”. CNET. 19 May 2017 [↑](#footnote-ref-8)