(Wolf & Fresco, 2016)

Ethical Issues Stemming from the Stockpiling of Zero-Day Vulnerabilities

An STS Research Paper submitted to the Department of Engineering and Society

Presented to the Faculty of the School of Engineering and Applied Science
University of Virginia • Charlottesville, Virginia

In Partial Fulfillment of the Requirements for the Degree
Bachelor of Science, School of Engineering

Derek Johnson

Fall Semester 2021

On my honor as a University Student, I have neither given nor received unauthorized aid on this assignment as defined by the Honor Guidelines for Thesis-Related Assignments

Student
_____________Derek Johnson________________Date_11/8/2021__

Advisor
_______________________________________Date 12/9/21
Richard D. Jacques, Ph.D., Department of Engineering and Society

Introduction:

Software bugs have plagued computer systems since the advent of programming. Most of these bugs are harmless byproducts of software development but when a they allow a third party to use software in an unintended manner, they becomes a vulnerability. In the art of war Sun Tzu says "If you know the enemy and know yourself, you need not fear the result of a hundred battles". It follows that the most dangerous vulnerabilities would be the ones software vendors do not know they have. These are known as zero-day vulnerabilities, their name derived from the fact that the software vendor has known about the vulnerability for zero days. These zero-days have proved to be effective cyber-weapons. There have been many examples of them being deployed for corporate espionage and the illegal capture of private information. There have also been times when our own government has used these exploits to infiltrate terrorist and criminal organizations (Wolf & Fresco, 2016). It has been made public that the NSA and CIA stockpile zero-day exploits with the intent of using them as offensive cyber weapons (Schwartz & Knake, 2016). However, by not disclosing these vulnerabilities to the software vendors affected, these government agencies are leaving American businesses and allies vulnerable to the same attacks.

In this paper I investigate the market for zero-day vulnerabilities as well as their impact on society. I use the consequentialist and non-consequentialist frameworks to identify potential ethical issues with stockpiling these vulnerabilities. Additionally, I make the case that there needs to be more accountability by the US government for how these cyber-weapons are handled. Like any weapon, zero-day vulnerabilities should be regulated, and their use should be understood.

Part 1: Inspection of the Zero-Day vulnerability market

In movies, hackers are often portrayed as geniuses attempting to outsmart rival computer systems. In reality, their job is similar to a prospector. They dig through machine code and try known exploits on systems day after day in the hope of finding an attack vector. This characterization is made not to minimize the skill required but to identify the difficulty of the task. No one hacker is capable of breaking into any system. Most of the skill required for the job comes in the form of knowing who and where to acquire information from. As noted by Ablon (2017), these hackers can be broadly sorted into two groups, white hat and black hat. White hat hackers "focus on finding zero-day vulnerabilities and giving them to the affected vendor, sometimes for a fee and sometimes for recognition" (Ablon & Bogart, 2017). Black hat hackers are not interested in disclosure. Instead, they seek zero-day vulnerabilities for private use.

Once discovered, the hacker is faced with the decision of what to do with the exploit. One option is to sell it to the organization affected by the vulnerability. Google, Apple, and Microsoft have all set up "bug bounty" programs that offer compensation to anyone who can identify and disclose vulnerabilities in their products (Wolf & Fresco, 2016). Payouts for the "bounties" range from several thousand dollars to a million dollars depending on the severity of the vulnerability (*Apple Security Bounty - Payouts - Apple Developer*, n.p.).

The other option these hackers have for profiting off zero-day exploits is to sell them on black or gray markets. Here, hackers will sell to clients from the private sector and governments. Wolf states that "the sale of exploits (...) appear to be almost always legal" (2017), however, these are still considered black/gray markets because the identity of the buyers and sellers as well as the terms of negotiations are undisclosed. The market for zero-days is characterized by Kesan as being "decentralized and unregulated" (2016).

Ethics of Purchasing Zero Day Vulnerabilities

For years, the United States government denied their purchase of zero-day vulnerabilities. However, we now know that they are involved in zero-day acquisitions in both the gray and black markets (Schwartz & Knake, 2016). Because of this it is important to identify some of the potential ethical concerns with engaging in these markets.

Purchasing zero-day vulnerabilities can easily be justified by arguing that it is better for these cyber-weapons to be in the hands of the US government than one of our adversaries. By not purchasing these vulnerabilities, the government would potentially be putting citizens at risk. However, by engaging in these markets, the government is at least passively legitimizing them. By leaving the markets unregulated, the sale of vulnerabilities to our enemies cannot effectively be slowed. This is a classic example of escalation of power. The US government has thus far refused to regulate sale of zero-days for fear of driving potential sellers to their adversaries. However, by engaging in the market, they have expanded them. More dollars spent by the US leads to more sellers. More sellers lead to more potential vulnerabilities that could fall in the hands of Russia, China, and North Korea. Understanding the importance of trading these vulnerabilities will involve exploring the dangers they pose.

Part 2: Analysis of risk posed by zero-day vulnerabilities

“Everything can be intercepted (...) everything is vulnerable” (Perlroth, 2021). This is what Dave Retz, one of the founding members of the first internet, identifies as the primary issue with the technology (2021). The internet and the technologies spurred on by its creation, have brought humanity closer together than anyone 50 years ago could have imagined. It is believed that over half the world’s population is now connected to the internet. This makes it one of the quickest spreading technology revolutions in human history. The internet allows creators and innovators to find markets and audiences continents away, it has allowed for the categorization and dissemination of the world's knowledge, and it has given millions of people control over their banking data.

Despite the good that comes from this interconnectedness, interception remains the central problem. As soon as data becomes connected to the internet, it becomes possible for it to be intercepted. For most of the data sent around the world this is not a significant issue. However, networked devices have become critical to almost all our essential infrastructure: water supplies, electric grids, air traffic control. Additionally, individuals entrust hospitals and banks with their sensitive medical and financial data. Access to all this information allows bad actors to exert tremendous levels of control. To combat this threat, individuals, corporations, and governments are all trying to increase their cybersecurity. According to Gartner, a leading technology consulting company, the cybersecurity market is expected to grow to $170.4 billion by 2022 (*Forecast Analysis*, n.p.). Despite the increase in spending, cybercrime is on the rise, both in scope and frequency. Cyber-attacks are the wrench thrown into the carefully calibrated cogs of the internet.

In May of 2017, the WannaCry ransomware attack was launched by a group of hackers backed by the North Korean government. The cyberattack utilized an exploit known as EternalBlue, which targeted older versions of Windows, a Microsoft operating system. This exploit had been developed by the United States National Security Agency several years prior but had not been disclosed to the vendor. Unfortunately, it was stolen and leaked by a group of international hackers. North Korea was then able to take this leaked exploit and unleash a ransomware attack of unprecedented scale (Eichensehr, 2017, p. 470).

The attack was ultimately able to be stopped mere hours after it had been deployed due to the efforts of security researchers from around the world. However, it had already affected more than 200,000 computers and resulted in hundreds of millions of dollars in damages. This incident brought international attention to the issue of zero-day stockpiling. In the aftermath of the attack, Brad Smith (2017), the president and vice chairman at Microsoft released a statement saying:

> Finally, this attack provides yet another example of why the stockpiling of vulnerabilities by governments is such a problem. This is an emerging pattern in 2017. 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. An equivalent scenario with conventional weapons would be the U.S. military having some of its Tomahawk missiles stolen (n.p.) .

The leadership at Microsoft clearly saw the NSA failing to disclose the EternalBlue exploit as an example of governmental overreach. They and many others called for reform in the wake of the attack. By comparing the exploit to a Tomahawk missile, they send a clear message. Cyber-Weapons should be thought of and regulated in the same way as traditional weapons. Regulations around who the US buys and sells weapons could potentially be extended to the exploits market. Cyber exploits do not produce explosions the same way tomahawk missiles do but they can cripple infrastructure in the exact same way.

One of the biggest risks posed by this cyberwar is the lack of trust felt by United States citizens. Cyber Security Expert and Author Nicole Perlroth (2021) writes “foreign states and cybercriminals are hitting American networks from so many sides that (...) it has become nearly impossible to keep track” (p. 800). The Pew Research Center has found that 70% of Americans anticipate major cyberattacks in the next five years (Smith, 2017, n.p.). Why then is the issue of cyber-warfare not a talking point for politicians? Eichensehr (2017) argues that the cybersecurity system in this country has been a “jury-rigged response to perceived security failures and market opportunities, and it has developed without democratic deliberation or even much public awareness” (p. 471). The problem stems from the lack of willingness of public and private entities to report security breaches. Companies and Government agencies, worried that disclosing these breaches will cause them to lose the public’s trust, have for decades dealt with these breaches internally. By repeatedly doing this, they make it harder for the public to know who has been compromised. Additionally, they reinforce the stigma around being hacked. If no one is confessing to having been breached it becomes harder for individual companies to confess. Due to the lack of transparency by these entities, the American people are put further at risk.

Current Stance by US Government

Little is known about the US’s policies around zero-day vulnerabilities. Recently, due to public pressure, information around their process for deciding when to disclose a vulnerability was released. This process is outlined in a document called the “Vulnerability Equities Process” or VEP (Schwartz & Knake, 2016). The document outlines a system with a bias toward full disclosure unless there is a “clear national security or law enforcement need…”(Schwartz & Knake, 2016). Many in the cybersecurity space have criticized this document for being vague and discouraging of disclosure (*Heartbleed*, 2014, n.p.). It is almost impossible to speculate on how many zero-day vulnerabilities the US government currently has stockpiled as this information would be classified. However, a stockpile of any size carries with it an ethical dilemma.

Part 3: Ethical Frameworks applied to Zero-Day Vulnerability Stockpiling

In researching zero-day stockpiling, two ethical viewpoints emerge: the consequentialist and non-consequentialist frameworks. The consequentialists argue that the optimal decision is the one that results in the most overall happiness. Another name for consequentialist thinking is utilitarianism. This type of thinking would not result in a clear-cut answer to the question of whether to stockpile. Instead, the voices in this camp tend to believe that the way to determine whether a vulnerability should be disclosed is to weigh its potential benefit against its potential danger. This could involve the creation of a scoring system, such as the one proposed by Pell & Finocchiaro (2017, p. 1565). This type of thinking seems to align with the position currently taken by the United States government. In attempting to weigh potential benefit versus harm for a zero-day, there are several factors that would need to be considered. These include the longevity of a vulnerability and the danger it could pose. Another important factor to consider is the likelihood that a zero-day vulnerability would be found independently by another entity (Ablon & Bogart, 2017). By choosing to not disclose a vulnerability, the government is taking the risk that this same vulnerability will not be discovered by an adversary. While exploits can be bought and sold, since they are intellectual property, there is never a guarantee that one is the sole proprietor. Under the consequentialist framework, it would make little sense to disclose zero-days that are difficult to find as there is little chance of another group independently discovering it.

The consequentialist argument has proven to be popular with policy makers, but ethicists seem more unsure of its utility. The main issue identified with this framework is the lack of differentiation between harm caused by action and harm caused by lack of action (Wicker, 2021). Additionally, to apply this type of thinking one must believe that they can make a reasonably accurate statement about potential benefit and harm. In the case of zero-days, it is possible that there is no good metric for the level of risk they pose. An outside observer could also see that it is a conflict of interest for the same people who will eventually use the exploits to be deciding if they should be disclosed. It may be that what is needed in these situations is a review board outside of the surveillance community ruling on zero-day disclosure.

The non-consequentialists framework assumes that one can not determine if an act is ethical based only on the outcome. Instead, the action taken must be ethical on its own. One inclined towards this way of thinking will most likely believe that all vulnerabilities should be disclosed. In this way, they avoid any of the calculated risks taken by the consequentialists. This argument is articulated by Wicker (2017) when he writes that the non-consequentialist approach "offers more traction, capturing our ethical intuition regarding the public risk that many think is inherent in zero-day exploits in particular and cyber warfare in general" (pg. 103). Although the NSA did not intend to cause damage to 200,000 computers when they created the EternalBlue exploit, they did have the intent of weaponizing it. The non-consequentialists would say that by not disclosing the vulnerability to Microsoft, the NSA acted unethically. This framework is more concerned with absolute morality. I believe that this framework will be more helpful when trying to craft legislation for zero-days.

At its core this is a hard technical problem. The US government has not demonstrated a strong ability to discern which vulnerabilities to disclose. In the future, although it may put the US at a tactical disadvantage in the short term, I believe a policy of disclosure will make US interests safer.

Conclusion

During the COVID-19 pandemic people became more dependent on cyber systems. These systems allowed us to work and learn from home, but they were also the target of attack. As we move forward in the process of digitizing our lives, it is imperative that cybersecurity is taken seriously by citizens, corporations, and government. Zero-day vulnerabilities are a commodity with a market fueled by desire for power. It is foreseeable that the wars of the future will be fought with these exploits. However, by not taking a hard stance on disclosure, the US government perpetuates this arms race. Cybersecurity, both domestic and abroad, cannot be gained with mutually assured destruction. By moving to a system of disclosure, we will be making our digital resources resilient and our ethical objections towards the cyber-warfare of our enemies more grounded.

References

Ablon, L., & Bogart, A. (2017). *Zero days, thousands of nights: The life and times of zero-day vulnerabilities and their exploits*. RAND Corporation.

Apple Security Bounty—Payouts—Apple Developer. (n.d.). Retrieved November 7, 2021, from https://developer.apple.com/security-bounty/payouts/

Eichensehr, K. (2017). Public-Private Cybersecurity. *Texas Law Review*, *95*(3), 467–538.

Forecast Analysis: Information Security, Worldwide, 2Q18 Update. (n.d.). Gartner. Retrieved November 7, 2021, from https://www.gartner.com/en/documents/3889055/forecast-analysis-information-security-worldwide-2q18-up

Heartbleed: Understanding When We Disclose Cyber Vulnerabilities. (2014, April 28). Whitehouse.Gov. https://obamawhitehouse.archives.gov/blog/2014/04/28/heartbleed-understanding-when-we-disclose-cyber-vulnerabilities

Perlroth, N. (2021). *This Is How They Tell Me the World Ends: The Cyberweapons Arms Race* (1st edition). Bloomsbury Publishing.

Schwartz, A., & Knake, R. (2016). *Government's Role in Vulnerability Disclosure: Creating a Permanent and Accountable Vulnerability Equities Process*. Belfer Center for Science and International Affairs. http://search.proquest.com/policyfile/docview/1923919527/CA7AE66278474220PQ/3

Smith, A. (2017, January 26). Americans and Cybersecurity. *Pew Research Center: Internet, Science & Tech*. https://www.pewresearch.org/internet/2017/01/26/americans-and-cybersecurity/

The need for urgent collective action to keep people safe online: Lessons from last week's cyberattack. (2017, May 14). Microsoft On the Issues. https://blogs.microsoft.com/on-the-issues/2017/05/14/need-urgent-collective-action-keep-people-safe-online-lessons-last-weeks-cyberattack/

Wicker, S. B. (2021). The ethics of zero-day exploits---: The NSA meets the trolley car. *Communications of the ACM*, *64*(1), 97–103. https://doi.org/10.1145/3393670

Wolf, M. J., & Fresco, N. (2016). Ethics of the software vulnerabilities and exploits market. *The Information Society*, *32*(4), 269–279. https://doi.org/10.1080/01972243.2016.1177764