Brinley Macnamara
Ming Chow
Comp 116 - Cyber Security
May 6, 2018

Buying Secrets: What you need to know about the gray market for zero day vulnerabilities

Abstract

A “zero day” is a term coined by security experts for a vulnerability in in piece of software that the vendor does not know about and has therefore not patched. The benefit of collecting zero days is the tactical advantage a zero day can provide for an entity seeking to infiltrate a system undetected. But there is also a notable cost: by opting to keep a zero day a secret instead of alerting the vendor of the vulnerability so it can be patched, users of the software are put at serious risk, as there is no stopping a bad actor from finding the same vulnerability and exploiting it. Over the years, a doctrine of “responsible disclosure” has developed, which says that security researchers should come forward with the zero days they discover so they can be properly patched by developers and a public advisory can be released alerting end users of the security update. However, without a solid incentive structure in place to motivate researchers to disclose their zero days, many have turned to the gray market to sell their findings. Buyers in the gray market include government agencies and private companies. The demand for anonymity by the parties selling and buying zero days has given rise to a new profession: vulnerability brokers who provide anonymity to the parties in exchange for a commission. After an extensive introduction on zero days, this paper will examine the various markets in which zero days are bought and sold, with a focus on the gray market as well as the middlemen that have emerged in mediating the sales of zero days.

Introduction

A vulnerability is a code defect that amounts to a security weakness. In turn, this security weakness can be exploited, resulting in “a negative impact to confidentiality, integrity or availability” (“Terminology”). A zero day vulnerability is a particularly nasty beast because it is unknown to the software vendor and has therefore not been patched. Upon discovering a zero day vulnerability, one can develop a zero day exploit that takes advantage of the defect “to access other parts of the system, execute [one’s] own code, act as an administrator, or perform some other action” (Albon and Bogart). The term zero day comes from the fact that software developers have known about the vulnerability for “zero days” and thus have no time to fix the vulnerability before it can be exploited by an adversary. In this paper, I will refer to zero day vulnerabilities and zero day exploits collectively as “zero days.”

I came across another definition of a zero day in my interview with a former boss, Dave Muran-de Assereto, a former Security Engineer for the Navy and now the Deputy Chief Security Officer at The Options Clearing Corporation in Chicago. He explained that a zero day is a vulnerability that “defense vendors do not know about” (Muran-de Assereto). In other words, a zero day vulnerability is one to which defensive tools are completely blind. “Since 99.9% of defensive tools are signature based, they depend on a static code signature like a hash or a

byte pattern or on some kind of reliable exploit method," and since by definition, a zero day has no known signature, these defensive tools are unable to detect zero days, which gives an attacker a huge "tactical advantage" in infiltrating a system undetected (Muran-de Assereto). Given the tactical advantage that zero days provide, nation states are very interested in collecting zero days. The interest in zero days is so prevalent, in fact, that a legitimate market has emerged for the buying and selling zero day vulnerabilities, in which researchers can sell their information on zero days to the highest bidder through vulnerability brokers. This market lies between the white market (bug bounties) and the black market (dark web forums in which zero days are bought and sold by cyber criminals) (Lemos). Given the difficulties that buyers and sellers face in validating the legitimacy of a zero day while protecting the intellectual property rights of the seller, vulnerability brokers have emerged as key players in mediating the sale of a zero day.

To the community

The intended audience for this paper is broad. I'm writing for non-technical readers with an interest in security as well as highly technical readers who are the leading the field in the development, disclosure, and weaponization of zero day exploits. I chose to write about the gray market for zero days because of how little is known about the sellers, brokers, and buyers who are operating in the market. I am also interested in the incentives pushing researchers towards the gray market and away from responsible disclosure, as well as the reasons buyers are shelling out large sums of cash to collect zero days. Vulnerability brokers have found a niche in this market that highlights its rapid growth, as well as the demand for anonymity and secrecy surrounding the dealings in this market, which the brokers help to provide. It is a fact that a researcher stands to make significantly more money selling their zero day on the gray market than by offering their finding to the software vendor in exchange for a bug bounty. Thus given the asymmetrical incentives pushing more and more researchers towards to the gray market, I think it is important for the community to know more about the middle men brokering these lucrative deals. In this paper, I hope to give the community a much needed look into the inner workings of this market as well as highlight the fact that there is still too little known about these dealings. I endeavor to impart a sense of urgency on the readers, who I hope will be compelled to lobby their representatives to take a closer look at the gray market for zero days.

More on zero day vulnerabilities

A zero day vulnerability comes from a bug in a piece of software. A bug is a defect in code, and as any software developer knows, they are quite common. According to Ablon and Bogart, the authors of a study on zero days sponsored by the Rand Corporation, there exist somewhere between "3 to 20 bugs per 1,000 lines of code." "However, not all bugs are vulnerabilities, and not all vulnerabilities can be usefully exploited. Some vulnerabilities may only enable an attacker to escalate privileges and conduct a denial-of-service attack, while others will actually allow an attacker to gain remote code execution—often thought of as the ultimate goal—whereby the compromised system runs an attacker's code without the user's

knowledge" (Ablon and Bogart). As the authors of the Rand study point out, a vulnerability poses little threat if it cannot be exploited. Exploitability is the key. That's the goal of anyone looking for a zero day vulnerability.

Analyzing the longevity of zero days

In their seminal study, Ablon and Bogart analyzed a dataset, handed over to them by a vulnerability vendor, of 200 zero day vulnerabilities spanning 14 years. They found the average life expectancy of a zero day vulnerability to be "6.9 years," with roughly 25% surviving less than a year and a half and 25% surviving more than 9.5 years (Ablon and Bogart). According to the researchers, a zero day vulnerability is "alive" as long as it is not publicly known (Ablon and Bogart). In their study, Ablon and Bogart describe the different ways a vulnerability can die. It can be "killed by a researcher" who makes a vulnerability publicly known so it can be patched (Ablon and Bogart). A vulnerability can die "via a security patch" after a software developer is alerted to the existence of a zero day vulnerability by an internal pen tester or by an outside security researcher (Ablon and Bogart). Oftentimes, it is protocol to release an advisory with the patch, alerting the consumers to the existence of the vulnerability so they can effectively patch their own systems that use the compromised software. Sometimes, if a researcher comes across a defect, but is unaware that it is a security vulnerability, they may write about it in a book or a blog (Ablon and Bogart). In this case, the vulnerability dies via "publicly shared" (Ablon and Bogart). There is also a subset of zero day vulnerabilities that Ablon and Bogart call "zombie-like" vulnerabilities. These vulnerabilities get fixed via code updates and are never disclosed as security vulnerabilities and may still exist in older versions of the software (Ablon and Bogart). Finally, there is a subclass of vulnerabilities which the Rand researchers refer to as "immortal" because they live in software which is no longer maintained by the vendor and will thus never be patched (Ablon and Bogart).

Who is looking for zero day vulnerabilities anyway?

Researchers, cyber criminals, and nation state actors all have in interest in finding zero days. Researchers may be independent or they may be employed by software vendors. The vulnerabilities found by employees of a software company may be used to to fortify the company's products or in advanced penetration testing (Graham and Maynor 1). If an independent researcher finds a vulnerability, she may choose to hand it over to the software vendor and be rewarded a modest bug bounty, or she may choose to sell it on black or gray markets. Cyber criminals have an obvious interest in finding zero days, as they give them a strong tactical advantage in infiltrating systems. But there is some evidence that cyber criminals are more interested in so-called "one day" vulnerabilities ("A World of Vulnerabilities"). One day vulnerabilities are known vulnerabilities ("A World of Vulnerabilities"). Attacks using this kind of vulnerability are much less expensive to engineer given how "expensive" and "time-consuming" it is to conduct the research necessary to "discover and exploit a [zero day] vulnerability" ("A World of Vulnerabilities"). Tools exploiting one day vulnerabilities are widely available online and are far less expensive than zero day exploits. According to Muran-de Assereto, the key idea

when thinking about the motivations of cyber criminals is “return on investment.” “The most effective assertion here is that an attacker will use the minimum investment required to achieve their ends” (Muran-de Assereto). That means opting to use more economical vectors of attack if they are just as effective at achieving the end goal as using a zero day would be. Moreover, consumers are notoriously bad a patching their systems, making it easy for attackers to leverage one day vulnerabilities to gain access. In an interview with Infosec, David Harley, a senior researcher, explained: “the increase in volume of one day exploits suggests that even if zero days’ research prices itself out of the mass market for exploits, inadequate update/patch take-up among users is leaving plenty of room for exploits of already-patched vulnerabilities (as with the current spate of Tibet attacks)” (qtd in “A World of Vulnerabilities”). The Tibet attacks Harley is referring to were a series of attacks, thought to be sponsored by Beijing, against Tibetan activists as well as companies in Japan and India (“Chinese hackers and Operation ‘Luckycat’”). The attack exploited a known Office stack overflow vulnerability (“Chinese hackers and Operation ‘Luckycat’”). According to Pierluigi Paganini, a writer for Security Affairs, “the malware used is a variant of Gh0st RAT, a well know remote access Trojan, that enables [the attacker] to acquire the total control of the target allowing documents theft and cyber espionage.” The bottom line here is that if the target machines had been properly patched, this exploit would have been ineffective. Instead, companies routinely fail to patch their systems, leaving themselves vulnerable to one day exploits like the one used in the Tibet attacks. Moreover, this assertion is strongly supported by the the data. According to the 2015 Verizon Data Breach Investigations Report, “99.9 percent of the exploited vulnerabilities had been compromised more than a year after the associated CVE was published.” It is those who are seeking to penetrate more hardened infrastructure who are the most interested in zero days. Nation states fall into this category. According to Sebastian Anthony, who writes for Ars Technica, zero days are weapons of precision: “think of an exploit based on a zero day vulnerability as a laser-targeted, bunker-busting bomb for solving a single problem rather than a panacea.” A prime example of this type of zero day usage is Stuxnet, a malicious worm that exploited four Windows zero day vulnerabilities (“Stuxnet Attackers Used 4 Windows Zero-Day Exploits”). The worm wreaked havoc on Iran’s centrifuges, causing significant damage to its nuclear program (“Stuxnet Attackers Used 4 Windows Zero-Day Exploits”). Presumably, the machines controlling Iran’s centrifuges were well patched, which forced the developers of Stuxnet to think of more creative ways to undermine Iran’s nuclear infrastructure. It seems that the use of zero days was necessary in order to penetrate Iran’s well fortified machines.

What is the likelihood that two researchers will come across the same zero day?

Authors Ablon and Bogart of the Rand study on zero days sought to weigh the pros and cons of nation states collecting zero days, opting to keep them to themselves rather than disclosing them to the software vendors. This is a policy question that I will not delve too deep into in this paper, but it is worth mentioning that the likelihood that two researches will find the same zero day, which the Rand researchers call the “collision rate,” is non-zero (Ablon and Bogart 60). According to the authors of the Rand study, “for a given stockpile of zero day vulnerabilities, after a year approximately 5.7% have been discovered by others” (Ablon and

Bogart) This finding suggests that stockpiling zero day vulnerabilities carries some risk, as it leaves a nation state's citizens exposed to the potential for an adversary to come across the same vulnerability and exploit it in an attack against a defenseless population. The Rand researchers conclude by suggesting that if an intelligence agency thinks there is a good chance another researcher may find the same vulnerability, they should disclose (Ablon and Bogart). Otherwise, it is in the interest of national security to keep the zero day a secret (Ablon and Bogart).

To publicly disclose or not to publicly disclose

In his reporting for Ars Technica, Sebastian Anthony describes three outcomes for a newly discovered zero day: it can be published on a public forum, it can be disclosed privately to the vendor, or it can be sold to a third party. The key question here is whether or not public disclosure does more harm than good. According to Adriel Desautels, a senior researcher and CEO of Netragard, a company in the business of buying and selling zero days, public disclosure is reckless (Anthony). He cites the Verizon Data Breach Report from 2015, which found that half of the attacks using known vulnerabilities were attempted within just three weeks of the vulnerabilities' public disclosure. "When you publish a vulnerability," says Desautels, "when you publish information—even if it's partial information—you are telling the world that a specific piece of software can be hacked" (qtd in Anthony). On the other side of the debate is Dave Muran-de Assereto, who believes public disclosure is necessary to motivate software companies to fix their vulnerabilities. In his mind, public disclosure puts pressure on companies to patch their systems, and without it, they'd have little incentive to issue free patches (Muran-de Assereto). "The problem with proprietary software in general is that the entire Software Development Life Cycle," he says, "is governed solely by the profit motivation. And there is little margin in providing free patches" (Muran-de Assereto). I think I come down on Muran-de Assereto's side of this debate. Although there is demonstrated risk in publicly disclosing vulnerabilities, having a public record of vulnerabilities is necessary not only to keep companies accountable, but also for educational and research purposes. There is value in keeping a public record of vulnerabilities so that newly minted software engineers don't make the same mistakes as their predecessors, and in the likely chance that they do, there is a regularized process for patching and publishing the vulnerability based not on shame and secrecy but on openness and transparency.

Where zero days are bought and sold: The white, black, and gray markets for zero day vulnerabilities

According to Robert Lemos, a writer for TechTarget, there are three markets in which zero day sales take place. In the white market, discoverers of zero days hand over their information to software vendors in exchange for modest bug bounties and public recognition (Lemos; Algarni and Malaiya). Additionally, the white market includes sales to third parties who are in the business of helping software developers fix their vulnerabilities (Lemos; Algarni and Malaiya). An example of such a third party is HP's Zero Day Initiative, whose website advertises

its mission to encourage researchers to come forward with their vulnerabilities and its work to support affected companies in the patch and advisory process (*Zero Day Initiative*). Either way, the end result of a vulnerability sale in the white market is the disclosure and the ultimate patching of the vulnerability. Alternatively, a researcher can sell their vulnerability on the black market for a substantial price (Ablon, Golay, and Libicki 26). Buyers in this market include cyber criminals, cyber terrorists and even government agencies (Algarni and Malaiya). Sales in the black market typically happen on dark web forums and payments are made in cryptocurrency (Ungerleider). Although the payouts in the black market tend to be higher than the average bug bounty, selling in this market is risky, as the seller could face criminal prosecution for doing so (Miller 2). For risk-averse researchers seeking large payouts for their findings, selling on the gray market may be an enticing option. According to Lemos, buyers in this market include government agencies (documents released by Edward Snowden show that the NSA spent more than $25 million on purchasing zero days in 2013 alone), as well as “vendors of espionage and monitoring Trojans, who argue that exploiting vulnerabilities to surveil criminals or potential enemies is a natural evolution of today’s digital society” (Krebs). Prices in this market are typically more negotiable (Algarni and Malaiya). While the researcher can earn a couple hundred dollars to $10,000 from a bug bounty on the white market, they stand to earn from $20,000 to $200,000 by selling to gray market buyers (Lemos). According to a study conducted by the Rand Corporation on markets for software vulnerabilities, a “researcher could earn 10-100 times [in the gray and black markets] what a software vendor with a bug bounty would pay” (Ablon, Golay, and Libicki 26). Sales of vulnerabilities in black and gray markets are similar in that the vulnerabilities sold are never disclosed. Instead, the buyers choose to hoard the vulnerabilities so they can be used in offensive operations against their opponents or in defensive operations, such as penetration testing (Ablon and Bogart 3).

Gauging the price of a zero day vulnerability

There are a multitude of factors that affect the price of a zero day vulnerability. An obvious factor is how difficult it is to find the vulnerability (“A World of Vulnerabilities”). Andy Greenberg, a technology writer for Forbes, says that Grugq, a vulnerability broker based in Bangkok, told him that “an iOS exploit pays more than one that targets Android devices partly because it requires significantly tougher security features. This means that agencies can simply develop their own Android attacks, while ones that can penetrate the iPhone are rare and pricey” (“Shopping for Zero-Days”). Another factor is how popular the vulnerable application is (“A World of Vulnerabilities”). If it’s a popular product, like an iOS device, the price will be higher. Another factor affecting price is whether the application is “included by default with the OS” (“A World of Vulnerabilities”). A vulnerability in Internet Explorer, for example, may be worth more than an application that must be downloaded by the user onto a Windows operating system. Another factor is whether or not “typical firewall configurations block access to the application” (“A World of Vulnerabilities”). Additionally, the vulnerability will be worth more if user interaction is not required to exploit the vulnerability (“A World of Vulnerabilities”). Vulnerabilities in more recent versions of software typically command high prices (“A World of Vulnerabilities”). And

finally, vulnerabilities in newer technologies have higher value than vulnerabilities affecting older technologies (“A World of Vulnerabilities”).

The role of vulnerability brokers in a market for secrets

According to security expert Charlie Miller, although a sale of a zero day to a buyer on the gray market has the potential to earn her the largest return on investment, the security researcher faces many challenges in coordinating the sale of her zero day (2). The first is that the sale of a zero day, Charlie Miller says, is an extremely “time-sensitive” matter (2). The value of a zero day depends on it being a secret. As soon as a zero day is published, it is no longer a zero day and has substantially less value to the buyer. If another researcher happens to find the same zero day, which is entirely possible, “the value of the sale could decay to zero if any third party preemptively divulges information on the vulnerability” (“A World of Vulnerabilities”). In other words, time is not on the side of the zero day seller. She must find a buyer promptly, before her information is rendered worthless. The second issue a seller faces is the lack of “transparent guidelines” for pricing (Miller 3). The third issue a seller must overcome is the difficulty in finding a reliable buyer (Miller 3). But perhaps the most difficult issue a seller faces is supplying a potential buyer a proof-of-concept without disclosing too much information about the vulnerability and the mechanisms of exploiting it (Miller 4). If the seller happens to divulge too much information, the buyer could find the vulnerability on her own and would have no reason to shell out the cash to pay for the seller’s findings. “To respond to [the emerging needs of zero day sellers], and to regulate the transactions between buyers and sellers, a new profession specializing in mediation was born: brokers for sales of zero day exploits who provide anonymity to the bargaining parties in return for a commission” (“A World of Vulnerabilities”). Typically, vulnerability brokers have large rosters of clients, which makes it possible for them to connect a seller with a interested buyer in a timely manner. Moreover, they are paid a commission of the final sale price and thus have an interest in selling the vulnerability to the highest bidder, which is obviously good for the seller (“Shopping for Zero-Days”). Additionally, they can help to iron out the details of arranging a demo of the zero day for the buyer. Again, they have an interest in protecting the seller’s intellectual property rights, as if one sale falls through, they want to be able to retain the seller in case another interested buyer comes knocking. This doesn’t eliminate the risk in providing a proof-of-concept, but it certainly makes it easier, as vulnerability brokers boast lots of experience in this line of work, and can provide valuable expertise, especially if the researcher is a first time seller.

There are too many companies and individuals in the business of vulnerability brokering to mention all of them. The Economist estimates there are more than two hundred vulnerability brokers in the business of mediating vulnerability sales (“The Exploits of Bug Hunters”). But it is important to note that many vulnerability brokers employ their own researchers to find zero days to sell to their clients. Additionally, instead of mediating deals between discoverers of zero days and potential buyers, many vulnerability brokers choose to purchase zero days from their discoverers, which they go on to resell to their clients. Some well known vulnerability brokers include individuals like Grugq, a Bangkok-based broker, start-ups who specialize in vulnerability

brokering like Vupen, Netragard, and ReVuln, and larger enterprises like Raytheon and Northrop Grumman (“Shopping for Zero-Days”; “A World of Vulnerabilities;” Perlroth and Sanger).

In the early 2010s, the success of two state sponsored cyber-attacks leveraging zero day flaws fueled a surge of interest in the market for zero day vulnerabilities (Lemos). The first attack was Stuxnet, an operation thought to be carried out by US and Israeli intelligence agencies that used four zero days in Windows to infect the computers controlling Iranian centrifuges (“Stuxnet Attackers Used 4 Windows Zero-Day Exploits”). The second was Aurora, a Chinese-sponsored attack targeting technology companies in the US which exploited a zero day in Internet Explorer that allowed attackers to inject malware into a target’s computer (Zetter). The success of these highly sophisticated attacks demonstrated the enormous value of zero day vulnerabilities, which stoked interest among hackers and researchers in finding these vulnerabilities and drove an increasing number of deep-pocketed buyers to the gray market with the hopes of collecting these high-value high-precision cyber weapons (Lemos). According to Adriel Desautels, the chief executive of Netragard, the market “exploded” in the early 2010s (qtd in “A World of Vulnerabilities”). He says that “time for a purchase accelerated from months to weeks” and sellers are now offering him more exploits (qtd in “A World of Vulnerabilities”). As a result, Netragard’s “exploit acquisition program has doubled in size” (Perlroth and Sanger). The exploits Netragard sells go from $16,000 to more than $250,000, which the average flaw selling from $35,000 to $160,000 (Gallagher; Perlroth and Sanger). Netragard refuses to sell to anyone outside the US (Ungerleider).

In an interview with Forbes, a vulnerability broker whose goes by the name of Grugq says he netted a million dollars in 2012 (“Shopping for Zero-Days”). He claims that he only sells to American and European agencies “not merely out of ethical concerns, but also because they pay more” (“Shopping for Zero-Days”). Russia, he says, doesn’t pay enough, and the market in China is flooded with vulnerabilities, which depresses prices (“Shopping for Zero-Days”).

French-based Vupen employs its own team of hackers to find vulnerabilities in software, which it goes on to sell to its roster of clients (“Meet the Hackers”). The company recently chose to forgo a $60,000 prize offered by Google for a zero day its team found in Chrome (“Meet the Hackers”). Instead, Vupen will sell this vulnerability to its clients who pay “$100,000 annually for a subscription plan, which gives them the privilege of shopping for Vupen’s techniques” (“Meet the Hackers”). The subscription fee does not cover the cost of each vulnerability (Perlroth and Sanger). Clients pay for those separately (Perlroth and Sanger). According to Vupen’s chief executive, Chaouki Bekrar, in Vupen’s nascent years, the company sought to disclose the vulnerabilities it found so the software vendors could fix their flaws (“Meet the Hackers”). But after a venture capital firm invested $1.5 million into the company, Vupen switched gears and began keeping their findings secret so they could be sold with exclusivity rights to government agencies and private companies (“Meet the Hackers”). Vupen reported earning $1.2 million in revenue in 2011 (Gallagher). The company says its selective about who it sells its zero day

vulnerabilities to, limiting its sales to 60 countries that are members or partners of NATO and refusing to sell to any countries against which export sanctions have been levied (Gallagher).

Like Vupen, ReVuln, lead by Luigi Auriemma, employs its own team of researchers to find flaws in the industrial control systems that run water treatment facilities, oil and gas pipelines, and power plants (Perlroth and Sanger). This is Auriemma's specialty. According to Brian Krebs, a former Washington Post reporter who writes about security, ReVuln sells more than 9 exploits a year for undisclosed amounts. Revuln is transparent about who they will and will not sell to. They say on their website that they will not do business with "countries which are subject to international embargoes adopted by the United Nations" ("Vulnerabilities: 0-Day Technologies"). They also say that they will limit their sales to "governments, law enforcement, trusted security vendors, and worldwide companies and corporations" ("Vulnerabilities: 0-Day Technologies").

Ethical concerns about the gray market

One of the most outspoken critics of vulnerability brokers is Christopher Soghoian, formerly the principal technologist at the American Civil Liberties Union. Soghoian thinks that by profiting from the sales of zero days to their clients rather than taking the route of responsible disclosure, vulnerability brokers are playing a dangerous game. "As soon as one of these weaponized zero days sold to governments is obtained by a bad guy," Soghoian says, "and [is] used to attack critical US infrastructure, the shit will hit the fan" (qtd in "0-Day Exploit Middlemen Are Cowboys"). Soghoian has called vulnerability brokers like Vupen and Netragard "cowboys," "a ticking bomb," and "modern-day merchants of death" selling "the bullets of cyberwar" (qtd in "0-Day Exploit Middlemen Are Cowboys"; qtd in Gallagher). Others argue that vulnerability brokers provide a much needed service to their government clients, providing them with the most advanced cyber weapons so they can "keep pace with what adversaries [...] are doing" (Gallagher). When I asked Muran-de Assereto about the ethics of buying zero days on the gray market, he agreed that it is a "dangerous game, but so is mutually assured destruction." "So is the idea that everybody has a large standing military force in order to back up their national will" (Muran-de Assereto). "Nation states," he went on, "have a need to understand what other nation states or entities are doing, and that might not be information that they want you to know so you have to be able to conduct espionage. And you have to be able to defend yourself against offense or even in same cases launch an offensive" (Muran-de Assereto). Despite the compelling arguments made by Soghoian and Muran-de Assereto, I'm of the opinion that there is just not enough data to make strong assertions about the ethical dilemma that the gray market poses. Many of the companies and individuals in the business of vulnerability brokering operate under a shroud of secrecy. It is rare for leaders in this business to openly discuss their work. Chief executives like Adriel Desautels and Chaouki Bekrar, who have been willing to talk to reporters about their work, are outliers among their peers, who make a living guaranteeing secrecy to their clients. Netragard, Vupen, and ReVuln all claim to be scrupulous about who they sell their exploits to. They all say they refuse to sell to embargoed nation states, although there is some evidence this might not be the industry standard. According to leaked emails

belonging to Hacking Team, a Milanese broker, the firm sold exploits to Bahrain, Egypt, Morocco, Russia, Saudi Arabia, Sudan, and the United Arab Emirates--countries, some subject to sanctions, with troubled human rights records ("The Exploits of Bug Hunters"). And even if every vulnerability broker properly vetted their buyers and practiced selectivity based on human rights, the governments they would choose to do business with would still be willing to use these cyber weapons in an attack against another nation's populace. From a target's perspective, these sales are not legitimate. Rather, they are tainted by the eschewing of ethics on the part of the seller, broker, and buyer in favor of making a profit. Of course, the brokers would counter by saying that by arming nation states with zero day exploits, they are doing a service to society, as the theory of deterrence says that the wide circulation of these exploits precludes nation states from using these weapons, as the threat of an opponent using them in retaliation is too great. All that said, I am not willing to stake a claim. There is just not enough public information about the nature of this market, its buyers, and the exploits being sold. I am comfortable with punting the ethical question to policy makers, who should work to shine some light on this market that has long been shrouded in secrecy.

In Summary

Zero day vulnerabilities pose a significant threat to modern day technology users. While there is some evidence that cyber criminals are more interested in so called one day vulnerabilities--known flaws that can be exploited due to the inadequate patch compliance by end users--nation states and private companies have shown a keen interest in the collection of zero day vulnerabilities, which they can purchase with the help of vulnerability brokers on the gray market. There has long been a standard for "responsible disclosure" in the security community, which presumes vulnerability discoverers will be motivated by ethical concerns to disclose their findings to the affected software vendor, but the rapid growth of the gray market for vulnerabilities shows that the assumption that vulnerability researchers will be guided by their ethics, rather than the profit motive, may be naive. Vulnerability brokers have emerged as formidable players in the gray market, with many employing their own teams of hackers to find zero days that they go on to sell to their large rosters of eager clients. Some brokers, such as Netragard, Vupen, and ReVuln, abide by strict guidelines for who they will sell their product to, refusing to do business with governments that have been sanctioned by the United Nations. Others, like Hacking Team, are less scrupulous, prompting ethical concerns about these powerful tools falling into the wrong hands, namely countries with dubious human rights records. While these concerns are legitimate, there is too little data about these companies to make broad assertions about their ethics. That should be up to policy makers, who should work to shed light on an industry that has long be shrouded in secrecy.

References

2015 Data Breach Investigations Report. Verizon, 2015, *2015 Data Breach Investigations Report*,

www.verizonenterprise.com/resources/reports/rp_data-breach-investigation-report_2015_en_xg.pdf.

Ablon, Lillian, and Andy Bogart. *Zero Days, Thousands of Nights*. Rand Corporation, 2017, *Zero Days, Thousands of Nights*, www.rand.org/content/dam/rand/pubs/research_reports/RR1700/RR1751/RAND_RR1751.pdf.

Ablon, Lillian, Golay, Andrea and Libicki Martin. *Markets for Cybercrime Tools and Stolen Data*. Rand Corporation, 2014, *Markets for Cybercrime Tools and Stolen Data*, www.rand.org/content/dam/rand/pubs/research_reports/RR600/RR610/RAND_RR610.pdf.

Algarni, Abdullah M, and Yashwant K Malaiya. "Software Vulnerability Market: Discoverers and Buyers." *International Journal of Computer, Information Science and Engineering*, vol. 8, 2014, pp. 71–81., pdfs.semanticscholar.org/2d8a/9d88cf83993c1774ddc66f30b086b6f300ab.pdf.

Anthony, Sebastian. "The First Rule of Zero-Days Is No One Talks about Zero-Days (so We'll Explain)." *Ars Technica*, Conde Nast, 20 Oct. 2015, arstechnica.com/information-technology/2015/10/the-rise-of-the-zero-day-market/.

Gallagher, Ryan. "Cyberwar's Gray Market." *Slate*, The Slate Group, www.slate.com/articles/technology/future_tense/2013/01/zero_day_exploits_should_the_hacker_gray_market_be_regulated.html.

Graham, Robert, and David Maynor. "Black Hat." Errata Security, *A Simpler Way of Finding 0day*, www.blackhat.com/presentations/bh-usa-07/Maynor_and_Graham/Whitepaper/bh-usa-07-maynor_and_graham-WP.pdf.

Greenberg, Andy. "Meet the Hackers Who Sell Spies the Tools to Crack Your PC (And Get Paid Six-Figure Fees)." *Forbes*, Forbes Media, 21 Mar. 2012, www.forbes.com/sites/andygreenberg/2012/03/21/meet-the-hackers-who-sell-spies-the-tools-to-crack-your-pc-and-get-paid-six-figure-fees/#57d123171f74.

Greenberg, Andy. "Shopping For Zero-Days: A Price List of Hackers' Secret Software Exploits." *Forbes*, Forbes Media, 23 Mar. 2012, www.forbes.com/sites/andygreenberg/2012/03/23/shopping-for-zero-days-an-price-list-for-hackers-secret-software-exploits/#2202ecc52660.

Krebs, Brian. "How Many Zero-Days Hit You Today?" *Krebs on Security*, Krebs on Security, krebsonsecurity.com/2013/12/how-many-zero-days-hit-you-today/.

Lemos, Robert. "Private Market Growing for Zero-Day Exploits and Vulnerabilities." *SearchSecurity*, TechTarget,

searchsecurity.techtarget.com/feature/Private-market-growing-for-zero-day-exploits-and-vulnerabilities.

Macnamara, Brinley, and David Muran-de Assereto. 24 Apr. 2017.

Miller, Charlie. *The Legitimate Vulnerability Market*. Independent Security Evaluators, 2007, *The Legitimate Vulnerability Market*, www.econinfosec.org/archive/weis2007/papers/29.pdf.

Naraine, Ryan. “0-Day Exploit Middlemen Are Cowboys, Ticking Bomb.” *ZDNet*, CBS, 16 Feb. 2012, www.zdnet.com/article/0-day-exploit-middlemen-are-cowboys-ticking-bomb/.

Naraine, Ryan. “Stuxnet Attackers Used 4 Windows Zero-Day Exploits.” *ZDNet*, CBS, 14 Sept. 2010, www.zdnet.com/article/stuxnet-attackers-used-4-windows-zero-day-exploits/.

Paganini, Pierluigi. “A World of Vulnerabilities.” *Infosec*, Infosec Institute, resources.infosecinstitute.com/a-world-of-vulnerabilities/.

Paganini, Pierluigi. “Chinese Hackers and Operation ‘Luckycat’ against Japan, Tibet and India.” *Security Affairs*, 2 Apr. 2012, securityaffairs.co/wordpress/3845/hacking/chinese-hackers-operation-luckycat-against-japan-tibet-and-india.html.

Perlroth, Nicole, and David Sanger. “Nations Buying as Hackers Sell Flaws in Computer Code.” *New York Times*, New York Times, www.nytimes.com/2013/07/14/world/europe/nations-buying-as-hackers-sell-computer-flaws.html

“Terminology.” *Common Vulnerabilities and Exposures*, Mitre, 15 Dec. 2017, cve.mitre.org/about/terminology.html.

“The Exploits of Bug Hunters.” *The Economist*, The Economist Group, www.economist.com/news/science-and-technology/21722157-trading-software-flaws-booming-business-exploits-bug-hunters.

Ungerleider, Neal. “How Spies, Hackers, And the Government Bolster A Booming Software Exploit Market.” *Fast Company*, Fast Company, Inc., 1 May 2013, www.fastcompany.com/3009156/how-spies-hackers-and-the-government-bolster-a-booming-software-exploit-market.

“Vulnerabilities: 0-Day Technologies.” *Revuln*, Revuln, revuln.com/#page2-vulnerabilities.

Zero Day Initiative, HP, www.zerodayinitiative.com/.

Zetter, Kim. “Hack of Google, Adobe Conducted Through Zero-Day IE Flaw.” *Wired*, Condé Nast, 14 Jan. 2010, www.wired.com/2010/01/hack-of-adob/.