United States Naval Academy

MIDN Max Goldwasser
MIDN Zac Dannelly
MIDN Bill Young

Software Identified Exploits Reporting and Reward Agency

November 9th, 2016

Bug Bounties: Where are we?

Bug bounty programs, sometimes labeled as vulnerability reward programs, seek to discover zero-day exploits preemptively by offering financial rewards for their discovery. Some of these programs are event based, like "Battlehack", and try to encourage participation through incentives like gourmet food, beer breaks, and even a massages. Other programs are run by companies, which offer fiscal compensation for any bugs found on their software based on the severity of the flaw. Examples of these cooperation based systems include Facebook, Google, Paypal, and Microsoft. These typically result in proportionally larger rewards, with all of the programs paying more than $1 million during 2014 for valid bugs.

What sort of effect have these enticing social events and monetary rewards had on the prevalence of zero-day exploits in the wild? Not much. At any point in time over the last few years, an adversary could have accessed more than 85 of these invisible weapons and then persisted to utilize the breaches they created for more than 150 days. The overall lack of effect on this market stems from motivation gaps on both the sides of the buyers, companies whose vulnerabilities are to be discovered, and sellers, the white hat hackers tasked with rooting them out.

Economics

1. First to market: Companies have a long list of economic incentives to be the first with a new technology in the consumer space and in turn incur less liability when their software is launched riddled with vulnerabilities.

2. Not a big investment: Google, Facebook, Microsoft, and United, all of whom are touted as the top Bug Bounty Programs in the world, spend less than a half of a percent of their budget on their implementations.
3. Value discrepancy: The maximum payout for the companies listed above programs is only $150,000, compared to the market price for similar vulnerabilities on black-market sites, which is closer to $200,000 and can extend all the way to $250,000 for iOS zero-day exploits.

These conflicting economic incentives offer a unique place for a new entity to step in with an innovative and cooperative solution: The Software Identified-Exploits Reporting and Reward Agency (SIERRA).

What defines software?

Software generally refers to organized information in the form of operating systems, utilities, programs, and applications that enable computers to work. Software consists of carefully organized instructions and code written by programmers in any of various special computer languages. Software is divided commonly into two main categories:

1. System software: controls the basic (and invisible to the user) functions of a computer and comes usually preinstalled with the machine.

2. Application software: handles multitudes of common and specialized tasks a user wants to perform, such as accounting, communicating, data processing, word processing.

Tasking

SIERRA will assume the primary role of expanding the concept of bug bounty programs to all levels of industry. As with any national program, SIERRA will distribute the intellectual and fiscal capital cost of bug reporting and exploit patching across the national spread of software companies. It will focus exclusively on the software applications that US financial and critical infrastructure relies upon that are within the jurisdiction of the American government. The aim of the program is to incentivize people to easily and responsibly report bugs in software products. It is critical that these incentives be adequate to encourage hackers and capable users to disclose identified security vulnerabilities rather than exploit them or sell the discoveries on illicit marketplaces.

Scope

SIERRA is chiefly interested in the vulnerabilities within software, not the threats against organizations, systems, and the people who use them. Moreover, entities within government already exist to handle and respond to malware and therefore will not be addressed by SIERRA's reporting mechanisms. SIERRA seeks to improve software security farther up the supply chain and reduce the number of potential avenues for exploitation within applications before they are discovered and acted upon by malicious actors.

Structure

The organizational placement of this agency is a key consideration. SIERRA's goal of increasing the overall security within the US software industry makes it a natural fit into the mission set of the Department of Homeland Security. Underneath the funding and authorities of DHS, SIERRA will also be chiefly integrated with the National Institute of Standards and Technology as domain experts. Within SIERRA itself, there will be three primary divisions:

1. Software Analysis: Every identified software exploit entered into the SIERRA database will receive a software importance score (SIS), to be determined by the Technical Advisory Board. The technical advisory board will be a group of industry professionals tasked with quantifying the significance of a piece of software based on many factors including the total user base, primary usages, and sectors within which it is used. The SIS will be a key factor when determining the payout for bounties.

2. Reporting: The majority of current programs do not have a central portal for individuals to disclose vulnerabilities, which may turn away those willing to contribute but who may be lacking the time to decode the intricacies of multiple, disparate unique interfaces.

3. Public Engagement: SIERRA must remain in constant contact with its supported community of registered security researchers as well as private industry partners.

Considerations

A. Crowdsourced Security

Part of SIERRA's overall mission structure will consist of an opt-in bug bounty program for companies who wish to amortize the cost of software security across the industry. Under this framework, organizations will have the option to provide unreleased software to SIERRA for community testing and security research.

B. Anonymous Bug Reporting

SIERRA will provide a means for private entities to report bugs in software produced by any organization, regardless of the company's participation in the BETA testing program. This affords the nation a far stronger security posture.

C. Cyber Law: The Computer Fraud and Abuse Act

The SIERRA program will need to address two significant legal issues concerning the potential for legal action against both consumers and commercial entities alike. The majority of legislation regarding best practices for security researchers, white hat hackers, and concerned users is vague at best. The Computer Fraud and Abuse Act (CFAA) is the only relatively comprehensive legal framework regarding the appropriate use of information systems and the penalties for misuse and theft surrounding computers and intellectual property.

Crowdsourced Security

Software vendors that wish to join the SIERRA opt-in program will complete a registration process. Once registered, they gain the ability to add software to the SIERRA software database for vulnerability analysis. This software should be accessible in either a trial version or with a special SIERRA user key to limit functionality and prevent theft. The level of access granted to researchers will be at the discretion of the companies with the knowledge that with less access comes less program effectiveness. This is a decision that lies solely with participating companies, and SIERRA will be sensitive to their unique privacy concerns. Additionally, companies can submit software that is still in BETA testing and not currently available on the market. Companies that do this will incur a much lower liability if vulnerabilities are found.

Companies will pay a fee in order to submit software to the SIERRA database. The fee will depend primarily on the size and complexity of the software in question, as these factors tend

to correlate with the volume of bugs discovered. This fee will produce a means to both award bounties and contribute funds to SIERRA's operational expenses?

Participation & Reporting

There will be two options for those interested in participating in SIERRA: anonymous researcher and registered researcher.

> Anonymous: SIERRA recognizes the importance of offering the option to remain anonymous. As such, it respects the culture underpinning the majority of the exploit community and understands the potential risk non-US persons may incur by aiding in our national security. Anonymous researchers will have full access to the bug reporting portal but will not have access to privileged software provided to SIERRA by software vendors.
>
> Registered: Those who wish to be a part of the SIERRA-supported research community will, like companies participating in the BETA program, register online and be subject to an approval process. Those registered will be able to login and view all of the software that companies have added to the SIERRA database for analysis and possess the ability to download trial versions directly from the site with the denoted special keys for researchers. Registered users will enjoy certain legal protections, outlined in the legal section of this proposal. Similar to anonymous users, registered researchers will have full access to the bug reporting portal.

The reporting portal provides a secure means for both anonymous and registered researchers to submit detailed reports of their findings alongside evidence of unintended software behavior and assessment of its significance.

Post-Reporting: Assessment and Reward

Once a report occurs is reported it will be sent to NIST for documentation within the National Vulnerability Database as well as an assessment of the criticality of the report through the Common Vulnerability Scoring System v3.0. This determination of the CVSS will be factored in with the SIS of the particular piece of software to calculate the vulnerabilities raw criticality. This will be modified based on a current assessment of the exploit market that will generate a tangible value to be paid out.

Crowdsourced Security: Bugs discovered in BETA software

For bugs discovered in the BETA testing and crowdsource program, bounties shall be paid using the posting fee provided by the software vendor. The size of the bounty will vary based on the raw criticality of the bug, but will not exceed 85% of the value of the posting fee. After a six-month period, no bounties shall be paid, and the remaining value of the posting fee shall be deposited into the SIERRA general bounty fund.

Bugs discovered at-large

Bugs discovered in software programs at-large shall be paid using a combination of funds from the SIERRA general bounty fund as well as the originating software vendor responsible for the bug. The size of the bounty will vary based on the raw criticality of the bug and a multiplier that tracks current trends in the exploit market. Companies will owe an increasing amount toward the final bounty payout as time progresses without the deployment of a patch to address the vulnerability. The amount the companies are liable for is further determined by the state in which the software was found at time of test.

Balancing Interests

A critical consideration in the creation of such a program is balancing the potential loss of means used to gather foreign intelligence with promoting a more robust overall software security posture. This sort of tradeoff is certainly not unique to this problem set. In his remarks to the House Intelligence Committee, Mr. Chris Inglis, Deputy Director of the NSA at the time, stated that "When we take our oath to the Constitution, it's to the whole of it, not just to the national security side of the Constitution. It's to the protection of civil liberties [and] U.S. persons." In this same vein, when considering the structure of a national bug bounty program, it cannot subordinate user security to governmental interests. There must be a trust-based relationship between the Intelligence Community and the governing bodies of SIERRA ensuring that any of the intelligence capabilities thwarted by patching bugs will be overcome through improved tradecraft. The US government must rely on more than secret, subversive avenues of exploitation and instead develop the robust set of capabilities expected of a world power.

Beyond these considerations on the side of US losses in the gathering of foreign intelligence, there are also tangible benefits from the other side of our adversaries ability to collect on US citizens. To this end, SIERRA helps to bolster the counter-intelligence posture of the US by proportionally patching more flaws that affect all its citizens. While there may be a slight drop in our ability to conduct intelligence operations, a much greater loss will be endured by nation-states wishing to exploit those flaws to deliver effects against the US and for their own financial gain.

Economics of the Exploit Market

The economics of the existing exploit market are of key consideration in the implementation of a national bug bounty program. The entire goal of SIERRA is to secure the software that US

economic and national security interests rely upon. To do so, SIERRA will have to incentivize citizens to "scour the Internet" for potential security vulnerabilities. At the very least, it must compel people to report vulnerabilities on which they have prior knowledge. The initial uptick in reported patches will serve to tighten-up the seaworthiness of our proverbial security vessel so that larger problems may be addressed. One consequence of this decrease in exploit availability will be a natural increase in cost. Additionally, the demand for undiscovered zero-day exploits will also rise. Both of these factors must be considered in reward calculation. There must exist a capability to monitor the exploit markets to guarantee that as a potential buyer, SIERRA is remaining competitive with the underground vulnerability marketplace.

Cyber Law: The Computer Fraud and Abuse Act

SIERRA aims to facilitate a bug bounty program with United States based corporations. The existing programs in place with organizations like Facebook, Google, and United Airlines all maintain compliance with the CFAA by virtue of the fact that companies give consent for individuals to investigate the security of their products and systems. The CFAA does not specify a single method by which companies can provide consent or give proper authorization for attempting to find vulnerabilities on their systems. However, courts maintain that such authorization must be "clear and conspicuous," meaning an adequately worded web interface or public announcement can serve as an express authorization by the company to participate in such a program.

Background: CFAA

The CFAA was signed in to law by Congress in 1986. Although amended several times since then, and with proposals to further extend the legislation, the CFAA may stand at a detriment to a federal policy governing bug bounty programs. President Obama, through the Modernizing Law Enforcement Authorities to Combat Cyber Crime plan, hopes to take harsher and more

efficient action on domestic cyber incidents. However, the current "provisions are sufficiently vague" that there is room for computer security researchers to be investigated and prosecuted for their work.

Moving Forward

One method to combat these provisions and provide protection for security researchers and white hat hackers is the expansion of the CFAA with specific wording to safeguard those attempting to improve on or hunt down vulnerabilities in software. The clauses that currently stand as a barrier to a bug bounty program are subsections (a)(2) and (a)(5). Title 18 U.S. Code § 1030 (a)(2) states that "whoever intentionally accesses a computer without authorization or exceeds authorized access" can be held liable for damages and be charged and punished with subsequent criminal charges. Section (a)(5) addresses the "transmission of a program, information, code, or command" resulting in unauthorized access of protected machines or damages to information systems. Language could be included as an addendum to the CFAA to legally absolve bug bounty hunters of the potential for criminal charges given that they follow the Responsible Disclosure Policy put forth by SIERRA. This would alleviate legal strain on individual companies, and provide a single point of policy should the need to enforce it ever arise.

The goal of the legal division within SIERRA is to create an environment in which contributors feel comfortable sharing information about security flaws and best-practices. It is critical to develop a policy by which corporations will not be liable to shareholders for exploits aimed at a vulnerability that is being addressed within a timeframe as determined by SIERRA. Additionally, SIERRA has the responsibility to ensure that registered researchers will not be penalized for the responsible disclosure of security flaws through SIERRA reporting channels.

Similar to Facebook's policy, SIERRA will maintain a Responsible Disclosure Policy on behalf of contributors as a first line of defense against litigation and investigation by law enforcement. Following in suit with the need for a clear and conspicuous authorization to proceed with

security testing, bounty hunters also must adhere to any additional policies put out by the organization governing the program. Aside from the intricacies of the technical requirements for a bounty to be paid, company disclosure policies enumerate the conditions on which the authorization to waive the CFAA protection stand during the reporting process. Critical elements that will be incorporated into SIERRA's policy include no further distribution or attempt to exploit a bug, and prioritization of disclosure to SIERRA over other zero-day or illicit marketplaces.

Conclusion

"External actors probe and scan [Department of Defense] networks for vulnerabilities millions of time each day, and over one hundred foreign intelligence agencies continually attempt to infiltrate DoD networks" (Rosenbach, 2015). No matter which way it is sliced -- hundreds of thousands per hour, trillions per year -- the Department of Defense is under constant siege. This barrage is not unique towards governmental entities, but rather something costing the global financial system upwards of $385 billion per year. When looking across the span of this hemering monetary cost, one of the most deleterious and dangerous avenues these attacks take is the exploitation of zero-day vulnerabilities. These are the key target of SIERRA as even with proper updates, maintenance, and a great team of cyber analysts constantly checking your network for integrity, these incognito vulnerabilities can offer a free pass to adversaires onto even the most robust infrastructures. Currently, these valuable tools of unauthorized access are most prized within the bellows of the Internet. Naturally, this is then the first place sellers will go with their product. SIERRA will bring this black market into the light and fundamentally undermine the economic structure it is rooted on by offering a greater incitive to researchers willing to disclose these vulnerabilities in a constructive manner rather than for ill-intent.

The aggressors in the cyber domain SIERRA will combat have a dangerously low barrier to entry and minuscule personal risk for participation. Furthermore, they can act with almost

complete impunity for careless actions in this new battlespace that extends beyond the boundaries of war into commerce, education, and healthcare—all sharing the same servers and lines of communication. Due to the expansive and interconnected nature of this problem, governmental efforts alone will not offer a complete solution. It will take a joint effort from the public and private sector in order to produce a solution that will make a lasting and decisive impact. SIERRA is a first step in the collaboration and will serve as the exemplary model for how the government can begin leveraging it most powerful resource to secure the cyber domain --its people. ■