The Bug Bounty Program Entails Better Payouts

Sharanya Sudhakar

March 2017

Abstract

Hacking is illegal, but hacking with an intent to report and not interfere is legal. This is the central idea of the bug bounty program. This program encourages laypersons to hack a company for security breaches thereby identifying them for the company. The company's programmers then swoop in to patch the bug with the provided report. This largely benefits the company, which then analyses the report, classifies it from low to high risk and grants a bounty. The bounty offered is often less than impeccable.

Cybercrimes arise from flaws in exiting software programs. A flaw or bug in the computer code is an unintended consequence of its development process (Kuehn and Mueller). A computer program specialist exploits this vulnerability to access crucial information largely for monetary remuneration. Companies outsource the handling of security glitches and the loopholes are fixed with software patches once found, but most security issues are left unidentified. In 2013, a major media frenzy put the big technology companies, like Microsoft, Oracle and Adobe, in the spotlight for their severe security weaknesses (Kuehn and Mueller). Consequently, they started offering incentives to the public for responsible disclosure of security breaches. This way of handling security breaching is popularly called, the bug bounty program. These bounties are sometimes fixed or varied depending on the severity of the bug discovered and the company offering the incentive (Stirland). The bug bounty program is gaining a reputation that combats cybercrime on a large scale, but the compensation offered falls short. **The bug bounty program should offer higher incentives to security researchers.**

White-hat hackers need a wage

Initially, software companies were afraid of using hackers to solve cyber security issues. The huge potential has made them reconsider their strategy (Burningham). Despite, digital bugs are not free and white-hat hackers, though well intentioned, also need compensations.

Security researcher Khalil Shreateh found a flaw in Facebook and alerted them. Initially, Facebook's bug-bounty team ignored the vulnerability, failing to acknowledge the bug twice (Kerner, “Facebook Vs. Hackers”). Until Shreateh publicly attacked the company CEO Zuckerberg's Facebook wall to demonstrate the vulnerability (Kerner, “Facebook Vs. Hackers”). In a study on cybersecurity, test results indicate that average-skilled hackers often with no chance of better payouts resort to malicious activities, whereas highly skilled hackers with a better probability of getting paid favor legitimate ones (Allodi et al.). In the case of Facebook, Shreateh proved to be highly professional, contrastingly some might find other buyers which might involve less favorable results.

Max Justicz, an MIT Junior, is a white hat hacker. He hacks systems for security breaches to report them and collect bounty, but sometimes for his trouble he gets just a T-shirt (Burningham). These bugs have no financial payoffs, and to the students and young adults, who depend on the financial benefits attached, they become deterrents.

HackerOne, a company that overseas bug bounty programs, runs a boy scouts program. This program helps channel kids’ curiosity and energy into something productive. One hacker in this program is a 14-year-old Philippines boy who uses the bounty to pay for his tuition (Burningham). The bug bounty program has introduced a new avenue for earning, and the paygrade should reflect this growing industry.

Crowd-sourcing employs a wider range of expertise

The bounty program, opened to the public, attracts a broader spectrum of researchers. To ensure continuous results it should attract experienced researchers, who expect to be paid appropriately for the work they do.

GitHub, a version control repository and hosting service, has run a bug bounty program since 2014. Greg Ose, GitHub's Application Security Engineering Manager, said that one reported bug stood out and helped define a major focus area in GitHub's security, where the reporter not only demonstrated the vulnerability but also detailed a bypass (Kerner, "GitHub Bug Bounty"). When researchers identify, and solve the problem, a higher reward system is essential.

Mark Litchfield, a security researcher and entrepreneur, discovered a vulnerability in the Defense Video Imagery Distribution System (DVIDS), at the invite of the Department of Defense (Stirland). The Department of Defense launched the "Hack the Pentagon" program to discover security vulnerabilities in its systems. Litchfield participated and discovered a bug that could enable a malicious minded hacker to access and transmit content from the DVIDS's website directly(Stirland). Mark Litchfield was paid the highest bounty of $15000 (Stirland), in contrast to the millions the department saved.

Defense Secretary Ash Carter said that more than 1,400 security experts applied for the "Hack the Pentagon" program (Lemos). Hiring the best security companies will still mean a smaller pool of experts at a higher price when compared to what the bug bounty program can attract. With cybercrime growing at an alarming rate, a higher workforce is tantamount to fighting it and to be fair it should also be a better funded workforce to provides consistent outcomes.

Paying for bounty is cheaper

Bounty is economical than paying for the security breach. Companies can increase their payouts without affecting their bottom-line, because a breach will mean millions to fix the ensuing problems.

A 2015 report on bounties and how they are disbursed revealed that a total of 729 high priority loopholes were discovered across 166 programs. Of which 175 were deemed critical and offered bounties ("The Rapid Growth"). The cost of closing 729 known breaches is only 175 critical ones, and any company will gladly make the transaction. Security researchers were paid on an average of one in every five submissions ("The Rapid Growth"). Paying for bounty does not affect the bottom-line, it just ensures better outcomes.

The average annual cost for 58 benchmarked organizations is $15 million per year ("2015 Cost of Cyber Crime Study"). In contrast, the average cost per company for a bug bounty program is at most $100,000 - $150,000 in a year. GitHub paid out a total of $81,700 in 2016 (Kerner, "GitHub Bug Bounty"). The Department of Defense's $150,000, "Hack the Pentagon", program resolved close to 140 security glitches when in fact it would have taken more than a million dollars to resolve them the traditional way (Stirland).

Ransomware is the next cyberthreat of 2016. This is where companies budget money to buy back breached data after a ransomware event (Tuttle). Companies may pay them most often without involving law enforcement to avoid disruption of their businesses and blemishes to their brands (Tuttle). In cases like this it will just be prudent to patch the bug than to pay for it. Using a bug bounty program might not only be the safest option it will also spread the notion that the company is actively fighting breaches and will therefore add considerable consumer loyalty and trust.

Conclusion

Cyber security is no longer a state, or national phenomenon, it is a global one and as such should have global costs attached. With better reward systems companies are indirectly encouraging more white-hat hackers. Consequently, average researchers can get gainfully employed which will reduce their chances of malicious activities. When more people are involved more breaches are identified. When security breaches are identified from many different directions, more knowledge is gained and can be applied at the development stage of a program. Which in turn could mean better programs with less bugs at the production stage.

[word count: 1117]

References

Allodi, Luca, Massacci, Fabio, and Woohyun Shim. “Crime Pays If You Are Just an Average Hacker”. *Cyber Security International Conference 2012,* 14-16 Dec. 2012, p. 62-68, IEEE doi: 10.1109/CyberSecurity.2012.15. Accessed 3 Mar. 2017

Burningham, Grant. "Bugs Money." *Newsweek Global*, vol. 166, no. 6, 12 Feb. 2016, pp. 48-50. EBSCO*host*, offcampus.lib.washington.edu/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=a9h&AN=112712547&site=ehost-live. Accessed 3 Mar. 2017

“2015 Cost of Cyber Crime Study: United States”. *Phenomenon Institute.* 9 Oct. 2015, http://www.ponemon.org/blog/2015-cost-of-cyber-crime-united-states. Accessed 4 Mar. 2017

Kerner, Sean Michael. "Facebook Vs. Hackers: Win One, Lose One." *Eweek*, 19 Aug. 2013, p. 3. EBSCO*host*, offcampus.lib.washington.edu/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=a9h&AN=89992385&site=ehost-live Accessed 4 Mar. 2017

---."Github Bug Bounty Program Offers Bonus Rewards." *Eweek*, 23 Jan. 2017, p. 1. EBSCO*host ,* offcampus.lib.washington.edu/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=a9h&AN=120941277&site=ehost-live. Accessed 4 Mar. 2017

Kuehn, Andreas and Milton Mueller. “Analyzing Bug Bounty Programs: An Institutional Perspective on the Economics of Software Vulnerabilities”. *2014 TPRC Conference Paper.* 1 Aug. 2014. SSRN: https://ssrn.com/abstract=2418812 Accessed 4 Mar. 2017

Lemos, Robert. "Pentagon Bug Bounty Contest Uncovers at Least 100 Vulnerabilities." Eweek, 15 June 2016, p. 12. EBSCO*host* offcampus.lib.washington.edu/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=a9h&AN=116206175&site=ehost-live Accessed 4 Mar. 2017

Stirland, Sara Lai. “How DOD Embraced Bug Bounties -- and How Your Agency can, too” *The Business of Federal Technology.* 24 Oct. 2016 https://fcw.com/Articles/2016/10/24/stirland-dod-bug-bounty-buy-in.aspx?Page=1 Accessed 4 Mar. 2017

“The Rapid Growth of the Bug Bounty Economy”. *HelpNet Security.* 3 Aug. 2015, https://www.helpnetsecurity.com/2015/08/03/the-rapid-growth-of-the-bug-bounty-economy/. Accessed 4 Mar. 2017

Tuttle, Hilary. “The 2017 Cyberrisk Landscape”. *Risk Management,* 64.1, Jan / Feb 2017, pp 4, 6-7, *ProQuest,* http://search.proquest.com/openview/66a5ce226326d505746eceea137dce99/1?pq-origsite=gscholar&cbl=47271. Accessed Mar 4. 2017.