HACKER-POWERED FACTS

Data from the HackerOne Hacker-Powered Security Report 2017

hackerone

INTRODUCTION

The Hacker-Powered Security Report examines the largest dataset of more than 800 hacker-powered security programs, compiles learnings from application security practitioners and the hackers who participate in bug bounty and vulnerability disclosure programs. The report also analyzed vulnerability disclosure data from the world's 2,000 biggest publicly traded companies according to Forbes. Consider this your "cheat sheet" of the top findings. You can also download the full 27-page report packed with key learnings, graphs, and links to other helpful resources at https://www.hackerone.com/resources/hacker-powered-security-report.

HACKER-POWERED FACTS

1. Over half of bug bounty programs launched in 2016 are for technology companies.
2. 41% of bug bounty programs launched on HackerOne in 2016 are from industries other than technology.
3. Governments, media and entertainment, financial services and banking, and ecommerce and retail industries all showed significant growth year over year.
4. Ecommerce and retail had the most significant adoption rates year-over-year.
5. Gaming adoption increase had the second-highest year-over-year industry growth.
6. **Publicly disclosed vulnerability reports continue to increase year-over-year. See www.hackerone.com/hacktivity**
7. Security response efficiency is improving: The average time to first response for security issues was 6 days in 2017, compared to 7 days in 2016.
8. Ecommerce and retail organizations fixed security issues in four weeks, the fastest on average.
9. Responsive programs attract top hackers. Programs that are the fastest at acknowledging, validating, and resolving submitted vulnerabilities are the most attractive to hackers.
10. Loyalty matters — repeat hackers are to thank for the majority of valid reports.
11. Bounty payments are increasing. The average bounty paid to hackers for a critical vulnerability was $1,923 in 2017, compared to $1,624 in 2015 — an increase of 16%.
12. The top performing bug bounty programs award hackers an average of $50,000 a month, with some paying nearly $900,000 a year.
13. Despite increased bug bounty program adoption and recommendations from federal agencies, 94% of the top publicly-traded companies still do not have known vulnerability disclosure policies — unchanged from 2015.
14. Security vulnerabilities worry companies the most. 73% of surveyed customers said they are concerned about unknown security vulnerabilities being exploited.
15. 52% of HackerOne customers cite customer data and intellectual property theft as top concerns.
16. HackerOne hackers have submitted over 210,000 reports.
17. HackerOne has received 95,000 valid vulnerabilities.
18. HackerOne has over 120,000 hackers in our community.

19. **HackerOne hackers have earned more than $18 million in bounties as of June 29, 2017.**

20. In all industries except for financial services and banking, cross-site scripting (XSS, CWE-79) was the most common vulnerability type discovered by hackers using the HackerOne platform.

21. For financial services and banking, the most common vulnerability was improper authentication (CWE-287).

22. Healthcare programs have a notably high percentage of SQL injection vulnerabilities (6%) compared to other industries.

23. Financial services are often targeted by criminals. In 2016 over 200 million records were compromised in the financial services sector — a 937% increase year over year.[1]

24. Cross-site scripting (XSS) is the #1 most-reported vulnerability in every industry from 2013 to 2017...except in Financial & Banking, which counts Improper Authentication as it's most-reported vulnerability.

25. Improper Authentication is the #2 most-reported vulnerability in every industry from 2013 to 2017...except in Financial & Banking, which counts XSS as it's #2 most-reported vulnerability.

26. XSS accounts for nearly half (47%) of all vulnerabilities reported in the Travel & Hospitality industry, far surpassing the share of XSS vulnerabilities in every other industry.

27. **The Healthcare industry sees double or triple the number of SQL Injection vulnerabilities of every other industry.**

28. The Gaming industry has "Information Disclosure" vulnerabilities reported more often than every other industry.

29. Ecommerce & Retail companies see more than triple the volume of Denial of Service vulnerabilities reported than every other industry.

30. Ecommerce & Retail companies see nearly four-times the volume of Memory Corruption vulnerabilities reported than every other industry.

31. **77% of all bug bounty programs have their first vulnerability reported within 24 hours.**

32. 99% of vulnerabilities exploited through 2020 will continue to be known by security and IT professionals for at least one year.[2]

33. Travel and hospitality businesses pay the fastest, 18 days after the report is submitted.

34. The food and beverage pays out bounties in 19 days on average.

35. 18% of customers pay when a vulnerability is validated.

36. 48% of customers pay when a vulnerability is resolved.

37. 34% of customers pay on a case-by-case basis.

38. Bug bounty programs on the HackerOne platform that reward $15,000 on average for critical vulnerabilities are in the top 1%.

39. 60% of organizations on the platform reward $1,000 on average for critical vulnerabilities.

40. Google Chrome steadily increased their top bounty from $3,000 to $100,000 over the course of more than five years.[3]

41. HackerOne awarded hackers over $7 million in 2016.

42. The highest amount paid for a single critical vulnerability on the platform was $30,000 by a technology company — an amount that has been awarded multiple times.

43. In the last year, gaming, ecommerce and retail, and media and entertainment programs each awarded a $20,000 bounty to hackers for a critical vulnerability.

44. **In the past 12 months, 88 individual bounties were over $10,000.**

45. The highest average payments for critical vulnerabilities come from transportation ($4,491), followed by gaming ($3,583).

46. Percentage breakdown of vulnerabilities by severity: Critical (9%), High (23%), Medium (36%), Low (28%), None (4%).

47. Through May 2017, the average bounty for a critical issue paid to hackers on the HackerOne Platform was $1,923.

48. For all vulnerabilities reported of any severity, the average bounty payout was $467.

49. Since 2014, hackers have donated nearly $100,000.

50. From January 1 through May 2017, hackers elected to donate $39,450 in bounties. The best customer programs match the donations made by the hackers.

51. Hackers have donated to Doctors Without Borders, UNICEF, the Electronic Frontier Foundation, and the Freedom of the Press Foundation.

52. **Hackers in India have been paid $1.8M, 17% of all bounties paid from April 2016 to April 2017.**

53. Hackers in the U.S. have been paid $2.4M, 23% of all bounties paid from April 2016 to April 2017.

54. Hackers in Australia were paid more than $1M in bounties from April 2016 to April 2017, making them the #3 destination for bounties paid.

55. Companies in the U.S. have paid out 80% of all global bounties—just under $7M—from April 2016 to April 2017.

56. Canadian companies are the #2 source of bounties paid, with 7.6% of the total paid from April 2016 to April 2017.

57. Companies in the Netherlands are the #3 source of bounties paid, with 1.9% of the total paid from April 2016 to April 2017.

58. Argentina is the only country in South America to pay bounties in the past year, yet they account for nearly 5% of global bounties paid.

59. Companies in Luxembourg, despite having a population of just 570,000, paid out more bounties than companies in Japan, Singapore, Switzerland, UAE, and Mexico combined.

60. The Netherlands, despite having a Gross Domestic Product that is just 7% that of China's, paid out nearly 10% more in bounties than China.

61. India, despite having a $150B-plus IT industry, paid out just $50—yes, fifty dollars—in bounties last year.

62. Companies in Switzerland paid out nearly 400% more bounties than hackers in the country collected in bounties.

63. Hackers in Sweden collected more than 25 times the amount of bounties than companies in the country paid out in bounties.

64. Three countries—Argentina, Pakistan, and Morocco—paid out zero in bounties, yet hackers in those countries collected a combined $1.15M in bounties.

65. Private bug bounty programs make up 88% of all bug bounty programs on HackerOne.

66. 92% of the bug bounty programs launched in 2016 were private.

67. The majority of public bug bounty programs are from technology (64%) followed by financial services and banking (11%) and media and entertainment (8%).

68. 100% of programs are private in the travel and hospitality, healthcare, insurance, aviation, and telecommunications industries.

69. **Public bug bounty programs resolve 4x as many vulnerabilities as private programs.**

70. HackerOne has the highestpublished Signal-To-Noise Ratio (SNR) in the industry.

71. Signal-To-Noise Ratio for public programs, 2017 YTD: 70% signal, 30% noise.

72. 94% of the Forbes Global 2000 do not have known vulnerability disclosure policies.

73. Nearly 200 organizations rely on the HackerOne platform for their VDP, including the The U.S. Department of Defense, LinkedIn, NewRelic and General Motors.

74. Panasonic is the only consumer electronics company with a public VDP on the Forbes Global 2000 list.

75. Five of 36 conglomerates, have vulnerability disclosure programs, including General Electric, Siemens, Honeywell International, ABB, and Philips.

76. Two out of 24 airlines, United Airlines and Lufthansa, have vulnerability disclosure policies.

77. Three out of 31 auto and truck manufacturers have policies. They are General Motors, Tesla and Fiat Chrysler Automobiles.

78. Starbucks is the only restaurant on the list with a vulnerability disclosure or bug bounty program.

79. 54% of the top software/programming companies have programs: Microsoft, Oracle, SAP, VMware, Adobe Systems, Symantec, Salesforce.com, and Intuit (13 of 24).

80. Three out of 20 consumer financial services, including Visa, MasterCard and PayPal have programs.

81. **Only 6 out of 64 Major Banks have vuln disclosure policies: JPMorgan Chase, Citigroup, ING Group, Danske Bank, Swedbank, Royal Bank of Scotland.**

82. The United States Department of Defense, Food and Drug Administration, National Highway Traffic Safety Administration, National Telecommunications and Information Administration, National Institute of Standards and Technology,and Federal Trade Commission all recommend companies have a vulnerability disclosure policy.

83. **95% of HackerOne customers said they'd**

recommend hacker-powered security to their peers at other companies.

84. 78% of HackerOne customers work with hackers to better protect their customers.
85. 72% of HackerOne customers say they work with hackers to protect their technology and brand.
86. 57% of HackerOne customers work with hackers because it's a security best practice.
87. 59% of HackerOne customers started a bug bounty program to give a boost to internal teams.
88. 58% of HackerOne customers run bug bounty programs to figure out where their tech is most vulnerable.
89. 47% of HackerOne customers wanted to create a structure for working with hackers.
90. 33% of HackerOne customers stated they're better equipped to improve their security development lifecycle.
91. The most common worry of HackerOne customers is security vulnerabilities being exploited (73%), followed by customer data and intellectual property theft (52%), and inherited security debt (42%).
92. Top personal security worries of HackerOne customers relating to connected devices, are: identity theft (68%), access to credit cards or bank details (64%), and access to personal details (63%).
93. HackerOne's 2016 Bug Bounty Report found that hacker motivations like enjoyment (70%), personal challenge (66%) and doing good in the world (51%) are about as common as the desire to make money (72%).
94. 17% of hackers on the HackerOne platform rely solely on bug bounty programs for their income.
95. **In 2016, the number of hackers on the HackerOne platform grew nearly 300%.**
96. Hackers hail from 90 countries, with the biggest groups coming from India and the United States.
97. 59% of hackers spend less than 20 hours per week hacking while 24% spend over 40 hours per week hacking.
98. 50% of hackers on HackerOne are under 24.
99. 77% of HackerOne customers think hackers hack for financial gain.
100. 57% of hackers say they participate in programs that didn't offer bounty payouts.

---

1. IBM X-Force Research: https://media.scmagazine.com/documents/296/2017_ibm_x-force-_security_tre_73846.pdf
2. Gartner: http://www.gartner.com/smarterwithgartner/top-10-security-predictions-2016/
3. https://www.google.com/about/appsecurity/chrome-rewards/

https://www.hackerone.com/resources/hacker-powered-security-report

#hackerpoweredfacts

hackerone

SALES@HACKERONE.COM