Bugcrowd Report: 71% of Hackers Believe AI Technologies Increase the Value of Hacking, Compared to Only 21% in 2023

Submitted by: Zonic Corporation Limited
Wednesday, 16 October 2024

Annual “Inside the Mind of a Hacker” 2024 report delivers an inside look at trends impacting the hacking community

SAN FRANCISCO, October 16, 2024 — Bugcrowd (https://www.bugcrowd.com/), the leader in crowdsourced cybersecurity, today released its annual Inside the Mind of a Hacker 2024 report, which analyzed responses from 1,300 hackers, also known as ethical hackers and security researchers on the Bugcrowd Platform. This report provides a comprehensive overview of the hacking community and their perspectives on topics at the forefront of cybersecurity.

AI adoption and integration has continued its rapid momentum within the hacking community. Nevertheless, it continues to pose both benefits and unfortunate cyber risks. According to the report, 82% of hackers believe that the AI threat landscape is evolving too fast to adequately secure.

AI is the new attack vector

This year's report revealed a significant shift in the perceived value of AI in hacking compared to the previous year. While only 21% of hackers believed that AI technologies enhance the value of hacking in 2023, 71% reported it to have value in 2024. Additionally, hackers are increasingly using generative AI solutions, with 77% now reporting the adoption of such tools—a 13% increase from 2023.

While the use and value of AI solutions among hackers have increased, the 2024 report reaffirms that hackers believe AI has limitations. This year's survey revealed that only 22% of hackers believe that AI technologies outperform human hackers, and only 30% believe that AI can replicate human creativity. These results are consistent with those of the 2023 survey.

“There is no denying that AI remains a strong force within the hacking community, changing the very strategies hackers are using to find and report vulnerabilities,” says Dave Gerry, CEO of Bugcrowd. “Bugcrowd is in a privileged position to work with a creative, forward-thinking community that thrives on the cutting edge of cybersecurity. Celebrating hackers is part of the core of what we do at Bugcrowd, and these insights can help businesses understand the unique value this community brings to fighting against today’s AI-driven cyberattacks.”

Key findings from the survey include the following:

• 93% of hackers agree that companies using AI tools have created a new attack vector
• 82% believe that the AI threat landscape is evolving too rapidly to be effectively secured from cyberattacks
• 86% believe that AI has fundamentally changed their approach to hacking
• 74% agree that AI has made hacking more accessible, opening the door for newcomers to join the fold
• Despite these threats, 73% of hackers reported being confident in their ability to uncover vulnerabilities in AI-powered apps

These findings point towards the need for hackers in an organization’s defense against today’s cyberattacks. Although AI is introducing a new attack vector, the majority of hackers still report confidence in their ability to uncover these vulnerabilities, emphasizing the need for organizations to lean on human ingenuity alongside security tooling.

The Rise of Hardware Hacking

The report illuminated the rise of a surprising trend: the increasing prominence of hardware hacking. In the past 12 months, 81% of hardware hackers encountered a new vulnerability they had never seen before, and 64% believe that there are more vulnerabilities now than a year ago. Additionally, in response to the rise of AI, 83% of hardware hackers are now confident in their ability to hack AI-powered hardware and software, indicating a new potential avenue for exploitation. While those familiar with the field may recognize this growing threat, only 33% of hackers in general identified hardware hacking as one of the most valuable specialties. However, there is a low barrier to entry, with 80% of hardware hackers being self-taught.

“Hardware hacking, or the exploitation of vulnerabilities in the physical components of electronic devices, was once considered a specialized field,” says Michael Skelton, VP of Security Operations at Bugcrowd. “However, the proliferation of inexpensive, vulnerable smart devices has increased interest in hardware hacking among both ethical hackers and cybercriminals.”

A Career Path for a New Generation

This year’s survey results also emphasized hacking as a viable and strong career path, particularly for younger generations. Of the respondents, 88% were between the ages of 18 and 34. Additionally, 67% indicated that they are either hacking full-time or actively trying to pursue a full-time hacking career.

Additionally, hacking offers a career path for self-motivated individuals who are eager to learn new skills. While 73% of respondents reported having a college degree or higher, only 29% learned their hacking skills through academic or professional coursework. Instead, 87% reported learning through online resources, 78% through self-study, and 43% through trial and error. Hacking offers younger generations an incredibly desirable career with flexible hours, a remote work environment, and without the requirement of a college degree to achieve success.

Access the Full Report

The survey included 1,300 respondents from 85 countries, including the United States, India, Bangladesh, Pakistan, Nepal, Egypt, Nigeria, the United Kingdom, Vietnam, and Australia. Building upon the success of previous years, this year’s edition offers the latest demographic data on the hacking community, a detailed analysis of hackers' daily experiences, and direct insights into hackers’ journeys through extensive "Hacker Spotlight" interviews. Readers of this report will better understand how hackers can reduce risks for organizations, provide one of the most significant security returns on investment, and accelerate digital transformation. To download a copy of the Inside the Mind of a Hacker 2024 report,

click here (https://ww1.bugcrowd.com/inside-the-mind-of-a-hacker-2024/).

About Bugcrowd

We are Bugcrowd. Since 2012, we've been empowering organizations to take back control and stay ahead of threat actors by uniting the collective ingenuity and expertise of our customers and trusted alliance of elite hackers, with our patented data and AI-powered Security Knowledge Platform™. Our network of hackers brings diverse expertise to uncover hidden weaknesses, adapting swiftly to evolving threats, even against zero-day exploits. With unmatched scalability and adaptability, our data and AI-driven CrowdMatch™ technology in our platform finds the perfect talent for your unique fight. We are creating a new era of modern crowdsourced security that outpaces threat actors.

Unleash the ingenuity of the hacker community with Bugcrowd, visit www.bugcrowd.com (www.bugcrowd.com). Read our blog (https://www.bugcrowd.com/blog/).

PR Contact
Krison Thakkar
KThakkar@ZonicGroup.com