Bugcrowd Releases 2020 Inside The Mind Of A Hacker Report

Published on 23 Jun 2020

Bugcrowd, the crowdsourced security company, released its 2020 Inside the Mind of a Hacker report, the study to date on the global hacking community.

Among the report’s key findings, human ingenuity supported by actionable intelligence of the Bugcrowd platform were found to be critical ingredients to maintaining a resilient infrastructure.

**AI-powered solutions not enough**

In fact, 78% of hackers indicated AI-powered cybersecurity solutions alone aren’t enough to outmaneuver cyber attacks over the next decade. Nearly nine out of 10 hackers, 87%, say that scanners cannot find as many critical or unknown assets as humans.
Hackers can adapt four to five low-impact bugs to exploit a single high-impact attack

While 2019 was a record year for data breaches, the report found that hackers working on the Bugcrowd platform prevented $8.9B of cybercrime in 2019 and earned 38% more than they did in the previous period. In the next few years, hackers on the Bugcrowd platform are projected to prevent more than $55 billion in cybercrime for organisations worldwide.

“Globally-distributed good-faith hackers are increasing in number and diversifying. Bugcrowd gives organisations the power to proactively leverage human ingenuity – the enabler of malicious cyberattacks – at-scale to prevent them,” said Casey Ellis, founder, chairman, and CTO of Bugcrowd. “While AI has a role to play in helping to reduce cyber risk, companies need to integrate crowdsourced security throughout their security lifecycle if they hope to outsmart and outmanoeuvre cybercriminals.”

Limitations of machine intelligence

Hacking as a profession is lucrative and highly attractive to young people

“Hackers will always be one step ahead of AI when it comes to cybersecurity because humans are not confined by the logical limitations of machine intelligence,” said Jasmin Landry, Bugcrowd hacker. “For example, hackers can adapt four to five low-impact bugs to exploit a single high-impact attack vector that AI would likely miss without the creative flexibility of human decision-making. Experience allows hackers to recognize vulnerable misconfigurations that represent a true risk to organizations without all of the false positives that typically come with AI-powered solutions.”

Nearly half of neurodiverse hackers (6%) experience Attention-Deficit/Hyperactivity Disorder (AD/HD)

In addition, the report incorporates data from 1,549 programs and 7.7 million platform interactions to provide a striking and in-depth view of emerging trends among Bug Bounty, Penetration Testing, Attack Surface Management, and Vulnerability Disclosure Programs.

Younger and neurologically diverse hackers

Hacking as a profession is lucrative and highly attractive to young people, with 53% of hackers under the age of 24. Remarkably, the report uncovered that 13% of hackers are neurodiverse and possess neurological advantages that help them provide extraordinary depth and dimension in security testing.

Research found that hackers live on six continents and reside in more than 100 countries worldwide.

These unique strengths include exceptional memory skills, heightened perception, a precise eye for detail, and an enhanced understanding of systems.

Nearly half of neurodiverse hackers (6%) experience Attention-Deficit/Hyperactivity Disorder (AD/HD) and thrive in environments of rapid change, such as security research, where creativity and out-of-the-box thinking are rewarded generously.

Career Hacking in Emerging Countries Skyrockets

The research found that hackers live on six continents and reside in more than 100 countries worldwide. Most notably, the report identified an 83% growth in respondents living in India and nearly three out of four hackers (73%) speak two or more languages.
93% of hackers primarily hack out of care for the well-being of the organisations with which they work

Bugcrowd uncovered a growing social responsibility trend among businesses and hackers. 93% of hackers primarily hack out of care for the well-being of the organizations with which they work. Additionally, organizations made five-times the number of coordinated disclosures in the last twelve months.

“The exponential growth of these disclosures highlights the value of transparency to stakeholders and demonstrates organisations are taking social responsibility more seriously than ever,” said Ellis.

**COVID-19 pandemic Increasing demand for career hackers**

The FBI reported a 400% rise in cybercrime after COVID-19 was declared a pandemic and organizations are investing more in bug bounty programs as a result. More than half of hackers (61%) have noticed an increase in available bug bounty programs to participate in due to widespread remote working conditions related to the COVID-19.

Hackers (48%) believe the Healthcare industry is vulnerable to cybercrime during the unfolding crisis

“We are in unprecedented territory – and COVID-19 has forced many businesses to accelerate digital transformation efforts,” said Ashish Gupta, CEO and president of Bugcrowd. “The rush to digitize businesses can create serious lapses in security and organizations are turning to bug bounty programs to proactively safeguard new products and applications against vulnerabilities.”

**Alternative polling methods not favored by hackers**
Like the larger security industry, career hackers also noted concerns about COVID-related fraud. Nearly half of hackers (48%) believe the Healthcare industry is vulnerable to cybercrime during the unfolding crisis, followed by Education and Community Support (17%) and Government and Military (16%).

Additionally, as the government faces the potential impact of COVID-19 on the upcoming 2020 US Presidential election, 72% of hackers independently reported that they do not trust alternative polling methods, like electronic polling or mail-in ballots.
You may also be interested in...

**The Role Of Building Systems To Ensure Safety As Employees Return To Work...**

Returning to work after the global pandemic will not be business as usual, and security systems are an important asset when it comes to help...

**Map Illustrates Usage Of Facial Recognition Around The World**

Governments around the world use facial recognition for applications such as identifying persons on public video feeds. The technology is al...

**4 Ways To Keep Your Workplace Protected From COVID-19**

The unprecedented global impact of COVID-19 has taken its toll on all of us, but as cases of the virus thankfully recede, employers are now...

**Automatic Gates: Making The Right Investment For Access Control**

The experience of the COVID-19 pandemic has made us all more conscious of who is coming and going from our property. Whether it is a family...