Hacker-Powered Security: The Hacker Community

January 20, 2020
The global leader in hacker-powered security

1,600+ customers
600,000+ hackers
141,000+ valid reports
$74 million+ bounties paid

$110m in funding
What Is A Hacker and Who Are They?
What do people think about hackers?
What do hackers look like?
Aka “Security Researchers”, “Finders”

HACK’ER

/ˈhaːkər/
noun
One who enjoys the intellectual challenge of creatively overcoming limitations.
Criminals Steal, Hackers Help

Most people have good intentions and they just want to help. Let them. There are those who just want to “watch the world burn” and those who want to help.
<table>
<thead>
<tr>
<th>Motivation</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>To Make Money</td>
<td>14.3%</td>
</tr>
<tr>
<td>To Learn Tips and Techniques</td>
<td>14.3%</td>
</tr>
<tr>
<td>To Be Challenged</td>
<td>13.5%</td>
</tr>
<tr>
<td>To Have Fun</td>
<td>13.5%</td>
</tr>
<tr>
<td>To Advance My Career</td>
<td>12.7%</td>
</tr>
<tr>
<td>To Protect and Defend</td>
<td>9.9%</td>
</tr>
<tr>
<td>To Do Good in the World</td>
<td>9.3%</td>
</tr>
<tr>
<td>To Help Others</td>
<td>8.3%</td>
</tr>
<tr>
<td>To Show Off</td>
<td>2.7%</td>
</tr>
<tr>
<td>Other</td>
<td>1.5%</td>
</tr>
</tbody>
</table>
TRENDS IN HACKER EDUCATION

- None: 8.8%
- Continuing Education: 15.2%
- High School: 23.3%
- Graduate School: 19.4%
- Undergraduate School: 33.3%
Reactions To Hackers

In Your Opinion, Over the Last Year, What Best Describes Companies' Reactions to Receiving Vulnerability Reports From Security Researchers?

- They are far more open: 33.8%
- They are somewhat more open: 38.4%
- They are neither more nor less open: 16.5%
- They are somewhat less open: 4.7%
What do hackers value more than anything?

Respect

Best way for you to show respect is by being responsive and having empathy. Assume good intent. Don’t take unreasonable punitive actions against finders, like making legal threats or referring matters to law enforcement. Suppress the urge for a cease and desist letter.
Hacker Vetting

Reputation Scoring
Internal scoring based on validity and severity of submissions and platform activity
- Signal
- Impact
- Reputation

HackerOne VPN
Engage hackers, assign access, and monitor activity with HackerOne VPN
- Test assets not available to the public internet
- Authorize individual researchers to access specific assets

HackerOne Clearance
Work exclusively with vetted hackers who meet your precise specifications
- Background checked and ID verified
- Proven performance and clear track record

HackerOne Custom Contracts
Easily insert custom language into researcher agreements and be compliant with your regulatory and internal requirements
- Use custom contract language specific for your business
- Enable simple click through e-sign researcher agreements
Companies working with hackers

... so is the government...
Hackers and Social Media
Hackers love twitter

@MorningstarInc I would like to report a security vulnerability to you, having trouble finding a contact.

@Cisco @CiscoSecurity tried to report possible security vulnerability with SPA phones. Told to buy a service contract to do so. Unbelievable

@24hourfitness Do you guys have a security vulnerability disclosure program? I'd like to report a few things.
What an organization should do before that

- Ideally set up an ISO standard 29147 compliant vulnerability disclosure policy. Or second best thing would be to get a security@ email address setup ... if that’s out of reach then your stuck with personal email or twitter DMs or homing pigeons.
- Regardless, create a response playbook with verbiage approved by Marketing and Legal
Step #1: Don’t assume evil

If determined that this person is acting in good faith do the following:

- **Follow your playbook** of responses. Likely reply on twitter with instructions on where to continue the dialogue.
- **Work the problem**, talk to the hacker
- **Close the loop** with them (but I would recommend you do NOT reply back on the post on social, it will just loop into the social platforms algorithms and give the tweet more air, could bring a story back to life). Ideally you respond right away.
- **Triage / validate / remediate**. All the while continue to have a consistent conversation with the hacker - keeping them posted of your progress. They will appreciate that.
- If you have a private bug bounty program, you could invite them and **reward them** for their efforts.
Step #2: Don’t assume evil
(but if the shoe fits)

If determined that this person is acting in a malicious manner, do the following:

- This is tough because it’s always a case by case situation. My broad suggestions are (and these are just my suggestions mind you)...
- First thing: forward to your legal counsel and loop in comms/pr. If you’re technical then assess the claims, if you’re not technical your security team needs to assess the merits.
- Attempt to DM and if no reply (which is probably unlikely) contact in other ways if through your OSINT. You want to establish a conversation and do so in a coordinated way.
The hacker within

- Many of you in this room may consider yourself a hacker. I’ll wager that several of your CIOs or technical teams hack (or children of your friends....)
So how can you advocate for security researchers?

- Tell other hackers stories - spread the word to your workplace, your IT and Security teams
- Read the Hacker Report and Share the Hacker Report with people 😊
Empower the World to Build a Safer Internet.