Apple pays hackers six figures to find bugs in its software. Then it sits on their findings.

Lack of communication, confusion about payments and long delays have security researchers fed up with Apple's bug bounty program

Reed Albergotti September 9, 2021 at 7:53 a.m. EDT

(The Washington Post; iStock)

Hoping to discover hidden weaknesses, Apple for five years now has invited hackers to break into its services and its iconic phones and laptops, offering up to $1 million to learn of its most serious security flaws.

Across the tech industry, similar "bug bounty" programs have become a prized tool in maintaining security — a way to find vulnerabilities and encourage hackers to report them rather than abuse them.

But many who are familiar with the program say Apple is slow to fix reported bugs and does not always pay hackers what they believe they're owed. Ultimately, they say, Apple's insular culture has hurt the program and created a blind spot on security.

"It's a bug bounty program where the house always wins," said Katie Moussouris, CEO and founder of Luta Security, which worked with the Defense Department to set up its first bug bounty program. She said Apple's bad reputation in the security industry will lead to "less secure products for their customers and more cost down the line."

Apple said its program, launched in 2016, is a work in progress. Until 2019, the program was not officially opened to the public, although researchers say the program was never exclusive.

"The Apple Security Bounty program has been a runaway success," Ivan Krstic, head of Apple Security Engineering and Architecture, said in an emailed statement. Apple has nearly doubled the amount it has paid in bug bounties this year compared to last, and it leads the industry in the average amount paid per bounty, he said.

"We are working hard to scale the program during its dramatic growth, and we will continue to offer top rewards to security researchers working with us side by side to protect our users and their data on more than a billion Apple devices around the world," he added.

In interviews with more than two dozen security researchers, some of whom spoke on the condition of anonymity because of nondisclosure agreements, the approaches taken by Apple's rivals were held up for comparison. Facebook, Microsoft and Google publicize their programs

and highlight security researchers who receive bounties in blog posts and leader boards. They hold conferences and provide resources to encourage a broad international audience to participate.

And most of them pay more money each year than Apple, which is at times the world's most valuable company. Microsoft paid $13.6 million in the 12-month period beginning July 2020. Google paid $6.7 million in 2020. Apple spent $3.7 million last year, Krstic said in his statement. He said that number is likely to increase this year.

Payment amounts aren't the only measure of success, however. The best programs support open conversations between the hackers and the companies. Apple, already known for being tight-lipped, limits communication and feedback on why it chooses to pay or not pay for a bug, according to security researchers who have submitted bugs to the bounty program and a former employee who spoke on the condition of anonymity because of a nondisclosure agreement.

Apple also has a massive backlog of bugs that it hasn't fixed, according to the former employee and a current employee, who also spoke on the condition of anonymity because of an NDA.

"You have to have a healthy internal bug fixing mechanism before you can attempt to have a healthy bug vulnerability disclosure program," said Moussouris, who helped create Microsoft's bug bounty program. She says she asks prospective clients, "What do you expect is going to happen if they report a bug that you already knew about but haven't fixed? Or if they report something that takes you 500 days to fix it?"

The unfriendly nature of its bug bounty program has discouraged some security researchers from pointing out flaws to Apple, these people said. That's prompted some to sell them to "gray market" customers like government agencies or companies that sell sophisticated hacking services, or go public without notifying Apple, which could put customers

at risk.

Cedric Owens, 39, earlier this year chose to tell Apple when he found a massive flaw that allowed hackers to install malicious software on Mac computers, bypassing Apple's security measures. Patrick Wardle, an expert in Mac security, said in a blog post that the vulnerability put Mac users "at grave risk." And Jamf, a cybersecurity firm, said it found evidence that hackers were already using it.

Apple's bug bounty program offers $100,000 for attacks that gain "unauthorized access to sensitive data." Apple defines sensitive data as access to contacts, mail, messages, notes, photos or location data. While Owens's hack didn't allow access to those specific areas, Owens and others in the industry argued that the data hackers were getting was, indeed, sensitive. Owens created a hypothetical attack that gave hackers access to the victim's files. He said in an interview that it could have hypothetically allowed hackers to access corporate servers, if the target computer were used by a corporation. That would be valuable in use for ransomware attacks, for instance.

Apple paid the Charlotte-based security researcher $5,000, or 5 percent of what Owens believed he deserved, he said. Apple declined to reconsider. While he said he will continue to submit bugs despite a higher payout on the gray market, other researchers probably won't. Apple declined to comment on Owens's bug bounty.

"The end result could be more gaping holes in Apple's processes and in their products they're releasing," he said.

Apple's Krstic said the company has gathered feedback and would "continue to scale and improve" what it said was a rapidly growing program, reducing response times and improving communication.

"We are also planning to introduce new rewards for researchers to keep

expanding participation in the program, and we are continuing to investigate paths to offer new and even better research tools that meet our rigorous, industry-leading platform security model," he added.

Despite the hype, iPhone security no match for NSO spyware

The security of Apple products, particularly iPhones, has come under more scrutiny after revelations this summer by the Pegasus Project, an investigation by The Washington Post and 16 other media organizations that showed how software licensed by the Israeli company NSO Group had been used to hack phones belonging to human rights advocates, journalists and politicians. The investigation uncovered forensic evidence of successful or attempted hacks on 34 iPhones, including the latest models with the latest updates.

"Apple unequivocally condemns cyberattacks against journalists, human rights activists, and others seeking to make the world a better place," Krstic said in a statement at the time.

Krstic pushed for Apple's program to be implemented in 2016, when select researchers were allowed to submit bugs in exchange for payment. In 2019, Apple opened the program to all researchers and announced that it would begin paying up to $1 million to anyone who could hack an iPhone remotely, without requiring the target to do anything (many hacks require clicking on a link or email).

It also announced it would provide "security research devices" — special iPhones designed for security research — to people who have a proven track record of finding bugs.

Apple declined to say how many of the devices it has given to researchers or whether it has paid a $1 million bounty.

Jeff Bezos's iPhone had Apple's state-of-the-art security, and that may

have helped its alleged hackers

Sam Curry, a prominent 21-year-old security researcher in Omaha, set his sights on Apple's bug bounty program last summer. He and four friends got together for late-night, soda-fueled hacking sessions, poking holes in Apple's defenses. The group submitted a new bug every couple of days. Apple paid $50,000 for one of the bugs, and, in all, they earned about $500,000, Curry said.

The group was so successful, collecting at least 13 percent of what Apple paid in bug bounties over the course of the year, that Apple took notice, Curry said. He had conversations with some of the security researchers at the company. He said the time it takes Apple to pay researchers for bug bounties is too long compared with the rest of the industry.

"I think they're aware of how they're seen in the community, and they're trying to move forward," Curry said.

On the list: Ten prime ministers, three presidents and a king

Apple, according to some of the people, hired a new leader for its bug bounty program this year with the goal of reforming it. Apple declined to make the person, who works under Krstic, available for an interview.

In the endless and messy global war over Internet security, even the most vigilant companies have seen their defenses fall at the hands of nameless and faceless foes. Apple is no exception. This year alone, Apple has patched 13 zero-day exploits, or previously unknown security vulnerabilities, that could have been used by malicious hackers to breach its devices.

Nevertheless, Apple is considered a leader in cybersecurity and has implemented advanced techniques, such as specialized microprocessors in iPhones devoted to stopping hacks. IPhones are often compared

favorably to competing handsets running Google's Android, including in Apple's advertisements.

The security of iPhones is one of Apple's key marketing claims. One company advertisement around 2017 depicted a burglar easily breaking into the "competing" mobile operating system and then being locked out of iOS.

The FBI wanted to unlock the San Bernardino shooter's iPhone. It turned to a little-known Australian firm.

But there is one aspect of cybersecurity that doesn't mix with Apple's cultural DNA. The field of cybersecurity grew out of a hacker culture in which the open and free flow of information is among the most important values.

The open nature of the cybersecurity industry contrasts with Apple's corporate culture. The company, like its competitors, prefers to keep its products secret until they're released. The methods Apple uses to ensure secrecy are more stringent than those employed by its peers. For instance, Apple employees are told not to discuss their work even with co-workers.

"It's not a surprise they haven't embraced this public security researcher culture until recently, when their hand was forced into launching a bug bounty program," said Jay Kaplan, a founder and the chief executive of Synack, which helps companies crowdsource vulnerabilities in critical technology. Kaplan said researchers weren't coming to Apple to report bugs. "Instead, they were going to security conferences and speaking about it publicly and selling it on the black market," he said.

Indeed, some researchers think Apple would prefer not to see its software picked apart by researchers, even if the result is that more flaws are fixed. Apple makes it as difficult as possible for researchers to remove software

protections that limit the kinds of research that can be conducted on iPhones. According to the current and former security employees, the company's view is that such protections make its phones more secure.

Apple is appealing its loss in a federal copyright lawsuit against a small Florida company called Corellium that makes a tool that allows researchers more easily to search for flaws in iPhone software.

Google uncovers 2-year iPhone hack that was 'sustained' and 'indiscriminate'

Tian Zhang, an iOS software engineer, first reported a bug to Apple in 2017. After months of waiting for Apple to fix the bug, Zhang lost patience and decided to blog about his discovery. The second time he reported a security flaw, he says, Apple fixed it but ignored him. In July, Zhang submitted another bug to Apple that he says was eligible for a reward. The software was quickly fixed, but Zhang didn't receive a reward. Instead, he was kicked out of the Apple Developer Program. Membership in the program is required to be able to submit apps to the App Store. Apple did not comment on Zhang's allegations.

"It's a mixed feeling," Zhang said in an interview. "On one side, as an engineer, you want to make sure the products you're building are safe for other people," he said. On the other hand, he says, "it seems like Apple thinks people reporting bugs are annoying and they want to discourage people from doing so."

Alex Rice, chief technology officer and co-founder of HackerOne, which provides bug bounty services to companies, said it can take time to fix bugs in more complicated software systems but that it is important to educate researchers on why it is taking so long. "It takes a little bit of good faith. And it takes a little bit of transparency and collaboration," he said. Still, "faster is always better."

Despite Apple's bounty program, there continues to be a big market for vulnerabilities on Apple devices. Researchers can sell exploits for iPhones for as much as $2 million, according to a price list published by Zerodium, a company that buys and sells exploits for use by firms such as NSO Group. The same kind of exploit for Google's Android operating system goes for $2.5 million.

People who have sold exploits to companies like Zerodium told The Post that they view the price list as a rough proxy of how difficult it is to find an exploit. The higher the price, the more secure the operating system. But there is no objective way to measure or compare iOS security to Android, in part because the people buying and selling the exploits keep that information secret. Zerodium, which says on its website that it sells to government agencies, mainly in Europe and North America, did not respond to a request for comment.

The Wayback Machine, a service run by the Internet Archive, which saves old webpages, shows how quickly the difficulty of hacking Android devices increased in five years. In 2016, Zerodium would pay only $200,000 for the most valuable exploit.

Dave Aitel, a former National Security Agency research scientist and co-author of "The Hacker's Handbook," said Apple's closed-off approach hinders its security efforts.

"Having a good relationship with the security community gives you a strategic vision that goes beyond your product cycle. It lets you know what's coming down the pike," he said. "Hiring a bunch of smart people only gets you so far."

Apple is prying into iPhones to find sexual predators, but privacy activists worry governments could weaponize the feature

Some of Apple's poor reputation in the bug bounty world could be

improved with some minor changes, according to experts in the field.

Casey Ellis, founder of Bugcrowd, an Australian firm that operates bug bounty programs for companies, said one "core rule" in the industry is that if a company changes its code in response to a bug report, it should pay the person who reports it, even if it doesn't meet the company's strict interpretation of the guidelines.

"The more good faith that goes on, the more productive bounty programs are going to be," he said.

Other big Silicon Valley companies have worked for years to earn favor in the research world. Facebook and Google co-host a conference called BountyCon, which is aimed at bringing security researchers with different skills together to collaborate and identify talent through the two companies' bug bounty programs.

Nicolas Brunner was developing an app for the Swiss Federal Railways last year that would help blind people navigate the train system. While testing the app, Brunner noticed that even if users declined to share their location, he could still see their every move.

Brunner had stumbled upon a serious security bug in Apple's location tracking system, he said in an interview. A colleague recommended he submit it to Apple's bug bounty program.

Expecting to be paid somewhere around $50,000, Brunner told his 30 colleagues that when he received his check, he would throw a barbecue for all of them. Apple thanked him for reporting the bug and said it would credit him with finding it. But eight months later, Apple responded to Brunner with disappointing news: His bug did not qualify for the program, despite Apple's promising rewards ranging from roughly $25,000 to $100,000 for flaws that allow access to "sensitive data," including "real-time or precise location data." After months of delays, Apple decided not

to pay him at all, saying the bug he had found did not qualify for the program.

“I like the idea of Apple’s bug bounty program. I don’t like the implementation,” Brunner said in an interview.

“When we make mistakes, we work hard to correct them quickly, and learn from them to rapidly improve the program,” Krstic said in the statement when asked to comment on Brunner’s case.