Is the iDefense challenge worth it?

The vulnerability experts at iDefense Labs challenged hackers to poke holes in Microsoft products by March 31 in exchange for an unprecedented public reward that has some in the industry raising their eyebrows.

Ericka Chickowski

The company, a division of VeriSign, offered a $10,000 prize for a first-time flaw discovery as a part of the its newly-introduced quarterly hacking challenge. Announced last week, this first quarterly challenge is to find flaws in Microsoft products that lead to a critical bulletin being released by the Redmond, Wash.-based company. It is part of iDefense's nearly four-year-old Vulnerability Contributor Program (VCP), which pays anonymous researchers for their vulnerability finds.

"We pay people directly for their submissions, and then we also have various programs to reward our loyal contributors and keep them working with us," said Michael Sutton, director of iDefense Labs. "This is our latest effort to further reward them."

The quarterly challenge was developed as a way to direct iDefense contributors toward research it believes will most benefit its customers, Sutton said, explaining that contributors who submit flaws that generate a critical bulletin from Microsoft will be paid the $10,000 reward on top of their normal payments.

"Keep in mind these aren't employees, so I don't have the power to task them with something," Sutton said, "all I have the power to do is incentivize them."

Predictably, Microsoft representatives openly criticized the new challenge. The company has never backed programs such as VCP that offer money to hackers. This stance didn't change with the announcement of a challenge that specifically targets its products.

"Microsoft works closely with many security research and security software companies and does not believe that offering compensation for vulnerability information is the best way they can help protect their customers," a Microsoft spokesperson said in a prepared statement. "Microsoft believes that responsible disclosure, which involves making sure that an update is available from software vendors the same day the vulnerability is first broadly known, is the best way to protect the end user."

According to Sutton, however, this latest challenge is the optimal way to help its customers using Microsoft products to plug critical vulnerability holes.

"Our clients have made it clear to us that critical Microsoft vulnerabilities are at the top of their lists," he said. "In the end, I really feel that we are benefiting the users of Microsoft software, and we're benefiting Microsoft because we're helping to find vulnerabilities, we're reporting (those vulnerabilities) to them and we're picking up the tab."

But others in the industry wondered at how helpful iDefense's policy of paying for vulnerability information really is, saying that this latest reward is less about security than it is about marketing.

"My initial reaction is that I think it sounds like a publicity stunt to me," said Caleb Sima, chief technology officer at SPI Dynamics, a web application security firm. "I don't think this is something bad that iDefense is doing, I know they are a good company, but I just don't see a lot of value in it."

At best, Sima said, finding a one-time Microsoft vulnerability flaw isn't going to put a dent in the security issues that the community faces. Not only that, according to him, the program only encourages a "bartering system" with hackers whose stakes will only increase as time goes on. And at worst, this quarterly challenge will only overburden those scrambling to stay on top of the latest vulnerabilities made public, he said.

"We've got enough vulnerabilities to deal with. Why do we need more?" Sima said. "What ends up happening is Microsoft immediately issues a patch, and then people are going to decompile the patch, find the exploit and then immediately start exploiting it. Sometimes zero day should stay zero day for a reason."

Sutton disagreed, "People talk about zero day, we're preventing zero day because we're making sure that when an issue becomes public there is a patch available for that and we work with the vendor to coordinate on that disclosure."

He said that in spite of criticisms from different camps, he remains confident in what iDefense is doing with its latest reward program.

"With any initiative that strays from the norm there's always going to be people who believe in it and people that don't believe in it," Sutton said, "As a company, we have demonstrated that we are willing to be leading edge, we're willing to take chances to further our efforts and benefit our clients and the community at large."