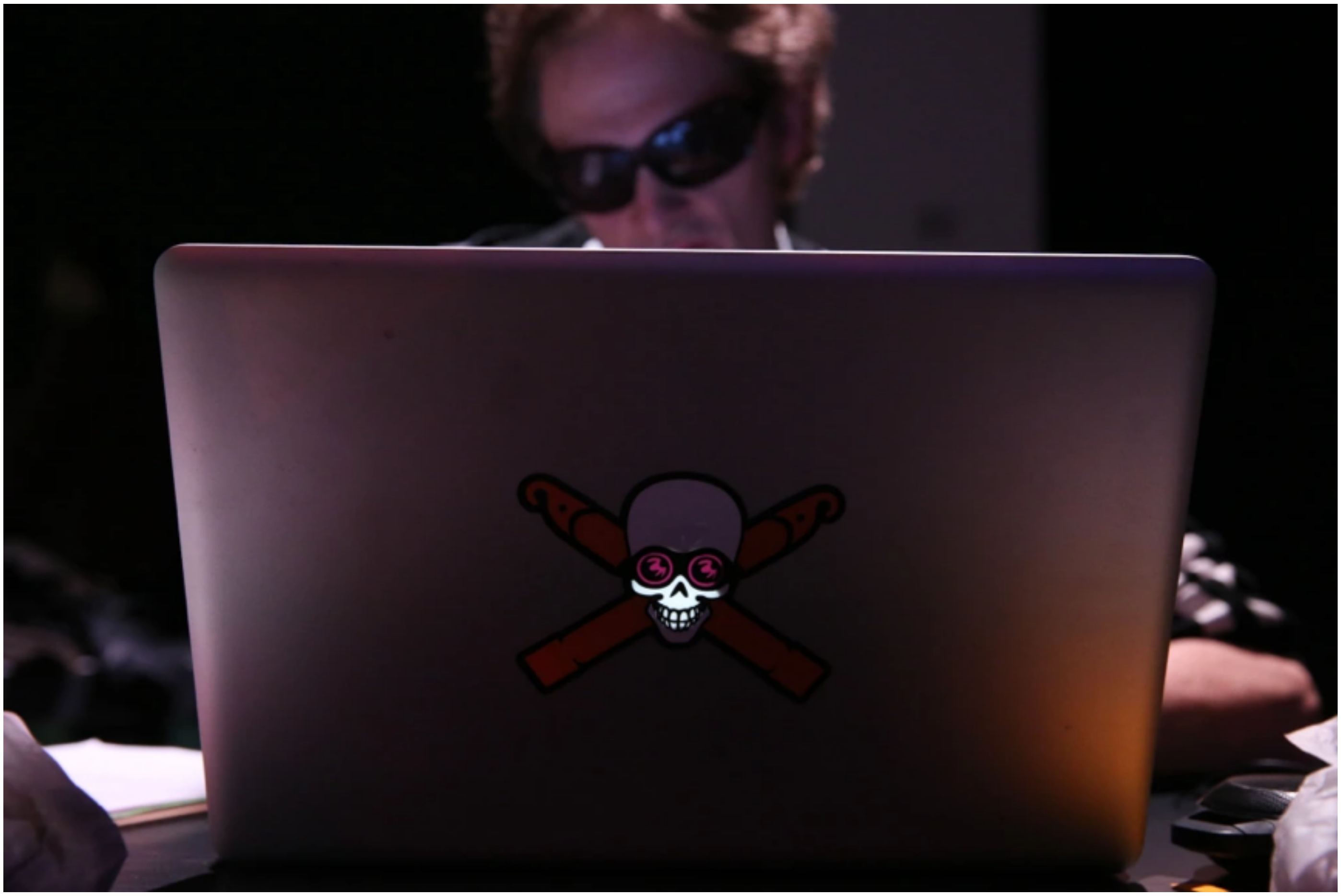
DOD pays out $75K for vulnerabilities discovered by white hat hackers

In the latest iteration of DOD's bug bounty program, ethical hackers discovered nearly 350 bugs inside the department's networks.

Mark Pomerleau September 29, 2022



A hacker using a laptop computer at the Hacked By Def Con Press Preview during the 2016 Tribeca Film Festival at Spring Studios on April 15, 2016 in New York City. (Photo by Rob Kim/Getty Images for Tribeca Film Festival)

By

The Department of Defense paid out $75,000 in bounties recently to ethical hackers who discovered nearly 350 bugs inside its networks.

The payouts were part of the ongoing bug bounty initiative in which vetted hackers are invited to find and disclose network vulnerabilities to the DOD in exchange for payment. Allowing these so-called white hat hackers to alert the Pentagon to the vulnerabilities discovered allows the department to fix them before they're found and exploited by adversaries.

"We have to make sure we stay two steps ahead of any malicious actor. By paying out monetary rewards to ethical hackers, we harden our defenses in a very impactful way. This crowd-sourced security approach is a key step to identifying and closing potential gaps in our attack surface," said Katie Savage, deputy chief digital and artificial intelligence officer for the Defense Digital Service.

The most recent campaign, dubbed Hack the U.S., kicked off on July 4 in partnership with the Pentagon's Chief Digital and Artificial Intelligence Office (CDAO), DOD Cyber Crime Center (DC3) and HackerOne. It involved 267 hackers, 139 of which were new to the DOD's vulnerability disclosure program.

In total, the department paid $75,000 in bounties and $35,000 in bonuses with 648 reports submitted, 349 of which were actionable.

"We knew from years of a successful [vulnerability disclosure program] that professional hackers are a critical extension of our team. This bounty challenge shows the extra value we can earn by leveraging their subject matter expertise in an incentivized manner," Melissa Vice, director of the disclosure program at DC3, said in a blog post shared with reporters prior to its scheduled publication on Thursday.

“Through initial evaluation of Hack U.S. reporting, the most commonly identified vulnerability is categorized as ‘Information Disclosure.’ With the identification of vulnerability trends, we can seek out patterns of detection and ultimately create new processes and system checks to ensure we address the root cause and develop further mitigations against malicious actors who might try to exploit our systems,” she said.

This particular iteration of the program was focused on identifying critical vulnerabilities while previous efforts were invite-only and focused on a specific group of assets hacked for a limited time, according to a DOD spokesperson. This effort covered a broader scope of assets under the DOD’s vulnerability disclosure program. It was also publicly open to hackers on the HackerOne platform, the spokesperson added, noting this is atypical for DOD’s reward-driven bug bounty initiatives.

Savage noted that by running these types of programs over the past six years, the partnership between ethical hackers and the government has yielded thousands of security insights.