Skilled hackers with good intentions

Federal Monthly Insights - Hacker-Powered Security - May 20, 2021

In the 1983 movie "*WarGames,"* a young American hacker nearly ends the Cold War by ending the world. That plot resulted in a hit movie that filled the seats, back when people exclusively went to theaters for such excitement.

Kris Johnson, director of the Defense Department's Vulnerability Disclosure Program (VDP) in the DoD Cyber Crime Center, likes a different kind of hacker-centric plot, although it won't sell many tickets.

"I totally went and I found vulnerabilities and we secured the system and nothing happened. I don't know if they're going to get a Michael Bay explosion movie out of it," said Johnson on ***Federal Monthly Insights – Hacker-powered Security*****.**

Over the years, the DoD has been at the vanguard of ethical hacking and bug bounty programs, where the good guys find cybersecurity flaws in their systems and let them know. Those keyboard cowboys have many monikers: ethical hackers, white-hat hackers or security researchers.

"I think that there's a lot of movement, certainly in what OMB refers to as coordinated vulnerability disclosure, that's the overall umbrella that covers both your bug bounties and your vulnerability disclosure programs or VDPs," said Johnson on ***Federal Drive with Tom Temin***. "The big difference is that the bug bounties, pay money, while the VDPs pay reputation points."

Those participating in the VDPs are trying to build "street cred," Johnson said. The white-hat hackers can build their resumes to impress those who will perhaps, someday, pay them money for their skills.

“Until recently, the policy for VDP, which is how we provide legal safe harbor for the security researchers or ethical hackers, that policy has always been public-facing DoD websites,” Johnson said. “It’s a partnership and we provide that legal safe harbor against the Computer Fraud and Abuse Act, so that they can operate with the understanding that no one’s going to come kick down their door and come after them for either civil or criminal litigation.”

The rules of engagement for the hacker are fairly simple, Johnson said. And in the last five years, there has not been one incident of an ethical hacker violating a policy.

“Obviously, that’s always a concern for us,” Johnson said. “We’re an agency of the Department of Defense, but also we advocate for the security researcher, because we know how perilous their feeling could be. We want them to know they should stay within the scope that we have published, which tells them what they can do research on. And that’s kind of a three-legged milk stool, if you will. They can discover, they can test and then they must report. If they do that then we’re going to operate in good faith with them.”

VDP is now going beyond all DoD websites into so-called, “publicly accessible information systems,” which they can get to from home or a public space.

“Obviously no physical penetration,” Johnson said. “They’re not allowed to jump a fence at Fort Meade, but from where they’re at, everything’s pretty much in game. If they see something, they can report it and we’re going to be able to process it.”