PCWorld.com - HP, Bug-Hunters Declare Truce

HP, Bug-Hunters Declare Truce

Analysis: The story behind SnoSoft's pitch, the extortion charges, and the DMCA threat.

Kim Zetter, special to PCWorld.com

Friday, August 09, 2002

LAS VEGAS -- The relationship between software vendors and the bug hunters who sportingly seek out flaws in their products is often tenuous. Throw in some clashing egos, a perception of greed, and some poorly phrased communications and that relationship is likely to snap.

That's apparently what happened here last week during the BlackHat and Defcon security conferences when Hewlett-Packard and Secure Network Operations (SnoSoft) squared off over alleged bugs in an HP product. HP even accused SnoSoft of violating the Digital Millennium Copyright Act when someone associated with the researchers posted code that could be used to exploit one of the vulnerabilities.

Missed Pitch

The saga began last April, when SnoSoft co-founders Adriel Desautels and Kevin Finisterre told HP they had found 22 vulnerabilities in Tru64, the company's Unix operating system. The SnoSoft researchers, who had worked with HP previously on an unrelated project, say they decided to use their findings as leverage to get HP to hire them to audit Tru64 for more bugs.

Advertisement

The first day of the Black Hat conference, HP wrote to SnoSoft accusing the researchers of violating the DMCA and computer crime laws. One exploit for a vulnerability that SnoSoft found had been posted publicly on a security Web site.

Apparently HP retreated from the accusation after Chief Executive Officer Carly Fiorina was besieged with e-mail from HP employees, outside researchers, and techies, who complained that a strong-arm stance would curb vulnerability research. But the incident raised longstanding questions about full disclosure and how bug-hunters should communicate with vendors.

According to Desautels, HP interpreted the request for work as "extortion." Desautels now sees how HP might have interpreted his e-mail that way, but adds he never intended to barter the information. He says he planned to hand over the information on the 22 vulnerabilities free, in exchange for HP's consideration of the company for further work on

Tru64.

"We weren't asking for money for work we'd already done. Our goal was to show them the caliber of stuff we'd already found so they would hire us to find more bugs," he says.

In retrospect, Desautels says, it's clear he didn't do a good job communicating his intentions to HP.

HP executives declined to comment on the issue.

However, a company statement says its letter to SnoSoft "was not consistent or indicative of HP's policy. We can say emphatically that HP will not use the DMCA to stifle research or impede the flow of information that would benefit our customers and improve their system security."

Threats and Promises

At first, HP seemed to doubt the bugs were genuine, Desautels says. Then the company invited him to draft a contract. "Three weeks after they requested we put together a contract, they released information on 17 vulnerabilities. Some of them were the same bugs we had found," he says.

He believes HP stalled SnoSoft during contract negotiations to get time to conduct its own research and squash the bugs. Then HP's charge of extortion surfaced.

A hacker/researcher named Phased, who works with SnoSoft, was furious. He sent a scathing e-mail to HP, and then posted an exploit for a Tru64 vulnerability on the BugTraq security list.

"Instead of releasing the bugs outright, we wanted to help HP save face and protect their customers. But then they accused us of extortion," he wrote.

Desautels claims he didn't know Phased was going to post the exploit. Although the exploit dealt with a vulnerability discovered over a year ago by someone else, Desautels says he still disapproves of Phased's action.

That's when HP raised the DMCA accusations, which angered many Black Hat attendees. Some bug-hunters declared they would take vulnerability research underground, by posting the information on public forums instead of offering it to vendors.

Just a Misunderstanding?

Kent Ferson, vice president of HP's Unix Systems unit, has already acknowledged that the vendor misunderstood SnoSoft's intentions. HP says it has patched the vulnerabilities in question--although it didn't occur as quickly as the bug-hunters typically permit.

"Normally, we would give them only seven or eight days to produce a patch before revealing the vulnerabilities," Desautels says. "But we extended it to 45 days."

SnoSoft worked with HP and the federally funded computer and network security body, the Computer Emergency Response Team Coordination Center, based at Pittsburgh's Carnegie Mellon University, on the bug fix schedule. Through CERT, SnoSoft agreed to increase HP's grace period to 55 days to fix the 22 vulnerabilities. (HP has yet to post a fix.)

Hacker Ethics

Traditionally, bug-hunting is free work that bug researchers or benevolent hackers perform to help secure systems against criminal hackers--and to gain some fame for themselves. But in recent years, vulnerability research has emerged as a job specialty valuable to vendors. Hackers often seek research contracts with vendors to get paid for findings.

But young hackers, inexperienced in business communications, don't

always understand the subtleties of the process. As a result, their approach to companies can resemble blackmail or extortion. The hacker ethic frowns on "selling" found vulnerabilities to vendors, but supports a bug-hunter's effort to contract with companies in advance to find more holes.

The lines of acceptable conduct have blurred as hackers move into security consulting. The hacking community has long accused software developers of hiding bugs from customers. But the average vulnerability research contract commonly acknowledges that the findings belong to the vendor. Researchers can't independently publish their findings, and a vendor can choose to sit on the information.

A standard that balances the desires of vendors and researchers as well as customer needs has been a subject of public and often heated discussions. No solution has resulted, and the participants say misunderstandings are likely to continue.

Legal Remedy?

One lobbyist attending Black Hat says the HP-SnoSoft incident has stirred his interest in lobbying for a law to clarify how bug-hunters should handle vulnerability findings. Michael Morgenstern, a managing partner of security firm Global InterSec, says he wants a standard for the number of days bug-hunters should grant vendors to release a patch, and policies for vendors with regard to how to handle bug reports and researchers.

"It's clear that the current situation isn't working," Morgenstern says. "I'm not convinced legislation is the only way to do this. But I want to stimulate communication."

Desautels now acknowledges that HP was preoccupied with its Compaq merger when he approached the company. In fact, the firm was still deciding which products lines would survive, which might have slowed the

company's response.

"The lesson to be learned in all of this is that we need to find some way of approaching vendors and communicating with them," he says. In the future, SnoSoft will approach vendors and release findings to CERT, he says. CERT can then broker with vendors.

In the meantime, the incident gained SnoSoft a lot of attention. Desautels says its Web site received nearly 1 million hits in the week after HP's DMCA threat broke. It previously received about 1500 hits per week.

He says SnoSoft wants to continue its campaign to harden the Internet. The company's new goal is to audit all of the major operating systems for vulnerabilities. "I know that's ambitious but my eyes have always been bigger than my stomach," he adds.