washingtonpost.com

Site Plans to Sell Hacks to Highest Bidder

By Brian Krebs
washingtonpost.com Staff Writer
Thursday, July 12, 2007; 2:51 PM

A Swiss Internet start-up is raising the ire and eyebrows of the computer security community with the launch of an online auction house where software vulnerabilities are sold to the highest bidder.

The founders of WabiSabiLabi.com (pronounced wobby-sobby-lobby) say they hope the service presents a legitimate alternative for security researchers who might otherwise be tempted to sell their discoveries to criminals.

Several established vulnerability management companies already purchase information about software flaws from researchers, yet the terms of those deals are private and generally set by the companies. Letting all interested parties bid on security vulnerabilities in an "eBay"-style auction assures that researchers receive the fair market value for the work they do in finding the flaws, said Herman Zampariolo, WabiSabiLabi's chief executive.

"Without an open marketplace, it is impossible to know just how much this intellectual property is worth, and while the free market is not the most perfect way to discover that, it's a good proxy," Zampariolo said. "Sure, lots of companies are setting figures for what they think vulnerabilities are worth, but a majority of researchers are getting far less than what their information is worth, and that's scandalous."

Vulnerabilities that could be sold on the site range from those present in hardware that supports critical information infrastructure -- such as Internet routers -- to flaws in common desktop applications, such as Web browsers, instant messenger and e-mail programs. In many cases, the flaws could be exploited by criminals to gain control over home computers or business networks, giving them access to sensitive information.

What's scandalous, say some security experts, is the idea that the company can be sure that it is not selling instructions for breaking into computers and networks directly to the criminals most likely to use them.

"How do you know bidders aren't people with nefarious purposes," asked Teri Forslof, manager of security response for TippingPoint, a 3Com company that buys vulnerabilities from researchers. "It's really easy to create a shell company that looks good on paper that is set up to be nothing but a front for bad guys."

Zampariolo said the company thoroughly screens all potential sellers and buyers, requiring proof of identification, articles of incorporation, and even bank account information from all parties involved. For the first six months of operation, the service will be free, after which the auction house plans to take a 10 percent cut of the final selling price of a vulnerability. Security flaws up for auction that are not designated by the seller as "exclusive" for the buyer will be shared among a vulnerability alert club to which the company will sell access.

Still, the inability to positively "know your customer" was the prime reason that researcher Greg Hoglund abandoned an idea he had several years ago for setting up an online auction for software flaws. He even built the online auction portal, which he planned to call "Zero-Bay," a play on eBay and the term "zero-day." Zero-day (or "0day") threats are previously undocumented flaws that software vendors learn about only after cyber criminals have begun exploiting them online for financial gain.

Hoglund ultimately pulled the plug on the company the evening before its launch, concerned about possible legal liability if vulnerabilities sold through Zero-Bay were to wind up in the hands of cyber crooks.

"I was thinking vendors could purchase the research for a fair market price as opposed to expecting to receive the information for free," Hoglund said. "But I basically decided that if the bad guys get their hands on it, that could be a lot of people at risk, and that was a risk I wasn't willing to take."

Companies like TippingPoint and VeriSign's iDefense both pass along details of vulnerabilities they buy to the affected software vendors, and both withhold public disclosure of the flaws until the vendor has shipped a "patch" to plug the security holes. WabiSabiLabi's founder said the company currently has no plans to notify affected vendors, saying that could ultimately decrease the price buyers are willing to pay for any one vulnerability.

Matthew Murphy, a 20-year-old Los Angeles-based security researcher who has sold several vulnerabilities to iDefense, said he would be uncomfortable selling a flaw if he could not vouch for the buyer's intentions. But Murphy said he is more discomfited by the fact that vendors are not notified of the details behind flaws to be sold via WabiSabiLabi.

"I think that the people in the security research community who would sell to just anyone are in a relative minority," Murphy said. "Without a little bit of transparency and some kind of buyer credibility, it's not going to take off relative to other services out there."

Software vulnerability researcher Dino Dai Zovi said he's excited about the vulnerability auction service and its prospects for rewarding researchers with better prices.

"I can see this service creating much more incentives for researchers to find flaws," Dai Zovi said. "Not everyone is willing to spend 20 to 40 hours looking for vulnerabilities in [Microsoft Windows] software just to receive a little 'thank you' note in Microsoft's security advisories."

Dai Zovi said he has never sold a vulnerability, although he recently won a $10,000 bounty in an impromptu research challenge at a hacker conference in Canada. At the suggestion of conference organizers, TippingPoint offered the reward to anyone who could find a previously unknown flaw that would allow an attacker to break into a fully protected MacBook laptop computer from Apple. A few hours into the challenge, Dai Zovi found a vulnerability in QuickTime, the media player software loaded on all Apple computers as well as many Microsoft Windows machines worldwide.

It is unclear whether any major software vendors would bid on vulnerabilities in their own software. Microsoft has emphatically and publicly stated under no circumstances would it ever buy vulnerability research. Mozilla, the maker of the Firefox Web browser, offers a $500 "bug bounty" for each vulnerability privately reported to the company.

WabiSabiLabi already has opened bidding on four software vulnerabilities, which it claims its in-house researchers tested to ensure that prospective buyers will in fact receive what they purchased. So far, only two of them have attracted a total of three bids from interested buyers. But Zampariolo says he's received the necessary identifying documents from more than 200 security researchers interested in auctioning their wares.

Ironically, one inherent threat to each seller and to the auction house itself is the information contained in WabiSabiLabi's listings. Within hours of posting basic details about the four flaws on its auctions page, hackers on two different security research forums claimed to have located two of the vulnerabilities up for auction, posting computer code to back up their claims.

Zampariolo confirmed that one of the vulnerabilities publicly reported by researchers indeed was the exact same as a flaw being auctioned on the site -- a bug in an add-on component of an open source e-mail application called "SquirrelMail" -- and that it had since been patched by the vendor. However, he said the site is preparing to start an auction on a new flaw found in the newest, patched version of SquirrelMail.

The second auction researchers claimed to have foiled was instructions for exploiting a known vulnerability in the Linux operating system. The instructions hackers posted online for exploiting that flaw were similar to the exploit currently up for auction, WabiSabiLabi technicians told washingtonpost.com in an e-mail.

The company is touting both incidents as an example of how their service will serve to make software users safer in the long run.

"The SquirrelMail public disclosure has been pushing people from the community to quickly produce autonomous research in that direction, eventually ending with the discovery of the bug we had on sale in our marketplace and subsequently the immediate release of the new software version," Zampariolo said. "Two hidden vulnerabilities became

public, and that's a great step ahead for the industry."

Post a Comment

View all comments that have been posted about this article.

Your washingtonpost.com User ID will be displayed with your comment.

You must be logged in to leave a comment. Log in | Register

Submit

Comments that include profanity or personal attacks or other inappropriate comments or material will be removed from the site. Additionally, entries that are unsigned or contain "signatures" by someone other than the actual author will be removed. Finally, we will take steps to block users who violate any of our posting standards, terms of use or privacy policies or any other policies governing this site. Please review the full rules governing commentaries and discussions. You are fully responsible for the content that you post.