

NEWS & ANALYSIS

SECURITY INTELLIGENCE

Vulnerable Commodity

Security experts and practitioners debate the wisdom of buying info from the digital underground.

by SHAWNA McALEARNEY

Advance information on security vulnerabilities is golden, and at least one security intelligence firm is willing to pay handsomely for it, despite criticism that the practice undermines overall Internet security.

Since last August, **iDEFENSE** (www.idefense.com) has openly solicited information on previously unknown vulnerabilities, paying hackers between \$500 and \$1,000 for their discoveries.

The firm uses the data collected through its Vulnerability Contributor Program (VCP) to provide clients with advance security warnings and fixes.

“In one fell blow, we can provide our clients with timely vulnerability information while doing good for the Internet community by taking the announcement through the vendor disclosure process,” says David Endler, iDEFENSE’s director of technical intelligence. “A lot of vulnerabilities are traditionally just posted to Web sites and mailing lists without the benefit of vendor notification.”

Accepting vulnerability tips and information from the digital underground is nothing new. Security firms will often collaborate with hackers to verify and correct vulnerabilities.

What’s new is paying hackers, a practice that’s drawing mixed reviews.

“Security companies that provide financial incentives to find flaws in systems and share the vulnerabilities with vendors as they are discovered contribute to society by pumping money into security testing that would not otherwise occur,” says Stuart Schechter, a computer science doctoral candidate at Harvard University. “What these firms are really doing is paying for testing that the system’s developer should have paid for in the first place.”

However, in a recent **Packet Storm** (www.packetstorm.org) poll, only 9.1 percent of the respondents said firms that purchase vulnerabilities from hackers contribute to the security of the Internet. And nearly one-third say the practice stimulates the disclosure of zero-day vulnerabilities.

“The idea of rewarding people for trying to break into systems—even if they’re doing it benignly on their own as a hobby—really strikes me as the wrong approach,” says Gene Spafford, a Purdue University computer science professor and director of the **Center for Education and Research in Information Assurance and Security** (www.cerias.org).

“If companies hired these people as full-time, in-house



employees, that’s one thing,” Spafford adds. “But to be offering a bounty outside the company is conveying the message that anyone can break into systems and make money from it.”

Several security vendors and research firms contacted for this story say they don’t pay hackers for vulnerabilities. However, sources say that it’s a common under-the-table practice among IT consultancies and some security vendors, who use the information to gain an advantage over competitors.

“Security firms who use this practice don’t want their clients to know that they don’t have the talent in-house,” says Gary Bahadur, CIO of security firm **Foundstone** (www.foundstone.com).

Vetting Sources

iDEFENSE built VCP with controls to both ensure the information it buys comes from reliable, legitimate sources. Without going into too many specifics, the firm says it checks out contributors before accepting information.

In most cases, VCP contributors are students, white and gray hat security enthusiasts and professionals. Endler says the firm avoids dealing with black hats.

Depending on the severity of the vulnerability and the exclusivity of the information, iDEFENSE will pay between \$400 and \$900 per vulnerability, and a \$100 bonus for allowing iDEFENSE to lead the vendor notification process.

iDEFENSE declined to specify the maximum amount it has paid for a vulnerability, but indicated it would negotiate outside its established range for “juicy information.”

“The money is just an additional incentive for people sitting on vulnerabilities to release the information,” says Matt Conover, founder of the **w00w00** hacker group (www.w00w00.org).

CONTINUED ON P. 16

OWASP Releases Top 10 Web App Coding Problems

Poor coding is blamed for many security vulnerabilities, leading the **Open Web Application Security Project** (www.owasp.org) to draft a list of the 10 most common Web application development errors.

“Web developers need to know that the degree to which business applications and customer data are protected from the hostile Internet is directly determined by how securely they’ve written their code,” says Chris Wysopal, an OWASP founding member and director of research at security consultancy **@stake** (www.atstake.com).

The list contains several well-known coding mistakes, some easily exploitable by script-kiddies.

The following is the OWASP list:

- Information from Web requests not being validated before being used by a Web application.
- Authentication flaws that can allow attackers to access user accounts.
- Broken account and session management, where account credentials and session tokens aren’t properly protected.
- Cross-site scripting flaws, which allow a Web app to be used to launch attacks through the end user’s browser.
- Buffer overflows, where components such as CGI, libraries, drivers and Web-app servers can be manipulated.
- Command injection flaws, which allow malcode to be embedded in Web-app parameters.
- Error handling problems that can accidentally divulge detailed information that could enable a denial-of-service (DoS) attack.
- Insecure use of cryptography.
- Remote administrative flaws, caused when remote functions using a Web interface aren’t carefully protected, allowing attackers to obtain admin-level access.
- Web and application server misconfigurations, which can result in a compromise of the Web site.

Some security experts say the list is stating the obvious, but reinforces the importance of instilling good coding practices in software development projects. ▀

CONTINUED FROM P. 15

Critics say it’s nearly impossible to verify the identity of hackers peddling their wares, especially if those people want to remain anonymous.

“There are a lot of shades of gray heading toward black in this area,” says Foundstone’s Bahadur. “A legitimate researcher investigates vulnerabilities for name recognition and to try to help the security industry. If you’re in it for the money, odds are you’re using that exploit for some other purpose as well.”

iDEFENSE covers the misuse of vulnerability information through its contractual agreements. Hackers are prohibited from sharing their discoveries with others until the firm has completed its disclosure process—which usually takes two weeks.

“iDEFENSE is able to formulate stopgap workarounds and countermeasures to mitigate exploitation during the exposure window that exists until a vendor fix becomes available,” Endler says.

Pundits say contractual agreements are virtually meaningless to many members of the digital underground. While iDEFENSE may be protecting its paying customers, an unscrupulous hacker could collect his bounty and still exploit scores of enterprises that don’t receive the advance intelligence.

Critics also say there’s no way of controlling information once it’s released to a third party.

“Companies [that engage in this practice] may prohibit the discoverer from posting to underground lists, but taking into account all the recipients of the information, there’s no way to know for sure that it won’t be,” Spafford says.

Some information may leak, but supporters say this process is more responsible than many of the existing disclosure models.

“It’s better for someone to get paid to find a vulnerability and give it to a responsible security company that will contact the affected vendor and arrange for a fix, rather than allowing it to circulate in the underground, where it may remain unknown to the security community,” Conover says.

Legal and Ethical Concerns

The ultimate lack of control over purchased vulnerability information is what really concerns traditional white hat security practitioners. They say there’s too many “what ifs” to make this practice worthwhile.

“There’s the ethical issue of really not being able to control who is buying this stuff, followed by the liability issue that’s introduced that overwhelms the possible benefits of doing it,” says Ed Skoudis, VP of security strategy at **Predictive Systems** (www.predictive.com). “Overall, I think it’s unethical, and it doesn’t make economic or business sense because you’re going to be sued big time.”

The issues of legal liability, however, aren’t clearly defined.

“Several potential areas of liability may be implied, but I must emphasize that the law in this area is very unclear,” says Michael Overly, a partner at Foley & Lardner, a firm that specializes in Internet law. “While not specifically engaging in reverse engineering and other activities themselves, the security companies might be held ‘vicariously’ liable. They could be seen as simply paying money to someone else to engage in potentially illegal or unauthorized activity.”

Legal and ethical issues aside, iDEFENSE and other companies will likely continue vulnerability payment programs for the time being.

“I think this practice is completely widespread in the industry,” says Theo de Raadt, project leader of OpenBSD. “If we fix a whole bunch of these vulnerabilities now—even if money is what accelerates it—we’ll be more secure, and new vulnerabilities will be discovered and fixed in a continuous cycle.” ▀



“The idea of rewarding people for trying to break into systems really strikes me as the wrong approach.”

—GENE SPAFFORD