Private market growing for zero-day exploits and vulnerabilities

Robert Lemos, Contributor

This article can also be found in the Premium Editorial Download **"Information Security magazine: Market for vulnerability information grows."**

Download it now to read this article plus other related content.

In 2011, vulnerability researcher Luigi Auriemma discovered more than six dozen vulnerabilities in a variety of enterprise software packages, selling each software bug for a modest bounty to the Zero Day Initiative, a group set up by TippingPoint, and now a subsidiary of Hewlett-Packard.

A well-known white-market buyer for software vulnerabilities, HP's TippingPoint, uses the information to protect its customers while working with the vendor whose software is affected to close the security hole. While the company does not disclose how much it pays researchers, payments typically fall between $1,000 and $5,000, with most less than $2,000, according to sources.

Yet, with penetration testers, industrial spies, law enforcement, intelligence agencies and the military all looking for exploits to undisclosed flaws to fuel their cyber-operations, such modest bounties are no longer the incentive they once were. Vulnerability researchers, once starved for a market for their security flaws, now have new options.

Aureimma, for example, partnered with another researcher, Donato Ferrante, to launch his own firm ReVuln, which sells information on vulnerabilities to subscribers for both defensive and offensive purposes.

"We have our own team focused on researching vulnerabilities, and we don't report our findings to vendors in order to respect both the investments of our customers, and the other companies that follow a business model similar to ours," Aureimma said in an email interview.

Auriemma is not alone. Security researchers from the Zero Day Initiative split off to form their own firm, Exodus Intelligence, to report exploitable vulnerabilities to subscribers. Dustin Trammell and NSS Labs partnered to create ExploitHub, a place to resell exploits to penetration testers to use on their own, or their clients', networks. And offensive security firm VUPEN sells exploits for undisclosed vulnerabilities to governments worldwide.

"I absolutely see the more experienced researchers increasingly foregoing the route of non-disclosure or selective disclosure, and more often seeking to be compensated for their work," said Dustin Trammell, director of technology and co-founder of ExploitHub.

The result of a market that values vulnerability information is security research rapidly becoming privatized. While Microsoft has not strayed from its promise to not pay for vulnerability information, Facebook, Google and Mozilla all pay researchers who work with them. The Zero Day Initiative and the Vulnerability Contributor Program—the first bug bounty program started by security-intelligence firm iDefense, now part of VeriSign—also pay for vulnerability information. And a gray market, where researchers sell vulnerabilities to be used in offensive operations, is rapidly expanding.

“The market has evolved in a way such that this information is useful—it has some value that it didn’t have before,” said Aaron Portnoy, co-founder and vice president of research for vulnerability information startup Exodus Intelligence. “People [researchers] just don’t find value anymore in getting the accolade of their name on an advisory.”

Vulnerability Researchers: In Pursuit of Compensation

In the past, researchers typically had three options: full disclosure, no disclosure or work with an often-unappreciative vendor for free—so-called “responsible” disclosure. While most arguments focused on how to best serve software users, a secondary issue has always been whether researchers should be compensated for their work.

The ability to get paid for vulnerabilities that can be practically exploited is changing the market dynamics for researchers. Exploits have become the currency for all sorts of groups that have put themselves in the role of attacker on the Internet. From governments to cybercriminals to pen testers to industrial spies, many attacks need a working exploit to successfully compromise a target’s systems.

“The utopia of full-disclosure … to improve the security of the world, proved to be a failure for both final users waiting months for a patch, and for researchers who see their works used to make the business of other companies,” Auriemma said in an email interview.

At the turn of the century, security researchers largely fell into two opposing camps: Either the flaw finder turned in their vulnerability information to the vendor and worked through a long process to get the issue fixed, or the researcher decided to post the information publicly.

Security experts who supported full-disclosure argued that the shaming of a company and the resulting headaches would cause it to take security, and secure development, more seriously. Yet, the approach was also easier: Researchers did not have to worry about dealing with companies that had, for the most part, negative feelings.

“The idea of public disclosure is a good idea, because it forces software developers to get things done,” said Adriel Desautels, CEO and founder of Netragard, a security consultancy and vulnerability brokerage. “But the reality of the past 10 years is that has not been the case.”

In the midst of that debate, the first third-party white-market bounty programs were created. In August 2002, VeriSign’s iDefense established the Vulnerability Contributor Program (VCP), offering to pay researchers for information about flaws. TippingPoint—who hired David Endler, the original creator of iDefense’s VCPcreated its own program in 2005. In 2004, Mozilla started offering its own modest bounties of $500 for bugs, followed by Google, Facebook and now PayPal, which in June announced its own rewards for bugs found in the company’s websites.

Yet, buying vulnerabilities is of questionable value to software companies and defensive-technology companies. For the most part—except for Google and its Pwnium contest, which awards $60,000 for critical issues in the company’s Chrome browser—vulnerability information has not sold for what many researchers believe its worth.

“We have approached vendors about vulnerabilities, and many of them didn’t think it was important,” said Netragard’s Desautels. “Software vendors, for the most part, are focused on how much money they can make and not on securing their users.”

No wonder, then, that some researchers have turned to the morally gray area of selling to groups and organizations that intend to use the information to fuel attacks. While there has always been a shadowy gray market for vulnerability sales to governments, other programs have had mixed success. Two attempts to auction off vulnerabilities in 2005, for example, ran afoul of eBay's policies, and a vulnerability auction site, WabiSabiLabi, started up in 2007, but fizzled out in the face of legal and technical challenges.

White, Gray, Black: Money and Morals

With the success of several cyberattacks carried out by nation-states—such as Stuxnet, Flame and Aurora—that changed, however. The attacks have shown researchers that there is tremendous value in information on unknown, or not publicly disclosed, vulnerabilities, and that the sale of information is a legitimate endeavor. By demonstrating value, such attacks are driving a move to a more private market.

"The success of Stuxnet and Flame—and the use of the zero-day exploits in those attacks—would not be possible without a market out there," said Aviv Raff, chief technology officer for Israel-based security intelligence vendor Seculert. "I would not say those zero-days were necessarily sold on the market, but they are proof that a thriving market is feasible."

A gap between the number of exploitable zero-day vulnerabilities and the actual number of zero-day exploits developed suggests that researchers have a lot of fertile ground to explore, said ExploitHub's Trammell. In one analysis, NSS Labs found that the leading penetration testing products—such as Core Impact, Immunity's CANVAS and Metasploit—included less than 10% of the approximately 14,000 public vulnerabilities ranked high- or critical-risk that were disclosed over the prior five years.

"Any additional resources to help make up that more than 90% gap in coverage would be a good thing," Trammell said.

Sales of vulnerability information fall into a spectrum. At one end, the white market includes bounties offered by software vendors for vulnerability information in their own products as well as sales to third parties that work with the software developer to fix the issue. At the other end, a black market has evolved around sales of vulnerabilities to criminal enterprises.

In the middle lies the most interesting market for vulnerabilities: A gray market of legitimate buyers who do not report the issues, but intend to use the vulnerabilities to compromise systems. Government buyers fall into this category as do the vendors of espionage and monitoring Trojans, who argue that exploiting vulnerabilities to surveil criminals or potential enemies is a natural evolution of today's digital society.

Companies that sell services or software to be used in penetration testing are also in a gray area, because the buyer of the vulnerability does not inform the software vendor of the issues. Yet, such software is arguably a defensive technology, because it helps identify weak spots in corporate network security, said Seculert's Raff.

"I believe that if it helps pen testing, then it helps security," he said.

Other uses of vulnerability information are even harder to categorize. Hacking Team, based in Milano, Italy, develops a remote surveillance program know as the Remote Control System (RCS), which is used by a variety of governments to keep tabs and collect evidence on people breaking laws. The software has reportedly been sold to 30 different countries across five

continents. The company abides by the "various blacklists" and doesn't sell the software to restricted nations, said Eric Rabe, a spokesperson for the company. In addition, the company does not sell to private industry.

"We think it is an important product for the safety of society," Rabe said. "Because this is a new area, it is not clearly defined, but we as a company have made a decision that we don't want to see the software that we produce to be used by bad actors."

Sales in the gray market have driven competition in the white market. White market bounties typically vary from $500 to $5,000, though $10,000 is not unheard of. Gray market prices may start at $20,000 and reach up to $200,000 or more, experts estimated.

Yet, white market sales are driven by morals as well as money. While prices are typically higher in the gray market, researchers that sell to the white market are getting the vulnerability fixed, said Brian Gorenc, a security researcher with HP's Zero Day Initiative.

"There are researchers out there that don't want to focus on the research or on the business side of the market," he said. "They bring us the bugs so we can handle the responsible disclosure part."

Needed: A Less Vulnerable World

While the gray market offers more opportunity to security researchers, it has also reopened the debate over the sale and use of vulnerabilities to compromise computers. In many ways, sales to clients that intend to use the vulnerability information keeps the general user populace vulnerable. And making a value judgment about what is a "good" use of an attack is difficult, said Don Jackson, director of threat intelligence for Dell Secureworks, a managed security firm.

"The problem with making that judgment, is that our government is someone else's bad guy," Jackson said.

Yet, zero-day exploits are being used. In a recent academic paper, two Symantec researchers used analysis of antivirus detections and the vulnerabilities exploited by malware to find 18 zero-day attacks, including 11 that had not been previously discovered. At the end of the four-year analysis, more than two-thirds of the zero-day attacks were still ongoing.

"There are two possibilities," said Tudor Dumitras, senior research engineer with Symantec Research Labs. "Attackers are still using those attacks against vulnerable systems or they are using them even though some systems have been patched."

Stockpiling exploitable, unpublished vulnerabilities by intelligence and military agencies is like the United States military trying to prepare for the eventuality of two simultaneous wars, argued Chris Soghoian, principal technologist with the Speech, Privacy and Technology Project at the American Civil Liberties Union. They have to keep the ability for cyber-operations viable and that will drive the market. Moreover, the limited shelf life of vulnerabilities—at least 10 months after first use, according to Symantec's research—means that the military will always need new information.

"You could have a flaw that is good for a year, or a flaw that is good for a week," Soghoian said. "They don't know when Google or Microsoft will fix these things, so there is an unending demand."

Even if someone believes that stockpiling exploitable vulnerabilities for use on another nation's systems is a good idea, it's a poor exchange, if it means keeping our own systems vulnerable, he added. The key problem is that the software flaw only remains exploitable if we keep our own systems vulnerable as well.

"I'm not even arguing ethics," he said. "I think it is stupid to allow people to be vulnerable. We complain that the Iranians and the Chinese are hacking us, then we should want every U.S. computer to be up-to-date and patched."

Yet, Netragard's Desautels points out that zero-day attacks enabled by purchased vulnerabilities are not going to target the general populace. Any government would have specific targets that pose some risk.

"If the zero-day market disappeared today, it would have no impact on the proliferation of malware among public computers," he said. "Instead, it would be great if software vendors could be better about their development, and then there would be no zero-days left to sell."