Forget Disclosure — Hackers Should Keep Security Holes to Themselves

Vendors, governments and the information security industry have incentives to protect their interests over their users'. Not all the players will act ethically, or capably. So who should the hacker disclose to?

Andrew Auernheimer 11.29.2012 05:30 PM

photo: Stephanie Keith

Editor's Note: The *author of this opinion piece, aka "weev," was found guilty last week of computer intrusion for obtaining the unprotected e-mail addresses of more than 100,000 iPad owners from AT&T's website, and passing them to a journalist. His sentencing is set for February 25, 2013.*

Right now there's a hacker out there somewhere producing a zero-day attack. When he's done, his "exploit" will enable whatever parties possess

it to access thousands -- even millions -- of computer systems.

But the critical moment isn't production -- it's distribution. What will the hacker do with his exploit? Here's what could happen next:

The hacker decides to sell it to a third party. The hacker could sell the exploit to unscrupulous information-security vendors running a protection racket, offering their product as the "protection." Or the hacker could sell the exploit to repressive governments who can use it to spy on activists protesting their authority. (It's not unheard of for governments, including that of the U.S., to use exploits to gather both foreign and domestic intelligence.)* *

Andrew Auernheimer

An internet troll convicted of two consecutive computer crime felonies, Andrew 'weev' Auernheimer has over a decade of C, asm, Perl, and obnoxious IRC curmudgeonry under his belt. He is a liberty advocate and future federal prisoner of America.

__The hacker notifies the vendor, who may -- or may not -- patch.* __*The vendor may patch mission-critical customers (read: those paying more money) before other users. Or, the vendor may decide not to release a patch because a cost/benefit analysis conducted by an in-house MBA determines that it's cheaper to simply do ... nothing.* *

The vendor patches, but pickup is slow. It's not uncommon for large customers to do their own extensive testing -- often breaking software features that couldn't have been anticipated by the vendor -- before deploying improved patches to their employees. All of this means that vendor patches can be left undeployed for months (or even years) for the vast majority of users.* *

__The vendor creates an armored executable with anti-forensic methods to prevent reverse engineering. __This is the right way to deploy a patch. It's also manpower-intensive, which means it rarely happens. So discovering vulnerabilities is as easy as popping the old and new executable into an IDA Pro debugger with BinDiff to compare what's changed in the disassembled code. Like I said: easy.

Basically, exploiting the vast unpatched masses is an easy game for attackers. Everyone has their own interests to protect, and they aren't always the best interests of users.

Things Aren't So Black and White

Vendors are motivated to protect their profits and their shareholders' interests over everything else. Governments are motivated to value their own security interests over the individual rights of their citizens, let alone those of other nations. And for many information security players, it's far more lucrative to sell incrementally improved treatments of a disease's symptoms than it is to sell the cure.

Clearly, not all the players will act ethically, or capably. To top it all off, the original hacker rarely gets paid for his or her highly skilled application of a unique scientific discipline towards improving a vendor's software and ultimately protecting users.

So who should you tell? The answer: nobody at all.

White hats are the hackers who decide to disclose: to the vendor or to the public. Yet the so-called whitehats of the world have been playing a role in distributing digital arms through their disclosures.

Researcher Dan Guido reverse-engineered all the major malware toolkits used for mass exploitation (such as Zeus, SpyEye, Clampi, and others). His findings about the sources of exploits, as reported through the Exploit

Intelligence Project, are compelling:

> The so-called whitehats of the world have been playing a role in distributing digital arms.

- *None* of the exploits used for mass exploitation were developed by malware authors.
- Instead, all of the exploits came from "Advanced Persistent Threats" (an industry term for nation states) or from whitehat disclosures.
- Whitehat* *disclosures accounted for *100 percent *of the logic flaws used for exploitation.

Criminals actually "prefer whitehat code," according to Guido, because it works far more reliably than code provided from underground sources. Many malware authors actually lack the sophistication to alter even *existing* exploits to increase their effectiveness.

Navigating the Gray

A few farsighted hackers of the EFnet-based computer underground saw this morally conflicted security quagmire coming 14 years ago. Uninterested in acquiring personal wealth, they gave birth to the computational ethics movement known as Anti Security or "antisec."

Antisec hackers focused on exploit development as an intellectual, almost spiritual discipline. Antisec wasn't -- isn't -- a "group" so much as a philosophy with a single core position:

> An exploit is a powerful weapon that should *only* be disclosed to an individual whom you know (through personal experience) will act in the interest of social justice.

After all, dropping an exploit to unethical entities makes you a party to their crimes: It's no different than giving a rifle to a man you know is going to shoot someone.

> Dropping an exploit to unethical entities makes you a party to their crimes.

Though the movement is over a decade old, the term “antisec” has recently come back into the news. But now, I believe that state-sanctioned criminal acts are being branded as antisec. For example: Lulzsec's Sabu was first arrested last year on June 7, and his criminal actions were labeled “antisec” on June 20, which means everything Sabu did under this banner was done with the full knowledge and possible condonement of the FBI. (This included the public disclosure of tables of authentication data that compromised the identities of possibly millions of private individuals.)

This version of antisec has nothing in common with the principles behind the antisec movement I’m talking about.

But the children entrapped into criminal activity -- the hackers who made the morally bankrupt decision of selling exploits to governments -- are beginning to publicly defend their egregious sins. This is where antisec provides a useful cultural framework, and guiding philosophy, for addressing the gray areas of hacking. For example, a core function of antisec was making it unfashionable for young hackers to cultivate a relationship with the military-industrial complex.

> The only ethical place to take your zero-day is to someone who will use it in the interests of social justice.

Clearly, software exploitation brings society human rights abuses and privacy violations. And clearly, we need to do something about it. Yet I don’t believe in legislative controls on the development and sale of exploits. Those who sell exploits should not be barred from their free trade -- but they *should* be reviled.

In an age of rampant cyber espionage and crackdowns on dissidents, the

*only *ethical place to take your zero-day is to someone who will use it in the interests of social justice. And that's not the vendor, the governments, or the corporations -- it's the individuals.

In a few cases, that individual might be a journalist who can facilitate the public shaming of a web application operator. However, in many cases the harm of disclosure to the un-patched masses (and the loss of the exploit's potential as a tool against oppressive governments) greatly outweighs any benefit that comes from shaming vendors. In these cases, the antisec philosophy shines as morally superior and you shouldn't disclose to anyone.

So it's time for antisec to come back into the public dialogue about the ethics of disclosing hacks. This is the only way we can arm the good guys -- whoever you think they are -- for a change.

Wired Opinion Editor: Sonal Chokshi @smc90