

Jim Rapoza: Tech Directions

Requiem for a hacker

SECURITY INDUSTRY, LAWS STIFLE INDEPENDENT WHITE HATS



SECURITY HAS BECOME A VERY BIG BUSINESS IN IT over the past few years. You'd think its growth as a commercial market would have made all our information more secure. It hasn't.

Aside from the vendors that provide scanning, assessment and protection products, there are many specialized security consulting firms that will analyze your exposure and help secure your systems, as well as keep your company informed as new problems arise. With the growth of security as an industry, there have been many federal laws that aim to improve security standards and reporting requirements.

But does all this work better than it did a few years ago, when many researchers and hackers (people who need to figure out the inner workings of things, not bad guys) regularly looked for problems in commonly used applications and sites and reported on the problems they found, which often led quickly to fixes and resolutions?

One person who doesn't think so is prominent security hacker Rain Forest Puppy (better known as rfp), who recently announced that he will be stepping away from security research. You can find his announcement at www.wiretrip.net/rfp/txt/evolution.txt.

In case you don't know who rfp is, in the late 1990s he became one of the most respected hackers and researchers in the security community, discovering serious problems in products like Microsoft's IIS Web server and developing tools to assist in problem discovery. He became known for the even-handed way he handled disclosure of problems to vendors and the community. I still refer people to his excellent RFPolicy (www.wiretrip.net/rfp/policy.html) as a guideline for how researchers should deal with vendors when they find a security problem.

I remember being very impressed, at the Security Vulnerability Summit that eWEEK Labs hosted in 2000, by the collegial and cooperative discourse between rfp, looking every bit the modern hacker,

and the businesslike Steve Lipner, then the manager of Microsoft's Security Response Center.

But now rfp is walking away from it, or at least from free public security research, and I can't say that I blame him.

Now rfp is walking away from free public security research, and I can't say that I blame him.

I, too, don't like the way that security products and research have gone.

Just look at how the commercialization of security has changed things. As security firms became big commercial entities, they started to have big commercial clients. And these clients wanted special treatment. This has led to the common practice of security companies notifying their top clients of problems before noti-

fying the public. Giving a select few companies extra days of protection while leaving other companies vulnerable does not make the Internet more secure overall. Imagine the outcry if a police department were to notify special "gold" customers of dangerous felons roaming an area well before notifying everyone else.

I also agree with rfp when he talks about the move toward the "big box" of security solutions. Many customers want to buy a single overarching security product—a big box. They need one after they've laid off most of their security staffs. Owning a big box makes them think they've taken care of their problems. Never mind that this goes against everything that every security expert has recommended about securing IT resources.

Now many broad and sometimes-conflicting state, federal and international laws have made it harder on independent security researchers and hackers. Laws such as the state and federal DMCA's, the Patriot Act and EU anti-hacking bills leave security researchers facing legal consequences for everything from looking for problems in hosted applications to breaking encryption to running standard security tools. These concerns have led LaBrea anti-worm tool developer Tom Liston to pull it from his Web site and have led security researchers to seek the safety of large commercial security outfits.

The result of all this: There are fewer people looking for problems to help people, while there are still a lot of people looking for vulnerabilities to exploit.

It doesn't look good. But there's hope

that some will step up to follow in the footsteps of hackers like rfp. Hackers have to hack. And laws, fortunately, can be changed. And to rfp, thanks for all your work. You've helped to protect a lot of people from problems that vendors probably would have tried to hide. ☺

East Coast Technical Director Jim Rapoza is at jim_rapoza@ziffdavis.com.