technology review
Published by MIT

Tuesday, July 31, 2012

Hey, Hackers: Defense Is Sexy, Too

Is the computer security community so obsessed with demonstrating scary new attacks that it has neglected to improve defenses?
By Tom Simonite

Pleasing the crowd at the Black Hat and Def Con computer security conferences that took place in Las Vegas last week is relatively easy: simply hop on stage and confidently show how to compromise, or "pwn," a system that no one has hacked into before (see "Mobile Payment Chips Could Let Hackers into Your Phone").

Notoriety, cash, and multiple offers of work can be the rewards for those who demonstrate truly novel attacks. But some speakers at this year's events say that the obsession with breaking into systems has gone too far, and are calling for their community to show more interest in advancing defense techniques, which don't have such cachet.

At the same time, many experts say that existing defense technologies are too crude to deal with increasingly sophisticated computer break-ins that are often custom-built for a target and aimed at stealing valuable corporate data (see "The Antivirus Era Is Over"). Despite the billions spent on security products each year, most attacks on large companies are not detected until months or even years after they happen, according to a study published recently by Verizon.

"Modern detection systems are woefully poor at detecting the modern attacker," said John Flynn, known as Four, who works on intrusion detection systems at Facebook and previously led security operations at Google. "The data are really quite sad."

Flynn and others say that the excitement of showing off new attacks is partly to blame for the poor performance of defensive computer security technologies. Newly discovered vulnerabilities are usually quickly patched, but the cycle of finding and fixing flaws hasn't produced widely applicable defensive strategies, they say.

In a heavily oversubscribed talk at Black Hat last Wednesday, Flynn shared his ideas for new strategies that might better help detect when attackers have infiltrated a company's network. Existing defenses, such as firewalls and antivirus-style programs, explained Flynn, are focused on blocking an attack by detecting malicious code when it is deployed. Instead, he proposed, companies should draw on a wide range of data sources—seemingly innocent clusters of data from actions such as network traffic and files being updated—that together might suggest particular steps from another stage of an attack—for example, a hacker exploring a network in search of valuable data.

Ifatach Ian Amit, a researcher with computer security company IOActive, made a similar appeal to hackers and security industry workers in a Black Hat talk entitled "Sexy Defense."

"People are happy poking a bit of software and getting famous; it's fun, and when you take on a big vendor, you're the little researcher that could," Amit said. "But we need to expand the defensive strategy from just making fixes for a new attack and then waiting for the next one so we can respond again."

That piecemeal approach has created defenses that don't match the strategy or most of the

tactics of attackers, Amit said. His vision for defense involves searching more actively for signs of intrusion and also engaging in intelligence gathering and countersurveillance to check out suspicious but inconclusive evidence. Indeed, some of Amit's ideas about defense might even be called offense (see "Fighting Hackers without Sinking to Their Level").

Both Amit and Flynn acknowledge that their approaches require those protecting a company to build and maintain custom software and hardware systems. In reality, most of the people working in security for companies both large and small are not equipped with the necessary skills: they don't write code and are trained to operate only off-the-shelf security products such as firewalls.

A new prize on offer to hackers last week was also an attempt to inspire a renewed interest in defense. In contrast to the usual "bug bounties" some companies offer hackers who discover software flaws, Microsoft gave a $200,000 BlueHat Prize for new defense techniques capable of thwarting entire classes of attack.

The prize was awarded on Thursday night, in a Las Vegas nightclub, to Columbia University graduate student Vassilis Pappas, for a Kbouncer, a tool designed to foil a technique behind many new vulnerabilities known as prevent return-oriented programming. Two runners-up shared prizes worth $60,000. Pappas's work has already been incorporated by Microsoft into a toolkit offered to system administrators to protect Windows installations.

"We're asking the community to shift its thinking from attack to defense," said Mike Reavy, who leads the Microsoft Security Response Center, which is responsible for detecting and addressing new vulnerabilities in all the company's products. "Finding new flaws and fixing them will always be important, but it's not a long-term strategy."

Even with the BlueHat Prize, the cash and reputational rewards on offer to those who find new attacks will likely exceed those offered for defensive ideas for some time. However, Flynn and Amit are hopeful that the rewarding nature of playing defense will convert more hackers to their cause. "The wins feel really good when they happen," said Flynn, "and it's an intellectually stimulating problem."

Amit also suggested that working on defense requires greater technical mastery. "You can't just rely on the antivirus and firewalls, you start hacking people, processes, laws, and relationships," he said. "You keep getting challenged and having to learn about the world. It's really the essence of hacking."