

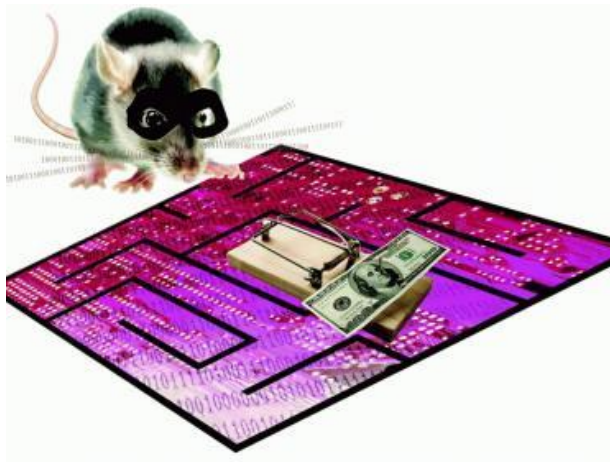
San Francisco Chronicle

Business Report The Chronicle with Bloomberg

November 30, 2011

<http://www.sfgate.com/cgi-bin/article.cgi?f=/c/a/2011/11/30/BUVP1M5245.DTL>

By James Temple



In late 2010, a team of Eastern European hackers began attacking the website of a Fortune 100 company.

They employed what's known as an SQL injection, manipulating the online forms where visitors enter information. The hope was to trick the underlying database into spitting out valuable corporate data.

They were sophisticated and persistent hackers, but kept tripping over roadblocks. The site continually slowed to a crawl. Their automated tools were thwarted by CAPTCHAs, those online boxes that force users to translate squiggly letters.

Finally, their computers were blocked from reaching the site. In effect, the hacker had been hacked.

That, at least, is the phrase employed by Mykonos Software, the Burlingame company behind this shadowy game of counterespionage. The 2-year-old firm's products detect Web intruders and steer them into virtual tar pits, slowing progress as they unwittingly reveal information that can be used to stop, identify or prosecute them.

Mykonos, which is getting increasing notice in the online security world, is one of the few companies offering these types of solutions for third-party websites. But in the face of escalating attacks and skyrocketing financial tolls, growing numbers of tech businesses and security groups are bolstering their own approaches to what some call "aggressive defense."

It's a deliberately artful term, however. There is a fine line between aggressive defense and outright offense, which begins to raise questions about legality and efficacy.

In either case, these approaches represent a markedly different tactic from simply setting up a firewall and patching holes after they're discovered or exploited. Analyst Wendy Nather calls that the "sitting duck" strategy.

"It's a very passive approach and, of course, it doesn't work very well," said Nather, research director for security at the 451 Group of New York.

In fact, hardly a week passes without some news of a costly or embarrassing online breach. In recent months, cyberattacks compromised the websites of Visa and MasterCard, knocked Sony's PlayStation Network offline for weeks, revealed the personal details of BART police officers and stole millions of dollars from Citigroup credit card accounts.

The specific defense strategies in any of these cases is unclear, but the broad trend suggests it's far too easy to break into or undermine websites. Mykonos chief executive David Koretz attributes it to a backward approach to security - reacting after attacks instead of acting to avoid them.

Studies also suggest corporate security priorities are severely out of whack. Research firm Gartner estimates that 70 percent of online attacks target Web applications, like e-mail, retail sites and banking services. Yet a Ponemon Institute survey found that nearly the same percentage of IT professionals say their companies spend more on corporate network security. In fact, 88 percent said the Web security budget falls below what the office spends on coffee. (It should, however, be pointed out that this survey was sponsored by security vendors.)

The security community is pushing for changes in various ways. Notably, the Open Web Application Security Project, an open source effort to create security tools and industry guidelines, is pursuing an "AppSensor" initiative to integrate automated "detection and response" systems into Web applications.

Scanning for signs

In the case of Mykonos, the company's software scans for telltale signs of hackers, such as manipulated online forms or modified cookies. Once flagged, the attackers are steered into the tar pits, where they can be tricked into revealing how sophisticated they are, where they are located and more.

In some cases, Mykonos might deliver a coup de grace in the form of a map of the hacker's neighborhood. It highlights nearby lawyers and delivers an ominous message like: "You're probably going to need some legal help."

But some security watchers note there are some risks to aggressive defense, which grow as it edges ever nearer to outright offense.

There are whispers about organizations going further than Mykonos by, for example, attempting



to physically damage or destroy the computer systems of their attackers. Industry observers declined to name any groups doing that.

One reason is it might well be illegal for individuals or corporations to play judge, juror and executioner in this [fashion](#). The other big risk of bragging about or pursuing offensive security measures is escalating conflicts with hackers.

"This is an area where a lot of us are very uncomfortable," said Heather Adkins, information security manager at Google. "I see an arms race building" if more companies adopt offensive security strategies.

She said that's a losing battle for businesses, because hackers "are more motivated and less restricted in what they can do."

Koretz recognizes that the law spells out clear boundaries for legitimate companies. But he insists the arms race is already well under way and that attackers clearly require no provocation beyond the lure of dollars.

As such, he believes the only successful security strategy is one that neutralizes that motive. The Mykonos software tricks hackers into wasting so much time and effort chasing dead ends that the economics of hacking start to break down, he claims.

"Hacking is fundamentally about dollars," he said.

Without addressing Mykonos specifically, Adkins said "aggressive defense" that stops short of blatant offensive tactics can be another useful tool in the security arsenal. But not all businesses will be able to take advantage because these techniques are difficult to automate.

Fixing key flaws

She thinks the more promising areas for improving Web security lie in fixing the fundamental flaws in the online architecture.

To take one example, security considerations weren't baked into the long-ago designed domain name system, which translates website names into the string of numbers denoting their location. But there is an effort under way to address that by moving to a new system of domain name security specifications.

"There is no silver bullet solution," Adkins said. "There is not one thing you can do or buy. You have to layer (solutions) upon each other."