To catch a hacker

Camarillo firm releases security system

STEPHEN NELLIS PHOTO

George Baldonado and Deborah Johnson of Camarillo-based Oasis Technology. The company has released a product called the Titan Cyber Security System, pictured, that blocks would-be hackers. The system is a self-learning tool, Baldonado said.

A small Camarillo IT firm is making its stand against the avalanche of hacking attempts that slows down Internet access on a daily basis.

Oasis Technology has released what it calls its Titan Cyber Security System. It's a black box that sits between your incoming Internet connection and existing network and acts like an eagle-eyed bouncer, creating rolling blacklists of would-be hackers.

The entire project got its start when Oasis CEO George Baldonado, a 30-year veteran of the IT business, noticed his own company's Internet was slow. He worked with Verizon, his Internet service provider, on the problem but couldn't find anything obviously wrong.

It turns out the pipes were clogged with hackers trying to get in. "We found out we were being hacked to the tune of one million hack attempts a day," Baldonado said. "It was eating up so much bandwidth that our legitimate users couldn't get through."

About 80 percent of the attacks were coming from China. The reason: There'd been a Canadian firm called Oasis Technology Ltd., with a similar web address, that made software for running ATMs and point-of-sale networks. The hackers were confused, targeting the Camarillo company and hoping to score sensitive financial data.

"Otherwise, how would they know about us?" said Deborah Johnson, chief financial officer at the firm.

At first, Baldonado tried writing a few simple scripts to stop the hack attempts. But the attacks would change faster than he could keep up. So he started designing a tool that would learn to recognize IP addresses that were acting shady and blacklist them temporarily, with ever-longer periods for known bad actors.

"This would be a self-learning tool that would track what kind of attacks were coming," he said. After a few months of testing, "it was alive. It was working."

It was a feat for the typical small IT shop, but not for Oasis. Baldonado founded the company in 1979 as a custom software outfit and has worked with many big names over the decades, including writing software for Verizon that is still in use.

"Back in those days, computers weren't that common," Baldonado said. "I had to focus on big companies in Los Angeles."

Over the years, Baldonado has had to be as inventive and tenacious as his new black boxes. The 1990s were a boom time, with companies spending big to deal with Y2K, the bug that crept up when early software programmers had represented the years of dates with two digits instead of four to save space. The result was that many systems would have thought Jan. 1, 2000 was Jan. 1, 1900.

"Y2K changed the whole fabric," Baldonado said. "The United States spent about a trillion dollars getting everything fixed. We even found for one customer that their elevators would have stopped."

The problem was that customers' software budgets were exhausted after fixing problems for Y2K. That created a drought for software shops that was followed by the burst of the dot-com bubble and the Sept. 11, 2001 terrorist attacks. "That tanked the whole industry. So we retooled ourselves," Baldonado said.

Oasis adapted to focus on corporate and government networks. It specializes in networks with tougher-than average security requirements, but it also has many small and mid-sized business clients as well. Customers include Amgen, the Camarillo Chamber of Commerce, Verizon and the Casitas Water District. "We're at the high end of the desktop support business," Baldonado said.

When Oasis started testing its Titan boxes with clients, it made some surprising findings. One was that the attacks came from odd places. Most of the attacks on Oasis came from China, but an oil-company customer saw mostly domestic attacks.

"Everyone is getting hacked," Baldonado said. "They just don't know it."

The sheer volume was also impressive. The reason attacks slow down Internet service comes from the basics of how the Internet works. Every device on the web has what's called an Internet Protocol, or IP, address.

And, in general, any IP address can ping any other address, either asking for an address or asking to be let in. While answering and rejecting these requests only takes a few milliseconds, those milliseconds add up when millions of bogus requests a day pile up.

Most routers and modems filter out the bogus requests, but those filters can clog. If you ever wonder why you inexplicably need to reset your home network, this is probably why, Baldonado said.

The problem is only set to get worse. There are currently about 4.6 billion IP addresses in existence, but the new scheme for assigning them means there could be 3.4×10^{38} addresses — each one a potential hacker.

The Oasis black box plugs in before an existing network and monitors the traffic, keeping track of which IP addresses are attempting hacks.

"It's this close to artificial intelligence on heuristics logic," Baldonado said. "We have a million different ways of slicing and dicing the data."

By Stephen Nellis
Staff Writer