Pulling the plug on huge hacking

July 4 2017, by Jill Leovy, Los Angeles Times

Hack attack. Wikipedia, CC BY-SA

Salim Neino had been waiting for something like WannaCry.

Fast, indiscriminate and disruptive, the computer infection locked up computers in British hospitals and was spreading across the world when Neino's company, Kryptos Logic, stepped into the ring.

One of his researchers found a so-called kill switch in the WannaCry code and pounced. "We put it in a triangle choke!" joked Neino, a mixed-martial-arts fan.

Not bad for a 33-year-old Lawndale native and Cal State Long Beach grad, who co-founded Kryptos eight years ago with $120,000.

The mid-May episode thrust the small Los Angeles cybersecurity company onto a world stage. At the same time, it has opened a new era of broad-scale ransomware attacks - a fact driven home last week when a second worm, exploiting the same methods as WannaCry, briefly seized computers worldwide again, this time hitting oil, electric and shipping operations.

Neino has been quick to capitalize on the business opportunities from his new prominence. But he has also tried to use this status as ransomware wrangler to push for policy changes - measures he says are needed to cope with this new landscape of cybermayhem.

Testifying before Congress between attacks, Neino spelled out his proposal for a cybersecurity "Richter scale" - a triage system to help the public prioritize threats - and warned lawmakers against underrating the peril.

With WannaCry, and the June 27 reprise of it, the world got off easy, he insisted: "They had the bomb, they didn't have the GPS."

Until May, Kryptos was just another little-known boutique cybersecurity company operating, as much as possible, "in stealth mode," Neino said. It does no marketing, employs no sales force and its workers guard their anonymity. The reason is that revenge hackers commonly target cybersecurity companies.

Genial, earnest and still fit from his wrestling days, Neino is the son of a Jordanian immigrant father and a Mexican American mother from Montebello. His father came to L.A. as a young man with no English but talent enough to rise in the region's aerospace industry.

Neino was raised speaking Arabic and Spanish, but he can't remember either language now. Maybe code took over that brain space, he said. He got his start as a self-taught teenage programmer, landed his first computer job at age 15, and became - after a sister - the second person in his family to go to college.

The background, he said, is typical of Angelenos his age raised by aerospace workers to whom cybertinkering came naturally.

After a few years as an independent cybersecurity specialist, Neino co-founded Kryptos while still in his twenties with friends-and-family seed money, and has used its revenue to expand ever since.

At first, Kryptos struggled. Neino could show potential clients that they had been hacked, but he couldn't convince them to care.

The problem is rife in cybersecurity, a vast but fuzzily defined industry sector worth perhaps hundreds of billions of dollars in the near future - if only its purveyors could explain what it's for.

People who are good at cybersecurity tend to speak in jargon; people who aren't good at cybersecurity can't understand them. Meanwhile, the fire hose of botnets and malware gushing through the Internet these days leaves victims feeling helpless. Throngs of companies peddle a mishmash of remedies: gadgets, software and services, in various combinations.

Then, on a lark, Neino joined a team that competed at the 2011 Defcon

19 hacking contest in Las Vegas and won a coveted Black Badge, a tchotchke shaped like a skull, almost actual size, designed to hang around the neck. The boost to Kryptos' reputation brought new clients and lucrative contracts.

Today, privately held Kryptos has about 25 employees - nearly all engineers spread out across the U.S. and Europe, nearly all male, many with self-taught hacking skills - and annual revenue in the tens of millions of dollars. Its young CEO has traded blue-collar Lawndale for an ocean-view home. The Black Badge is on display in his office.

The company gathers information about who is trying to hack its clients and why. Then it helps them decide how to fight back.

Day to day, its researchers spend their time reporting on malware to subscribers and tracking the tens of thousands of new malware codes that surface daily on the Web.

In essence, they operate like zoologists in the field: They detect malicious sequences by the signals they emit, catalog them and try to lure them into simulated targets so they can be dissected.

This is what Marcus Hutchins, a Kryptos researcher in the town of Ilfracombe on the Bristol Channel in southwest England, would have been doing on the morning of May 12 if he hadn't been on vacation. Neino was too - on his way to Italy for a long-planned vacation with his wife.

Neino had hired Hutchins last year after coming across his blog. An unemployed computer hobbyist and surfer, Hutchins impressed Neino with his skill and ethics. Despite his youth - Hutchins is 22 - Neino hired him to run one of his divisions.

Fortunately for Kryptos - and for unpatched Windows systems everywhere - Hutchins hadn't gone far from home.

As computers in Britain's hospitals locked up and companies in Europe started to report problems, Hutchins conferred with Neino, who was in a hotel in Munich, Germany, on his way to catch his plane to Venice, Italy. Hutchins began analyzing samples of the malware code, sharing information via Twitter with other cyber researchers.

WannaCry is a self-replicating worm that attacks a basic file-sharing protocol on older Windows operating systems. If successfully loaded, the ransomware spreads to any connected vulnerable terminal, locking files and demanding, in slightly broken English, a $300 to $600 ransom to release them.

The worm exploits a vulnerability embedded in the very bones of the world's most popular operating system. The code used in WannaCry, which can crack Windows systems, was stolen from the U.S. National Security Agency and shared on the Internet.

Like many in his industry, Neino knew that it was only a matter of time before ordinary bandits or terrorists put these military-grade spy tools to work. WannaCry, he realized, signaled that the moment had arrived.

From now on, he thought, vast sophisticated hacks, once limited to nation states, would be in reach of just about anyone.

Neino learned that Hutchins had found an unregistered domain to which WannaCry sent a signal prior to loading. Neither of them knew what it was for. But it was up for grabs.

Neino told Hutchins to "use best judgment" and headed to the airport.

By the time Neino got there, Hutchins had registered the domain, effectively throwing Kryptos' servers into the path of the oncoming attack. To both men's surprise, the domain functioned as a kill switch and stopped WannaCry from loading the ransom note in all subsequent infections.

With Kryptos controlling the domain, each new WannaCry infection produced a ping on its servers. So a stream of data was pouring in as the attack - now toothless - spread across the globe.

Neino couldn't log into Kryptos to see for himself because he had no secure connection and his plane was leaving. He flew over the Alps, two worries gnawing at him.

One was for Hutchins' safety. Because of blanket media coverage, Neino feared that Hutchins would be exposed and hackers would retaliate against him.

The other was for Kryptos' servers. Because the company had essentially inserted itself into WannaCry's protocol, Neino knew that law enforcement agencies might mistake the company for a source of the attack and seek to shut down its servers. That could inadvertently unleash the malware again.

Online again at last in his Venice hotel, he checked the dashboard, where tens of thousands of WannaCry's pings were piling up.

He didn't have time to marvel. Kryptos was under siege. Hutchins was being hounded. The story of the youthful hero who saved humanity from the world's biggest ransomware attack proved irresistible to aggressive British tabloids.

At the same time, hackers were attacking Kryptos. As soon as word of

the kill switch got out, a barrage of denial-of-service attacks were directed at the company's servers worldwide.

This "devilish flood" of malicious botnets and copycat hacks was the company's reward for stopping the worm, Neino said. He called some of the attackers "bandwagon jumpers" and said they probably just wanted to be pesky. But others were clearly trying to "take down the switch," he said - a serious threat.

Already, just as Neino had feared, two of Kryptos' servers had been mistakenly shut down by authorities in France, a common cyberfriendly-fire mishap.

His engineers pulled all-nighters. Neino spent his 10-day vacation hunched over his laptop in the hotel room, talking to security agencies, assuaging the media, managing his researchers and maintaining the kill switch. His wife made sure that he didn't forget to eat.

Attacks on Kryptos have continued for weeks. One recent botnet aimed at the company appeared to be coming from thousands of Russian routers, Neino said.

To the outside world, WannaCry quickly seemed overblown. One British publication suggested that it be renamed "What-a-wimp."

Its design was shoddy. Neino readily admits that Hutchins got lucky with the kill switch - ransomware usually doesn't have such a feature and it's not clear why this one did. Microsoft had patched a key vulnerability before the attack and subsequently released further patches, and Neino said the worm failed to load on most of the old Windows XP systems considered most vulnerable anyway.

Moreover, very few people paid the bitcoin ransom, which has yet to be

collected.

But at Kryptos, where the kill switch remains permanently under guard - "we own this baby now," Neino said - the picture is different. Neino said he has counted new WannaCry infections in the tens of millions - infections that Hutchins' quick action had rendered harmless.

Kryptos has a list of "every single person affected by WannaCry," he said. Among the would-be victims were major U.S. hospitals whose leaders may still have no idea, he told Congress.

"The brakes were fully on. This was residual smoke from the tires," Neino said.

Like WannaCry, last week's ransomware attack centered in Ukraine also seemed to quickly fizzle. It used the same stolen NSA forced-entry tool, locked computers and demanded bitcoin ransom, with similarly poor results.

But Neino said it spread even more quickly, infecting 2 million computers in the first hour. It also had the ability to steal credentials and gain access to even more machines.

Most different of all, it had no kill switch. Instead, the attack seemed to shut down by itself, Neino said, with domains that hosted its payload quickly going dark.

Using his data from WannaCry, Neino published a report late June 27 arguing that this new worm had even greater destructive potential.

By his own "Richter scale" measure, WannaCry might have rated a 7 and the new attack 7.2, said Neino, speaking as one raised in an earthquake zone. The pattern suggests "saber rattling, perhaps for a bigger event to

come," he said.

The day after the most recent attack, with theories swirling as to its purpose, Neino stressed a message that he'd given Congress after WannaCry:

Worry less about who did it and more about the problems such attacks expose, he said.

"If you leave the door open ... would it really matter ... who has done it?" he asked. "They do it because they can."