They predicted the 'WannaCry' ransomware cyberattack, so how come few listened?

May 18 2017, by Paresh Dave, Los Angeles Times

Misha Govshteyn and his colleagues at the cybersecurity start-up Alert Logic dropped all their projects about a month ago, except for one they deemed a graver threat than the rest.

Someone had stolen never-before-seen hacking tactics from the National Security Agency and posted them online. Working in shifts for 36 hours straight, dozens of Alert Logic engineers in Belfast in Northern Ireland, Cardiff in Britain, and Houston devoted their attention to analyzing the leaked computer code.

What they found could undermine the privacy of the crucial corporate files they protect for 4,000 media companies, retailers and app makers. They developed a way to stop their clients from falling victim to the spying and issued warnings to the public through blogs and social media.

Several security firms around the world echoed that sentiment, blasting alerts in mid-April instructing systems administrators to tighten defenses because the NSA leak was sure to lead to a cyberweapon, and signs of a brewing attack had emerged.

It's clear the advice didn't reach or sway everyone: The so-called WannaCry ransomware offensive seized an estimated 300,000 computers within the last week, with repairs and other associated costs possibly running into the billions of dollars globally.

WannaCry illustrates the challenge faced by cybersecurity companies as

data breaches, credit card theft and phishing become more common. Security researchers regularly sound the alarm - but they fear their warnings are getting lost in a sea.

The problem, they acknowledge, is partially their own making as researchers and firms sometimes overhype threats to gain publicity. But there also remains a gap between external advice and internal action across the corporate cybersecurity landscape.

This is a concern for Govshteyn and others in the industry. Even though WannaCry marked only a temporary inconvenience for most, cybersecurity experts continue to fear the next onslaught could take someone's life.

"What we're doing now with warnings by Alert Logic and other companies in the security industry clearly isn't working," Govshteyn said.

The answer, he says, could be governments holding companies accountable for failing to take proper precautions, especially in the face of warnings.

About a month ago, private researchers announced they had identified computers compromised by breach methods held by the NSA. The fact that they emanated from the intelligence agency was a sign to the researchers that the tactics were more likely than others to prove virulent and highly effective.

At that point, hackers aren't believed to have deployed a weapon such as ransomware to lock users' files. But they had an entryway to do so if they wanted.

"It's highly likely what we saw were precursors to WannaCry," said

Govshteyn, Alert Logic's co-founder and senior vice president of products.

Alert Logic quickly informed clients, including about two dozen customers whose security practices left open dangerous holes. Other information security companies shared news of thousands of infected computers.

Matthew Hickey, co-founder of Hacker House in Britain, said his teams had been tracking several similar leaks since late last year and saw this NSA-related batch as the most worrisome. As the days went on, Hacker House kept issuing ever-heightened warnings of a "Microsoft apocalypse."

The early detection should have led people to update their systems with a patch from Microsoft and adjust firewall settings, said Vladimir Vlaski, founder of Milwaukee firm BelowøDay.

Some heeded the advice. But many more apparently ignored it or weren't aware. The number of infected computers rose to more than 428,000 from 50,000 in five days, he said.

British computer security researcher Kevin Beaumont said people mocked his prediction that the NSA intrusion tactic would be used to set off a worm - malware that automatically crawls from computer to computer across networks. Many again sidestepped his concerns in the early hours of the eventual worm's launch last Friday. It wasn't until hours later, as computers worldwide fell into its grip, that more of the industry galvanized.

The chatter about the need to intensify security because of the NSA leak may have been drowned out by the news cycle surrounding President Trump in recent weeks, security consultants suspect. The lack of focus

on cybersecurity in some corners of the world outside of the U.S. may have also contributed to the damage.

People who were aware of the specter of WannaCry may have brushed aside the issue as overblown. Tiago Henriques, chief executive at Swiss company Binary Edge, can understand why. To many, people such as Henriques might just be the boy who cried wolf one too many times when no creature was lurking.

"It's very hard for us in the industry to work through all the noise, so you can imagine what it looks like to people outside," he said. "Every time a new vulnerability is released everyone tries to sell it as the most critical thing in the world when sometimes in reality they aren't so. I'm not surprised that sometimes people don't really listen to us anymore."

At Alert Logic, Govshteyn admits they certainly yelled fire unnecessarily to drum up customers in one case years back.

"And we made a decision we would never do it again," he said. "It wasn't trivial, but we added to the noise."

He suggested an impartial government institution perhaps could step in to prioritize threats. Until then, he described the closest thing as the Internet Storm Center - a global threat-sharing group sponsored by a for-profit technology training institute in Maryland.

Even if a warning comes from a source widely seen as credible, many of those affected by WannaCry may continue to defer upgrades, whether because of possible software malfunctions or complacency.

"It's a horrific idea to run outdated, unsupported systems in mission-critical environments," Govshteyn said. "But when someone has made bad decisions this many times, I wouldn't be expecting a warning to

matter much."

A test of whether they prove him wrong could soon. The same entity that released the NSA files last month proclaimed Tuesday that it would share more tactics to paying subscribers in the coming months.

Govshteyn said Alert Logic would subscribe, depending on the cost, and the cycle of analysis and warning would begin anew.