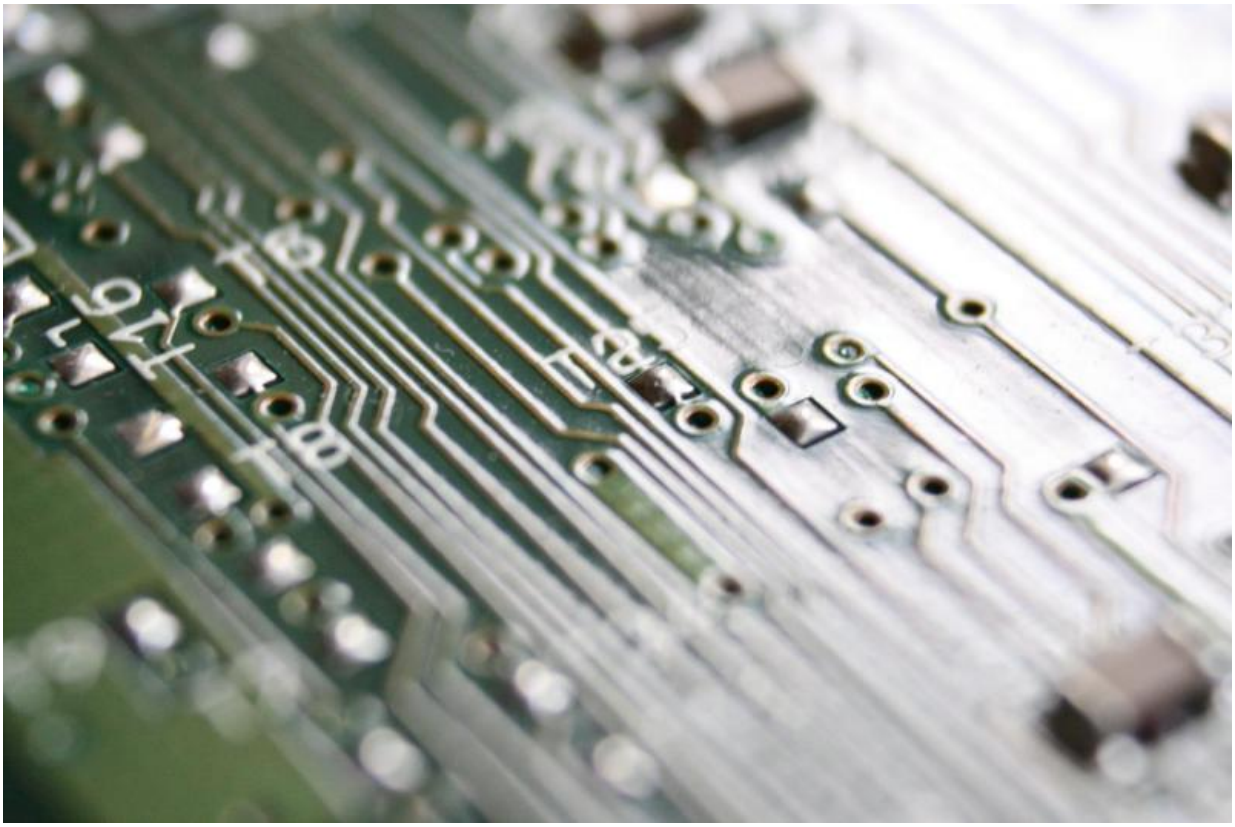
What's next after 'massive disruption' from cyber-attack? A view from the trenches

May 17 2017, by Nancy Dahlberg, Miami Herald



Credit: Public Domain

As the cyber-attack continues to spread around the globe causing massive disruption and damages for universities, hospitals, automakers and many other businesses including FedEx, only one thing is certain: It

won't be the last.

That's because the cyber criminals are running a multibillion enterprise with the help of ultra-sophisticated tools, said Yuri Frayman, co-founder and CEO of Aventura-based cybersecurity company Zenedge. The company, which launched in 2014 after two years of development, helps companies worldwide protect their web applications and networks against cyber-attacks with its proprietary technology.

"If this was not a wake-up call to the corporate world, I don't know what needs to happen next," said Frayman, offering his view from the trenches. "About 220,000 companies have been hit, and this is just what we know. We are seeing a massive disruption in the network operations across the globe," said Frayman, in an interview Monday.

None of the firms his company protects have reported any disruptions from the so-called "WannaCry" ransomware virus, he said. But as the attack has unfolded, Zenedge has been talking with industry security specialists around the globe about how they are mitigating the damage and seeking to stabilize large infrastructure companies.

What really worries Frayman is what comes next in this attack, and ones to follow.

Companies such as FedEx will throw everything at this problem in the next three or four days at an unbelievable cost, said Frayman, who has himself been expecting a FedEx delivery for the past two days. But less-sophisticated firms may may not even know a virus lurks in their system.

A second problem, he said, is the massive shortage of cyber-security experts. The enemies are hackers who are "years ahead."

Telecommuting also creates risk. "Ninety-eight percent of the world

population doesn't know if their home has been hacked. If I have your home, I can hack your corporate environment. Many people around the world work from home, and that is another black hole that is ready to explode."

The solution—beyond turning off the internet—is commitment to vigilance, he said. Generally, the largest financial services companies are very proactive, appropriating the proper budget, staff and training and putting key processes in place. But "take a step outside of that and you will see across the board that corporations have not taken this seriously."

Hiring a chief security officer is not enough, he said. "It's not about buying cyber insurance and hiring a couple of people—it's about discipline."

Having a dedicated staff and/or vendors whose single task is to secure and protect the company is key. So is continual staff training.

"You can't just be clicking anymore ... . Hackers are using very sophisticated tools to mimic regular emails you get every single day," he said. If you click on one that downloads a virus, it eventually could discover the system administration credentials. "Once (the hackers) know those, they can do whatever they want."

Zenedge currently has about 250 clients spanning the financial, ecommerce, gaming, healthcare and manufacturing industries worldwide and also protects large internet service providers. The company raised $6.2 million in September to finance its global expansion; in total it has raised $13.7 million in venture capital funding.

"Every single attack, every single malware, we take it apart, and we train our algorithyms to be able to pick up the behavior of an attacker," he said. "If you train a computer to think like a human, then you can protect

as many customers as we do without a need for a human interaction."