Case Study

Raytheon and Virsec Partner to Guard the Grid

With energy grids under constant threat of cyberattack, Raytheon is getting the technology of small, innovative software firms into the hands of big international customers.

The malware that blacked out parts of Kiev, Ukraine, was a ticking time bomb.

It slipped inside the networks of electrical substations through a flaw in an obscure device. It built back doors to other parts of those networks and waited. Then, at a time chosen by its programmers and written into its code, it destroyed. It commandeered circuit breakers, shut down relays and hobbled the control software.

The malware, known as both **CrashOverride and Industroyer**, showed how hackers not only understand the arcane networks of the energy industry, but are using that knowledge to carry out devastating cyber offensives. It also showed how urgently the keepers of critical infrastructure need to shore up their defenses.

To speed that along, Raytheon is working with innovative companies like Silicon Valley cybersecurity firm Virsec to license network-saving technology to government agencies and large enterprises including healthcare companies, financial institutions and utility providers. That partnership,answers a call in the **U.S. National Defense Strategy** for the defense industry to deliver new technologies faster. For Virsec, it also accelerates the long, difficult acquisition process smaller companies often encounter when breaking into the federal and international markets.

“Raytheon is clearly adept at changing that paradigm and bringing newer technologies and solution sets more quickly to its customer base,” said Ray Demeo, co-founder and chief operating officer of Virsec. “Without partners like Raytheon, the U.S. government would not be able to access essential and immediately needed technology. And this is important to all of us and its allies as citizens, the ability to change our defense posture. It really is a day-to-day battle.”

At the heart of the Raytheon-Virsec agreement is a defense against “memory-based” cyberattacks, or those that exploit weaknesses in legitimate applications, rather than installing malware. Well-known examples include the WannaCry and NotPetya ransomware attacks, which exploited a PC feature called Server Message Block that allows computers on a network to access shared resources such as printers.

Virsec calls its defense against memory-based attacks “Trusted Execution,” and it basically works like this: It learns what applications should and shouldn’t do, and when it sees an application executing an abnormal script, for example, it flags the activity and sends an alert that enables security to shut down the rogue function immediately.

The technology could fill a critical need, said John DeSimone, vice president of cybersecurity and special missions at Raytheon.

“Commercial tools from companies like Virsec can help bridge the gap for our global government and commercial customers and provide effective protection against the growing cyber threat,” he said.

About Virsec

Virsec is an innovative cyber security leader protecting organizations from today’s most sophisticated and damaging cyberattacks. Through its unique technology, Virsec definitively prevents zero-day threats, fileless attacks and memory corruption exploits that are invisible to conventional security tools. Virsec’s patented Trusted Execution™ system deterministically stops advanced security attacks in real-time, delivering unprecedented accuracy, without false positives. Virsec is headquartered in San Jose, California with a global presence in Europe, Asia, and Australia.

Author: John Zaremba, Raytheon

virsec

226 Airport Parkway, Suite 350 • San Jose, CA 95110

Email: info@virsec.com • Phone: (877) 213-3558 • Web: www.virsec.com • Twitter: virsecsystems