Hackers implant 'digital grenades' in industrial networks to be set-off when your company does corruption

BY TIM JOHNSON
tjohnson@mcclatchydc.com

HANOVER, MARYLAND The United States pioneered the use of cyberweapons when it shattered Iran's nuclear centrifuges in 2010 but such devastating cyber tools have spread and are now boomeranging to make industrial digital sabotage a growing concern to the United States.

The weapons can wreak destruction and kill people. Experts say cyber weapons can turn off power grids, derail trains, cause offshore oil rigs to list, turn petrochemical plants into bombs and shut down factories.

Twice in the past eight months, federal authorities have issued public warnings that foreign hackers are seeking to penetrate the U.S. electric grid and other parts of national critical infrastructure. The intent: Insert digital grenades that are dormant until the hacker's sponsor pulls the pin.

In a computer lab at Dragos, an industrial cybersecurity firm in Hanover, Maryland, founder and chief executive Robert M. Lee and his researchers chart the activities of foreign hacking teams plotting industrial sabotage. They say hackers are developing new, more sophisticated, cyberweapons at a quickening pace, and growing bolder in the process "My intel team is tracking eight different teams that are targeting infrastructure around the world," said Lee, 30, who spent five years working at the National Security

Agency and the Pentagon's Cyber Command before forming his company three years ago.

Lee said his company tracks operations and techniques but does not verify which nations deploy the teams. The top U.S. spy, though, does point a finger of blame. In his annual assessment to Congress in February, Director of National Intelligence Dan Coats said that Russia, China, Iran and North Korea pose the greatest cyber threats to the United States.

"What we're seeing almost exclusively maps to nation states and intelligence teams," Lee said.

Lee and other cyber experts said industrial cyber sabotage will be a facet of future wars. Already, they see foreign hackers probing U.S. networks that control natural gas, petrochemical plants, power grids, liquid fuel distribution networks, ports and other industrial facilities.

"Adversaries want to hold our infrastructure at risk. They are seeking to establish persistent, sustained presence in infrastructure networks. They are preparing the battlefield today so that if needed they can attack in the future," said Paul N. Stockton, a former assistant secretary of defense for homeland security who is now managing director of Sonecon LLC, an economic and security advisory firm in Washington.

U.S. and Israeli cyberwarriors blazed the trail on industrial cyber sabotage when they used the Stuxnet digital worm to cause centrifuges at Iran's Natanz nuclear facility to spin out of control and shatter, inflicting a major setback on Iran's efforts to enrich uranium to power nuclear weapons and reactors.

More recently, demonstrations of destructive cyber sabotage have piled up.

Russian hackers took down three regions of the Ukrainian power grid in late 2015, causing an outage for several hours that hit 225,000 customers, drawing hardly a peep internationally.

“No senior government leader anywhere in the world came out and even admonished the attack. Forget attribution,” Lee said. “It kind of set a precedent of it being an allowable thing.”

A new attack, again believed to be from Russia, hit a Ukrainian transmission substation in late 2016 that caused three times more power loss than the attack a year earlier.

But high-decibel warnings about industrial vulnerability are growing louder, partly due to public U.S. government alerts but also due to work that Lee and his team at Dragos have done in pulling the veil on a cyberattack that could have caused a major explosion at a petrochemical plant in Saudi Arabia late last year.

Hackers targeted a key component at the petrochemical plan – its safety system.

Such systems guard against high heat, pressure or machinery that operates at too fast speeds. Hackers attempted to disable equipment made by a French supplier, Schneider Electric, at the Saudi plant, specifically its Triconex safety instrumented system controllers. There was no misinterpreting their goal, Lee said. They wanted to trigger an explosion.

“That was the first time malware was ever designed to kill people,” Lee said, referring to malicious computer code. “By targeting that safety system, there’s no reason to do that other than to try to kill people. It is extremely black and white.”

Robert M. Lee, the founder and chief executive of Dragos, an industrial cybersecurity firm, stands before a mockup of an industrial system at his Hanover, Maryland, headquarters.
Tim Johnson tjohnson@mcclatchydc.com

The only reason the hackers didn't trigger a massive explosion at the Saudi plant, Lee said, is that they made "one simple coding error. It's very obvious that they just messed up."

Since reverse engineering the hackers' code, Lee said Dragos has detected signs that the hacking group is operating far outside of the Middle East, their initial target, and have targeted different kinds of safety systems.

Concerns about foreign hacking of U.S. critical infrastructure often centers on possible attacks on the electric grid, a decentralized system that comprises more than 3,000 power companies. Any regional outage could cause distress, and even fatalities, depending on length.

"If you were to impact the power grid in the middle of winter in the Northeast, you could have a significant lasting effect there," said John Harbaugh, chief operating officer of R9B, a Colorado Springs, Colorado, cybersecurity firm with roots in the Defense Department.

Last October, the Department of Homeland Security and the FBI issued an alert that foreign hackers had targeted "energy, water, aviation, nuclear, and critical manufacturing sectors." Private cybersecurity companies, such as FireEye, a Milpitas, California, cybersecurity company that also investigated the Triconex attack, blamed North Korea for the probing.

Then on March 15, DHS and the FBI issued an alert saying that Russian government hackers had launched "a multistage intrusion campaign" into U.S. nuclear and other energy facilities, using sophisticated tools to implant digital code and hijack networks, carefully covering tracks as they worked. The U.S. government hasn't said how successful its attempts to thwart such intrustions have been.

Larger utilities have been beefing up their cyber defenses, though, and any power disruption is likely to be only regional.

"I have more concern about Washington D.C. losing power for 30 minutes than I do about the North American power grid going down," Lee said, noting that the patchwork, distributed nature of U.S. power generation offers it some resiliency.

While a limited regional outage could alarm citizens, Lee is far more concerned about foreign hackers hitting gas pipelines, petrochemical plants, transportation networks and high-end manufacturing plants, including pharmaceutical companies. Gas pipeline companies don't operate with the rigorous standards and regulations that restrict power companies, he said.

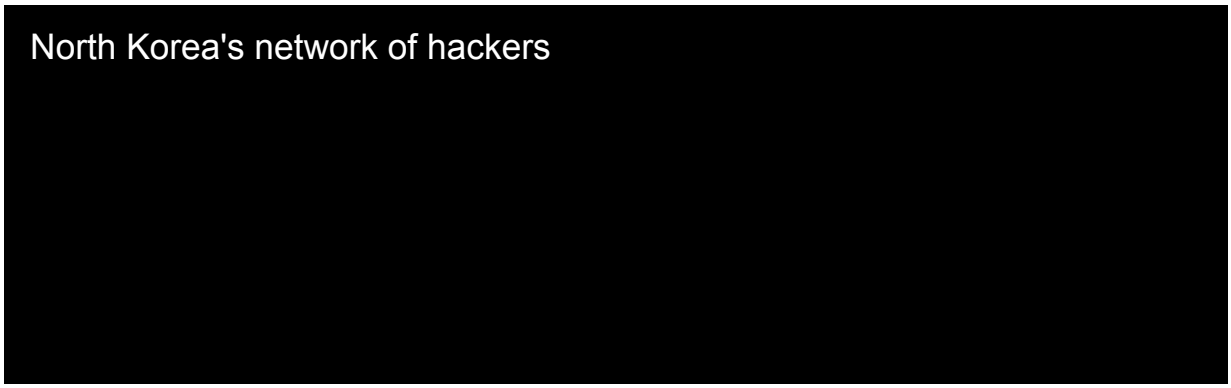
Other industrial experts said foreign nations are attempting to put military cyber arrows in their quills at a more rapid pace.

"The amount of time the attackers are taking to develop and test these attacks is shrinking," said David Hatchell, an expert on industrial digital systems expert who is a consultant at San Francisco-based Industrial Cyber Secure.

Getting digital worms inside target plants and factories is only one phase of an attack, he said: "Once they are inside the plant … how long does it take to develop, test and execute the attack?"

For the U.S.'s part, the Pentagon's Cyber Command has offensive cyber weapons capable of wreaking destruction on an enemy nation, U.S. officials say But it hasn't offered a display of its strength since hitting Iran in 2010. And consultants like Stockton say U.S. industries must prepare resiliency in the face of cyberattack, letting foreign nations steep in worry over what comes next.

"They know they are at risk of a counterstrike by the United States," Stockton said.



North Korea may be politically isolated, but the country is suspected of having thousands of hackers capable of carrying out global cyberattacks, like the attempts in 2016 and 2017.

By McClatchy

Tim Johnson: 202-383-6028, @timjohnson4

Robert M. Lee, chief executive of Dragos, says his Hanover, Maryland, cybersecurity firm is actively tracking eight different groups around the globe that are trying to breach industrial networks and electric grids and implant cyberweapons.

Robert M. Lee, chief executive of Dragos, says his Hanover, Maryland, cybersecurity firm is actively tracking eight different groups around the globe that are trying to breach industrial networks and electric grids and implant cyberweapons. **Tim Johnson** tjohnson@mcclatchydc.com