In Persian Gulf, computer hacking now a cross-border fear

September 12 2017, by Jon Gambrell

Tony Cole, Vice President of FireEye Inc., a cybersecurity firm headquartered in Milpitas, California, speaks at the FireEye Cyber Defence Live conference, Tuesday, Sept. 12, 2017, in Dubai, United Arab Emirates. State-sponsored hacks have become an increasing worry among countries across the Persian Gulf. They include suspected Iranian cyberattacks on Saudi Arabia to leaked emails causing consternation among nominally allied Arab nations. (AP Photo/Kamran Jebreili)

From suspected Iranian cyberattacks on Saudi Arabia to leaked emails causing consternation among nominally allied Arab nations, state-sponsored hacks have become an increasing worry among countries across the Persian Gulf.

Defending against such attacks has become a major industry in Dubai, as the city-state home to the world's tallest building and the long-haul airline Emirates increasingly bills itself as an interconnected "smart city" where robots now deliver wedding certificates.

They fear a massive attack on the scale of what Saudi Arabia suffered through in 2012 with Shamoon, a computer virus that destroyed systems of the kingdom's state-run oil company.

"It was and still is the worst physical attack we've ever seen," said Tony Cole, a vice president at FireEye Inc., a cybersecurity firm headquartered in Milpitas, California. "Destruction was what the adversary had in mind."

He added: "These are going to get worse as we look at more and more nation states that have some capability and quite literally they don't care how they look on the world stage."

Iran was the target of much of those fears and a point of discussion at an event Tuesday that Cole's company held in Dubai. The Islamic Republic developed its cyber capabilities in 2011 after the Stuxnet computer virus destroyed thousands of centrifuges involved in Iran's contested nuclear program. Stuxnet is widely believed to be an American and Israeli creation.

Iran is believed to be behind the spread of Stuxnet in 2012, which hit Saudi Arabian Oil Co. and Qatari natural gas producer RasGas. The virus deleted hard drives and then displayed a picture of a burning American flag on computer screens. Saudi Aramco ultimately shut down its network and destroyed over 30,000 computers.

A second version of Shamoon raced through Saudi government computers in late 2016, this time having the destroyed computers display

a photograph of the body of 3-year-old Syrian boy Aylan Kurdi, who drowned fleeing his country's civil war. Suspicion again fell on Iran.

But Iran isn't the only country in the region apparently with capabilities. An Emirati activist named Ahmed Mansoor became famous in August 2016 when he worked with security experts to reveal three previously undisclosed weaknesses in Apple's mobile operating system from him being targeted with a phishing text message he didn't click on.

Tony Cole, Vice President of FireEye Inc., a cybersecurity firm headquartered in Milpitas, California, speaks at the FireEye Cyber Defence Live conference, Tuesday, Sept. 12, 2017, in Dubai, United Arab Emirates. State-sponsored hacks have become an increasing worry among countries across the Persian Gulf. They include suspected Iranian cyberattacks on Saudi Arabia to leaked emails causing consternation among nominally allied Arab nations. (AP Photo/Kamran Jebreili)

Mansoor and others believed the United Arab Emirates was behind him being targeted, as it involved so-called "zero day" exploits that can be worth over a million dollars each. Mansoor was arrested by UAE authorities in March for his online posts.

In a more recent case, Qatar alleges hackers using iPhones in the UAE broke into the website of its state-run Qatar News Agency and in April planted inflammatory comments attributed to its ruling emir, Sheikh Tamim bin Hamad Al Thani. That hack later spiraled a short time later into the ongoing boycott of Qatar by the UAE, Saudi Arabia, Bahrain and Egypt. The UAE has denied being responsible for the hack.

Asked Tuesday about the Qatar News Agency hack by The Associated Press, Cole said: "It was a fascinating instance ... of politics moving into the cyberespionage realm." He declined to elaborate, saying: "I don't have information I wish to cover on that one."

Around the same time, a group began publishing embarrassing emails from the account of the Emirati ambassador to the United States, suggesting a tic-for-tat hack. Qatar has denied being involved.

But all that focus on government computers may distract from a bigger threat on the horizon.

As more household devices like coffeemakers and refrigerators find themselves connected to the internet, determined hackers can use them as a means to launch major attacks in the Gulf and elsewhere. That was the case during the October 2016 attack on Dyn Co., a firm that manages internet traffic, which caused outages to sites including Twitter, PayPal, Pinterest, Reddit and Spotify.

"My kitchen can become a hacker's paradise tomorrow," warned Kamran Ahsan, the senior director of digital security solutions for

telecommunications firm Etisalat.