Voice of America

December 18, 2015

Could IS Turn Next to Cyber War?

by Sharon Behn

The power is out. Gas stations are out of gas. Factories are going haywire.

It sounds like an action movie, but some analysts tell VOA that U.S. industries need to significantly ramp up their cyber security or risk having the Islamic State (IS) hack, attack and create mayhem inside their systems.

"This is definitely a threat to the U.S. government and other western governments, but also to our industrial control systems — the ones that run our manufacturing plants, moving energy across the country, that have vulnerabilities," said Bob Gourley, the former chief technology officer of the Defense Intelligence Agency.

Unlike cyberattacks by Russia and China, Gourley said, groups like IS are less interested in just extracting information and more interested in disrupting essential systems.

"They are going to want to cause mischief and grab attention, so destroying equipment or changing information that makes us question our own systems," said Gourley, who heads the firm Cognitio and is publisher of ThreatBrief.com.

As yet, he added, IS militants are not as capable as some criminal networks or rival nations, "but IS has more capabilities that any other terrorist organization that I know of. And they can gain more."

Protecting government systems

So far, IS has established itself as a leader in using Internet-based communications and social media to both send encrypted information and recruit thousands of people from more than 80 countries around the world.

"We are in a new age of this threat," Gourley said, "and the most important thing is we need to defend our systems better than they are currently being defended."

Clifton Triplett, recently named the Office of Personnel Management's senior cyber and information technology adviser, said he is already working to limit any kind of IS breach into the government department.

"I think what I have to do is … assume that, at some point in time, they may be successful," Triplett said at a conference organized by Bloomberg Government. "So how do I minimize the impact of their success? Right now, that really comes into access control."

OPM suffered a major hack earlier in 2015, resulting in the disclosure of private information of some 21.5 million people, including those who applied for security clearances.

Anticipating IS

But Al Berman, president and CEO of Disaster Recovery Institute International, which covers IT disasters, said it would be dangerous to assume that IS would stop at communication and marketing.

"This is not an unsophisticated organization. And if we look at it that way, we are vastly underestimating their capabilities," Berman told VOA.

One path of attack that IS could take, Berman said, would be to siphon money from institutions — perhaps in the U.S., perhaps in the Middle East — in order to increase their funding as the extremist group's oil and tax money streams start drying up.

"Money is incredibly important, and they will find other means if we shut down their traditional means," Berman said.

And IS does not have to do the hacking itself, it just needs to buy the information from hacking-obtained information auctions on the dark web.

Berman said IS could start to further refine their "social engineering" or "emotional marketing" techniques, basically by using the Internet in more sophisticated ways to track down and entice potential young recruits.

Vulnerable universities

For that, IS could hack into universities or buy information on the dark web from universities that have already been hacked.

According to Privacy Rights Clearinghouse, a California-based nonprofit that focuses on privacy protection, in the last five years hackers have accessed more than 2.5 million records from colleges and universities in the United States alone.

John Matherly, founder of Shodan, a search engine for Internet-connected devices, said exploiting student information would be far more likely than an IS attack on a facility such as a water treatment plant.

"Universities and educational institutions tend to have the worst security by far because they have these giant IP ranges. So students use a public IP address that anyone can see, and everything is exposed," Matherly said.

'Low-hanging fruit' for hackers

Conversely, complex Internet-connected control systems — such as those in water treatment plants, office buildings, factories, traffic lights, and solar power farms — are not always difficult to access, but they are difficult to compromise.

"There are devices that have no authentication. You don't need to provide a user name or a password. You can just access it; you can connect to it and talk. But there is a difference between connecting to a device and knowing what to do with it when you do," Matherly told VOA.

"It is important to separate the ability to access a control system from the ability to damage that system," he said. "The more likely scenario is that someone logs in and runs different commands and by accident causes it to fail."

But hackers such as IS do not have to be sophisticated to be damaging, Matherly said. Unpatched webservers, unprotected utility software accounts, individuals not keeping up with security updates, and even Instagram accounts could be easily attacked.

"Control systems are expensive and a long-term effort," Matherly said. "I am sure they are already looking into it, but if you are only looking for attention, it is much more effective to go after low-hanging fruit, and there is plenty out there."

---

http://www.voanews.com/content/islamic-state-cyber-war/3109289.html