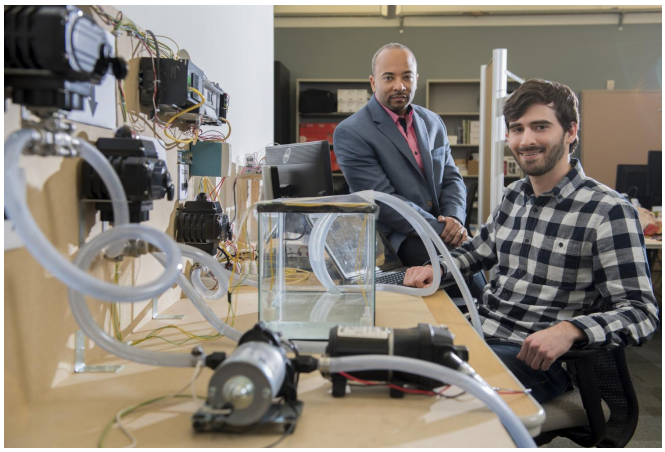
# Simulated ransomware attack shows vulnerability of industrial controls

13 February 2017



Georgia Tech researchers have developed a new form of ransomware that can take over control of a simulated water treatment plant. The simulated attack was designed to highlight vulnerabilities in the control systems used to operate industrial facilities. Shown are (left) Raheem Beyah, associate chair in the Georgia Tech School of Electrical and Computer Engineering, and David Formby, a Georgia Tech Ph.D. student. Credit: Christopher Moore, Georgia Tech

Cybersecurity researchers at the Georgia Institute of Technology have developed a new form of ransomware that can take over control of a simulated water treatment plant. After gaining access, they were able to command programmable logic controllers (PLCs) to shut valves, increase the amount of chlorine added to water, and display false readings.

The simulated attack was designed to highlight vulnerabilities in the control systems used to operate industrial facilities such as manufacturing plants, water and wastewater treatment facilities, and building management systems for controlling escalators, elevators and HVAC systems. Believed to be the first to demonstrate ransomware compromise of real PLCs, the research is scheduled to be presented February 13 at the RSA Conference in San Francisco.

Though no real ransomware attacks have been publicly reported on the process control components of industrial control systems, the attacks have become a significant problem for patient data in hospitals and customer data in businesses. Attackers gain access to these systems and encrypt the data, demanding a ransom to provide the encryption key that allows the data to be used again.

Ransomware generated an estimated $200 million for attackers during the first quarter of 2016, and the researchers believe it's only a matter of time before critical industrial systems are compromised and held for ransom.

"We are expecting ransomware to go one step farther, beyond the customer data to compromise the control systems themselves," said David Formby, a Ph.D. student in the Georgia Tech School of Electrical and Computer Engineering. "That could allow attackers to hold hostage critical systems such as water treatment plants and manufacturing facilities. Compromising the programmable logic controllers (PLCs) in these systems is a next logical step for these attackers."

Many industrial control systems lack strong security protocols, said Raheem Beyah, the Motorola Foundation Professor and associate chair in the School of Electrical and Computer Engineering and Formby's faculty advisor. That's likely because these systems haven't been targeted by ransomware so far, and because their vulnerabilities may not be well understood by their operators.

Formby and Beyah used a specialized search program to locate 1,400 PLCs of a single type that were directly accessible across the internet. But most such devices are located behind business

systems that provide some level of protection - until they are compromised. Once attackers get into a business system, they could pivot to enter control systems if they are not properly walled off.

"Many control systems assume that once you have access to the network, that you are authorized to make changes to the control systems," Formby said. "They may have very weak password policies and security policies that could let intruders take control of pumps, valves and other key components of the industrial control system."

In the past, control systems weren't designed for connection to the internet, and many users of the systems assume they aren't on the public network and therefore not susceptible to attack. Control systems may also have connections that are unknown to operators, including access points installed to allow maintenance, troubleshooting and updates.

"There are common misconceptions about what is connected to the internet," said Formby. "Operators may believe their systems are air-gapped and that there's no way to access the controllers, but these systems are often connected in some way."

To launch the research, the researchers identified several common PLCs in use at industrial facilities. They obtained three different devices and tested their security setup, including password protection and susceptibility to settings changes. The devices were then combined with pumps, tubes and tanks to create a simulated water treatment facility. In the place of chlorine normally used to disinfect water, the researchers used iodine. They also added starch to their water supply, which turned bright blue when a simulated attack added iodine to it.

"We were able to simulate a hacker who had gained access to this part of the system and is holding it hostage by threatening to dump large amounts of chlorine into the water unless the operator pays a ransom," Formby said. "In the right amount, chlorine disinfects the water and makes it safe to drink. But too much chlorine can create a bad reaction that would make the water unsafe."

Vulnerabilities in control systems have been known for more than a decade, but until the growth of ransomware, attackers had not been able to benefit financially from compromising the systems. As other ransomware targets become more difficult, Beyah believes attackers may turn to easier targets in the industrial control systems.

"It's quite likely that nation-state operators are already familiar with this and have attacks that they could use for political purposes, but ordinary attackers have had no interest in these systems," he said. "What we hope to do is bring attention to this issue. If we can successfully attack these control systems, others with a bad intention can also do it."

In addition to improving password security and limiting connections, Beyah says operators of these devices need to install intrusion monitoring systems to alert them if attackers are in the process control networks. Beyah and Formby have launched a company to make their strategies for protecting systems broadly available to control system operators.

Provided by Georgia Institute of Technology