Issued 2/23/17

New Ransomware Could Poison Your Town's Water Supply if You Don't Pay Up

A new form of ransomware, created by cybersecurity researchers at the Georgia Institute of Technology, was able to gain control of a simulated water treatment plant and threaten to shut off the water supply or poison it with increased amounts of chlorine. The ransomware, demonstrated at the 2017 RSA Conference in San Francisco, allowed researchers to access programmable logic controllers (PLCs), giving them the ability to shut valves, control the level of chlorine in the water, and display false readouts, a press release said. Given the increase in Internet of Things (IoT) and other connected systems in the industrial space, ransomware such as this could have dire consequences.

The research is believed to be the first successful demonstration of ransomware controlling actual PLCs, according to the release. The goal of the work was to highlight weaknesses in the systems that control such critical aspects of day-to-day life, such as water treatment plants, HVAC systems, and building management. Ransomware is typically used to encrypt data like hospital records or business files until the victim agrees to pay a monetary ransom. However, researchers at Georgia Tech believe that these industrial systems could be next in line. "We are expecting ransomware to go one step farther, beyond the customer data to compromise the control systems themselves," David Formby, a Ph.D.

student in the Georgia Tech School of Electrical and Computer Engineering, said in the release. "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." Raheem Beyah, associate chair in the School of Electrical and Computer Engineering, noted in the release that many real-world industrial systems don't have security in place to deal with ransomware, as they haven't been widely targeted by it yet and some of their vulnerabilities may not be fully understood. Many of the PLCs and control systems that were located by the researchers were accessible once they had access to the neighboring business systems. "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 in the release. "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." One of the core problems is that many operators make the assumption that their systems aren't connected to the internet, or that they are air-gapped, Formby said in the release. But, there are often connections for maintenance or other activities that may not be well understood.

To perform their test of the ransomware, the university researchers combined some PLCs with pumps, tubes, and tanks to make a simulated water supply. Instead of chlorine, the release noted, they used iodine, and put starch in the water so it would turn blue if it came in contact with the iodine. "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 release. "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." Nation-state actors and militaries have been using offensive cyber weapons to attack industrial systems for years, with programs like Stuxnet being used to take down nuclear centrifuges in Iran. However, ransomware adds a financial element to these type of attacks, and the money could be motivation to push more attackers to target these kinds of systems.