April 15, 2015

Targeted attacks on industrial control systems surge

Number of attacks are small, but outcomes could be catastrophic

FEATURED STORY **BY RODIKA TOLLEFSON, THIRDCERTAINTY**

When most of Turkey recently went dark for 10 hours in a massive power blackout, cyber criminal activity was among the suspected causes. While terrorism did not turn out to be the culprit, an increase in targeted attacks on industrial control systems in recent years make that scenario quite plausible.

Industrial control systems (ICS) — used in sectors such as energy, oil and critical manufacturing — had traditionally relied on passive defenses, such as architecture segmentation, firewalls and "air gapping" embedded devices.

But as the number of Internet-facing embedded devices and control systems rises, so does the number of targeted attacks by cyber criminals.

Featured Infographic: *Industrial controls under siege*

"Over the last couple of years, we've seen the development of a focused effort to attack industrial control systems, and attackers are more aware of industrial control system protocols, components and exploits," says Michael Assante, training lead for ICS and SCADA (supervisory control and data acquisition) security at the SANS Institute.

He says that while most attacks on these systems are still nontargeted, cyber criminals are increasingly honing their techniques to hack ICS, including through

traditional methods such as watering hole attacks, spear phishing and trojanized software.

Homeland Security's Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) responded to 245 incidents in fiscal 2014, a third of those in the energy sector. (Many more incidents go unreported, according to ICS-CERT.) Of the reported incidents, 55 percent involved advanced persistent threats or sophisticated actors.

The number of attacks is small compared to typical cyber incidents, but their potential outcomes are much more catastrophic.

"The motivation of the people targeting industrial control systems are often completely different from the vast majority of hacking that happens on the Internet," says Kurt Stammberger, senior vice president of market development at Norse Corp., a security company that provides live attack intelligence via 8 million sensors deployed across the Internet.

"Typical hacking is profit- or revenge-driven, but something targeting industrial control systems has a much more scarier motivation behind it," he says.

Outdated technology

Unlike typical computers and operating systems, embedded devices used in industrial control systems don't update every two to three years. The majority of the devices are five to 10 years old, built in the days when security was not a major concern.

"A lot of the systems have no capabilities to handle updates online, and even if patches exist, they have to be applied manually," Stammberger says.

The variety of hardware architecture, operating system platforms and communication protocols are adding to the complexity of monitoring those systems.

"Because they're so heterogeneous, it's hard to have a one-size-fits-all security protocol," says James Blaisdell, world-renowned expert on embedded security and CTO of Mocana, a security company specializing in smart connected devices.

Plethora of exploits

While targeted attacks on industrial control systems often are highly customized, the actors — frequently sponsored by nation-states — are using many of the usual techniques.

A watering hole attack, for example, can be used on a website of a vendor, infecting the computers of top engineers when they go to download a product spec sheet. Spear phishing can be used to attack the general business

network and understand the target, then infiltrate the ICS.

Free IDT911 white paper: *Breach, Privacy and Cyber Coverages: Fact and Fiction*

"Because we're seeing more control systems on the Internet, you can use general scanning techniques to identify and fingerprint control systems," Assante says. "You can quickly identify if it's a vulnerable version and may already have an existing exploit, or you can weaponize your own exploit."

Even basic tools like advanced Google searches can be used to look for these devices. And hackers are smart — they look for the easiest way to get in, Blaisdell says.

"Some of the attacks are real trivial," he says. "They don't have to work hard to get in."

Blaisdell notes that oftentimes, attacks on ICS are collateral damage. A bad actor may be hacking into a television set at a lab, for example, and not even know it.

"They think they're attacking a PC but they're actually attacking a device," he says. "They can take over the system and have it join a botnet … and it can cause unintended consequences."

Long way to go

There are encouraging signs that the industry is moving in the right direction. Blaisdell, for example, says Mocana is working with many clients who are taking a security-first approach with their devices.

And Assante is seeing an increased interest across industries in the SANS' ICS security curriculum. He points to the oil industry as an example.

"They're putting together industrial control systems security teams, with both information security folks and engineers, and making them available to the assets," he says.

But across the board, the amount of funding allocated to cybersecurity is slim. In a 2014 survey of 268 respondents from the ICS sector, SANS Institute found that 30 percent of organizations are only allocating 1 percent to 5 percent of the corporate budget to cybersecurity.

At the same time, the survey found that the number of suspected security breaches has increased to 40 percent, from 28 percent in 2013.

"In general, the industry is underinvesting in security and not moving quickly enough to cultivate the talents and tools we need for this problem," Stammberger says. "We're losing this fight, and we're losing this fight in a big

way, fast."

More on emerging best practices:

5 data protection tips for SMBs

What SMBs need to know about CISOs

Protecting your digital footprint in the post privacy era

Posted in Cybersecurity, Data Security, News & Analysis