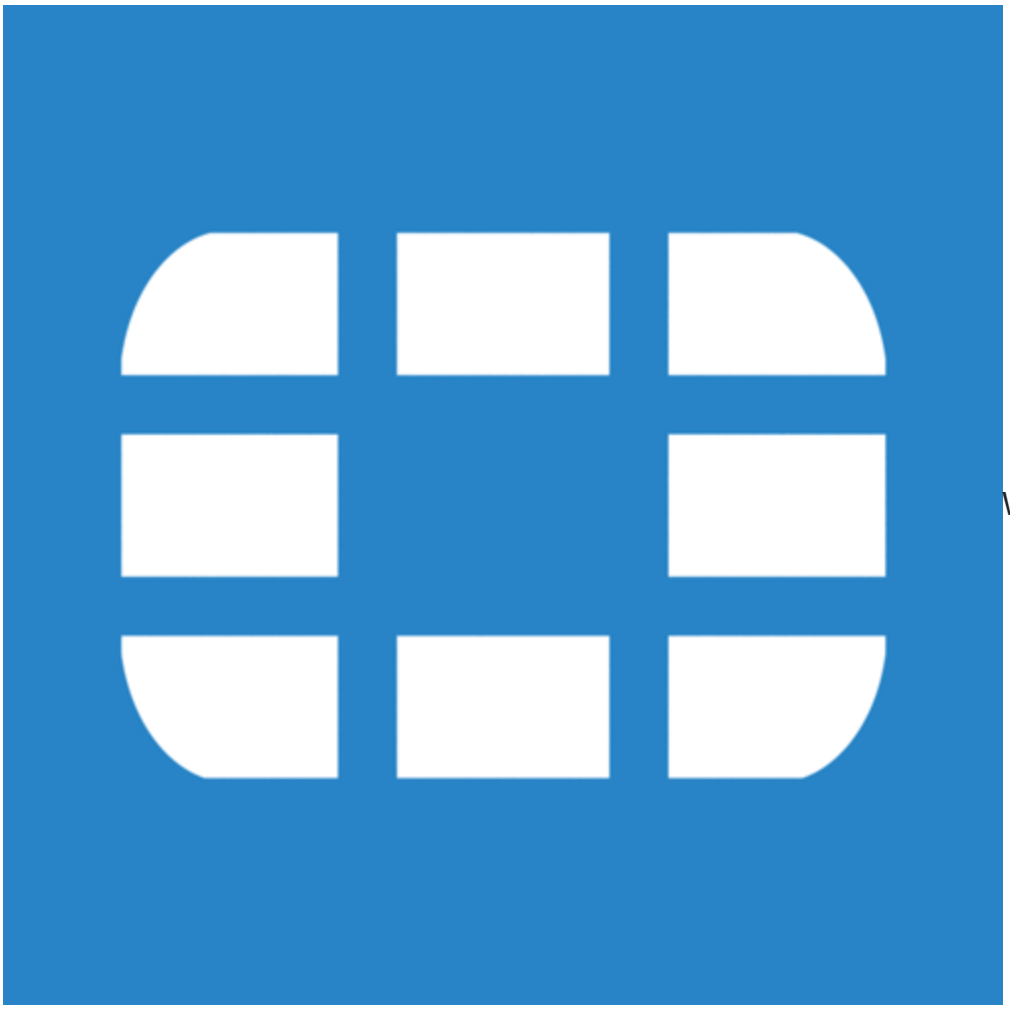
SCADA Security Report 2016

fortinet.com/blog/threat-research/scada-security-report-2016

April 5, 2016

FortiGuard Labs Threat Research

By Ruchna Nigam | April 05, 2016



While attackers are showing greater interest in both direct and indirect targeted attacks at Industrial Control Systems, it is perhaps a good time to assess where we stand with regards to protecting these systems.

Industrial Control Systems (ICS) are systems that control and monitor physical processes like the "transmission of electricity, transportation of gas and oil in pipelines, water distribution, traffic lights, and other systems used as the basis of modern society."

In recent years, the Industrial Control Systems (ICS) upon which much of our critical infrastructure and manufacturing industry depends have come under increasingly frequent and sophisticated cyber-attacks. In part, this is a consequence of the inevitable convergence

of Operational Technology (OT) with Information Technology (IT). As in all spheres of computing, the advantages of increased network connectivity through open standards such as Ethernet and TCP/IP, as well as the cost savings derived from replacing dedicated proprietary equipment with off-the-shelf hardware and software, come at the cost of increased vulnerability.

However, while the impact of a security breach on most IT systems is limited to financial loss, attacks on ICS have the added potential to destroy critical equipment, threaten national security, and even endanger human life.

With this critical distinction also comes a troubling difference in the profile and motivations of potential attackers. While the lion's share of modern cybercrime is motivated by financial reward, let's have a look back on the attackers' intentions in 2015 to find out more about why they wanted take down these ICS systems. The significant ones are highlighted below:

The First Hacker-caused Power Outage, in Ukraine

On 23rd December, 2015, a power outage was experienced across several regions in Western Ukraine due to blackouts in 57 power substations. This outage was first attributed to "interference" in the monitoring system by one of the affected power companies, but was later confirmed to be caused by a "hacker attack" on their Industrial Control Systems (ICS). The cause for the blackouts was confirmed by the Ukrainian CERT (CERT-UA) on 4th Jan, 2016 and is believed to be "the first power outage proven to have been caused by a cyberattack".

The attack was conducted in a sophisticated, well-planned manner as a 3-stage process consisting of:

- Infection of the systems through spear-phishing emails with MS Office documents as attachments. The documents contained malicious macros.
- Takedown and Recovery Prevention by wiping system files from the control systems.
- Distributed Denial of Service (DDoS) attacks targeted at the different power companies customer service centers using a barrage of fake calls, thereby delaying the company finding out about the problem.

The malware used in these attacks has been linked to the BlackEnergy malware family that has been around since 2007, other variants of which were also found collecting SCADA infrastructure information in 2014.

Confirmation of ICS Reconnaissance Attacks in the US

In December 2015, two reports on ICS attacks in the US revealed that they were reconnaissance attacks, i.e. attacks done with the intention of gathering intelligence rather than causing disruption.

The first report confirmed a previously unconfirmed attack on the Bowman Avenue Dam in New York in 2013. Although the dam wasn't compromised, the attack was focused at gathering queries and searches on the infected machines, possibly for targeted reconnaissance. It was also confirmed to have been attributed to Iranian hackers.

Similarly, the analysis of a computer belonging to a contractor of Calpine, "America's largest generator of electricity from natural gas and geothermal resources," revealed that it had been compromised and attackers had stolen Calpine company information. The stolen information was found on one of the attacker's FTP servers being contacted by the infected systems. The stolen information included usernames and passwords that could remotely connect to Calpine's networks, and detailed engineering drawings of networks and 71 power stations across the US.

Compromised SCADA Systems for Sale in the Underground

Internet forum posts offering to sell compromised SCADA systems were found in underground forums, complete with a screenshot of the compromised system and even three French IP addresses and VNC passwords. The authenticity of these credentials hasn't been confirmed. However, this introduces the very real possibility of ready-to-use vulnerable SCADA systems becoming another commodity that can be readily bought in the underground.

These attacks are only three cases among many others. According to **The ICS-CERT Monitor Newsletter: Oct 2014 - Sept 2015**, a total of **295** incidents were reported to the ICS-CERT in fiscal year 2015. The highest number of reported incidents were targeted at Critical Manufacturing infrastructures (97), followed by the Energy sector (46). The rise in attacks at Critical Manufacturing systems compared to 2014 was attributed to a widespread spear-phishing campaign that primarily targeted companies in that sector, along with limited targets in other sectors.

One of the top challenges for organizations to secure ICS is, as detailed above, the sophistication of today's cybercriminals. However, there are additional challenges, such as industry-specific systems, regulations, and practices. Most industrial control systems come from very different vendors and run proprietary operating systems, applications, and protocols (GE, Rockwell, DNP3, Modbus). As a result, host-based security developed for IT is generally not available for ICS, and many network security controls developed for common enterprise applications and protocols do not offer much in the way of support for those used by ICS.

Based on the facts listed in the ICS-CERT Monitor Newsletter article, here are some security recommendations organizations can use to avoid making headlines:

- **Beware of phishing emails**: As convincing as a phishing email might seem, good antivirus software could add another layer of security by warning about malicious attachments. Spear-phishing emails have been found, in practice, to have been used in all attacks, making it as popular in the ICS world as it is in the enterprise world. To quote a related incident, a spear-phishing attack was reported to the ICS-CERT that involved attackers making use of a social media account to post as a prospective candidate for employment. Using this account, attackers managed to gather information such as the name of the company's IT manager and current versions of active software from employees of the critical infrastructure asset owner. Following this, employees were sent an email with the supposed candidate's resume attached as 'resume.rar'. The attachment contained a piece of malware that successfully infected the employees' systems, but was fortunately prevented from spreading to or impacting control systems.
- **Logging and Regular Network Scanning**: Logs are a great way of monitoring activity on systems, and help investigators put together the various pieces of the puzzle in the event of an incident. They can also serve as early detectors of infection. Log maintenance is highly recommended to ICS sysadmins for the same reason. Finally, regular Network Scanning is another security best-practice that can serve as an early indicator of an infection.

The good news is that, in recent years, the inherent problems and vulnerabilities of ICS have become more widely recognized, and first steps have now been taken to rectify them.

One way this is occurring is through the help of government bodies such as the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) in the US, and the Centre for Protection of National Infrastructure (CPNI) in the UK, both of which publish advice and guidance on security best practice for ICS.

Another way is through the definition of common standards such as ISA/IEC-62443 (formerly ISA-99). Created by the International Society for Automation (ISA) as ISA-99, and later renumbered 62443 to align with the corresponding International Electro-Technical Commission (IEC) standards, these documents outline a comprehensive framework for the design, planning, integration, and management of secure ICS.

Apart from standardization, security vendors have begun to step up to the challenge of securing critical infrastructures. Fortinet's own solution, Rugged, has been designed to address the challenges unique to these ICS systems, brought upon by

- industry-specific systems, regulations and practices
- environmental conditions and

- distributed, remote locations

More information about Fortinet Rugged can be found here: (http://www.fortinet.com/solutions/critical-infrastructure-scada.html)