ARE INDUSTRIAL CONTROL SYSTEMS THE LATEST WEAPON IN MODERN WARFARE?

Submitted by: Nuvias (Wick Hill)
Wednesday, 10 February 2016

By Barry Mattacott, marketing director, Wick Hill (https://www.wickhill.com/) Group

Are industrial control and SCADA (Supervisory Control and Data Acquisition) systems the new frontier, not just for cyber-crime but also for cyberwar? Until recently, when you were at war with a country, you sent in your bombers. First they hit the military targets. Once they had finished those off, they would hit infrastructure, with attacks designed to destroy industry and demoralise the civilian population.

Electricity production, oil and gas, even water and waste services would all be targeted. However, nowadays, you don't need brute force to turn the lights off. This was recently demonstrated by hackers attacking The Ukraine, who succeeded in knocking out power supplies to up to 1.4 million residents through the social engineering attack known as spear phishing. An infected Word document was used to introduce BlackEnergy malware into critical systems.

http://www.bankinfosecurity.com/ukrainian-power-grid-hacked-a-8779/op-1

It was also social engineering which introduced that classic piece of industrial control malware, Stuxnet. It is now widely believed that Stuxnet was originally developed by an American/Israeli alliance, specifically to attack the control systems within Iran's nuclear industry. It eventually destroyed around 20% of Iran's centrifuges. The belief is that it was introduced into their system via an infected USB stick. Statistically, 60% of found USB sticks get plugged straight in, with this rising to 90% if the USB stick has a recognizable logo on it.

https://en.m.wikipedia.org/wiki/Stuxnet

More recently, researchers revealed a vulnerability in the Chrysler Jeep which caused the virtual recall of 1.4 million vehicles. It was demonstrated that a hacker could wirelessly access the control systems of the Jeep with the potential to disable the brakes and steering. Although a recall notice was issued, owners were sent a USB stick that allowed them to apply an update themselves without the need to take the vehicles back to a dealer. Chrysler also implemented network level security protection to block the exploit on the Sprint cellular network that connects their cars to the Internet.

http://www.wired.com/2015/07/jeep-hack-chrysler-recalls-1-4m-vehicles-bug-fix/

Let's not stop at cars, let's think big - The Great Train Robbery 21st Century style. Now they can steal the whole train! A hacking team has discovered vulnerabilities within the control systems used in train networks worldwide that could allow attackers to cause derailments and even steal a whole train.

https://www.rt.com/usa/327514-absolutely-easy-hacking-train-systems/

Other worrying hacking incidents include The Slammer Worm, which affected critical infrastructure as diverse as emergency services, air traffic control, water systems, ATMs, electrical companies, and a nuclear power plant’s process computers and safety display systems.

So why are these system all so vulnerable? It’s probably due to a number of widely held misconceptions which were highlighted in research by Kaspersky Lab entitled ‘Five Myths of Industrial Control Systems Security.’

http://media.kaspersky.com/pdf/DataSheet_KESB_5Myths-ICSS_Eng_WEB.pdf

1. Myth
Industrial control systems are not connected to the outside world.

Fact:
Most industrial control systems have eleven connections to the Internet.

2. Myth
We are safe because we have a firewall.

Fact
Most firewalls allow "any" service on inbound rules.

3. Myth
Hackers don't understand SCADA.

Fact
More and more hackers are specifically investigating this area.

4. Myth
We are not a target.

Fact
Stuxnet showed us that just because you weren't the intended target of industrial hacking, doesn't mean you won't become a victim.

5. Myth
Our safety system will protect us.

Fact
The chances are that your safety and control is using the same operating system with the same vulnerabilities.

Conclusion
Little recognised, dangerous, seriously disruptive, disabling, potentially lethal, and not widely defended against, industrial control and SCADA systems have the potential to be the new front line in modern warfare. Instead of brute force, countries can be softened up by the loss of essential infrastructure and services.

Infrastructure providers, utility companies, transport companies and any organisation whose disruption could cause serious problems, as well as governments themselves, need to look much more seriously at how to defend against such cyber- attacks. Or there could be serious consequences for national security.

About the author

Barry Mattacott is marketing director of Wick Hill (https://www.wickhill.com/) Group, which is based in Woking, Surrey and Hamburg Germany. Wick Hill Group is part of Rigby Private Equity (RPE), a subsidiary of Rigby Group Investments, an independent company within Rigby Group plc. Specialist distributor Zycko (http://www.zycko.com/) is also part of RPE, and in co-operation with Zycko, Wick Hill can offer a pan-European service which provides a common proposition and consistent delivery for vendor and reseller partners covering 13 countries.

Users of products sourced through Wick Hill include most of the Times Top 1000 companies, in addition to many non-commercial organisations, government departments and SMEs across all business sectors. Through its channel partners, the company has delivered IT solutions to more than a million users world-wide.
Wick Hill currently has offices in Woking, Surrey, with sister offices in Hamburg.

ENDS
For further press information, please contact Annabelle Brown on 01326 318212, email pr@wickhill.com, Wick Hill https://www.wickhill.com