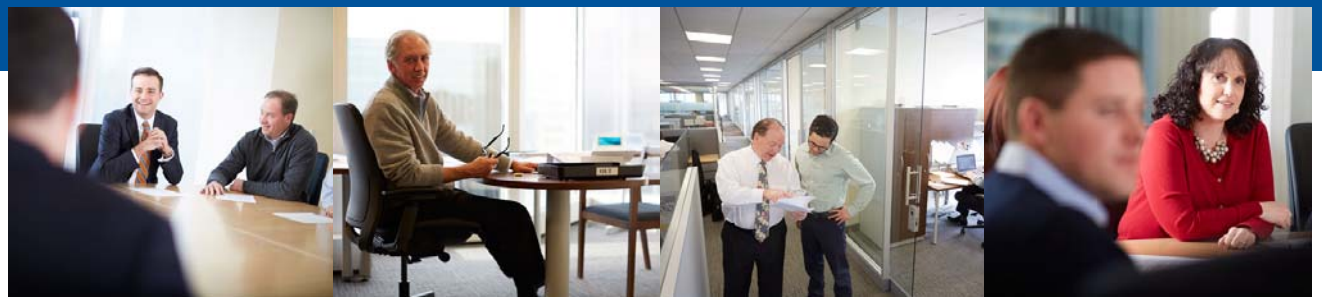
SCHNEIDER DOWNS

INFORMATION SECURITY RISK ADVISORY SERVICES

AIR GAPPED SCADA & ICS NETWORKS NOW THREATENED FROM RANSOMWARE



8/18/2016

Big Thinking. Personal Focus.

SCHNEIDER DOWNS

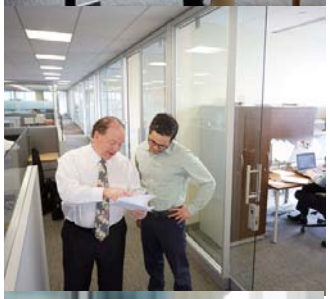
Schneider Downs Information Security Risk Advisory Services

AIR GAPPED SCADA/ICS NETWORKS NOW THREATENED FROM RANSOMWARE

- In July, Rockwell Automation issued an alert that Ransomware malware posing as a Rockwell Automation software update was distributed as "Allenbradleyupdate.zip" posing as a legitimate Rockwell Allen Bradley patch.
- It appears this malware is targeting the electricity energy sector. This is one of the first of its kind specifically targeting commercial utility systems. There are no known victims at this time.
- This attack, like the 2010 Stuxnet Iranian SCADA attack, proves that even air gapped networks are vulnerable to malware infections through malware passed via laptop or USB file transfer.

SCHNEIDER DOWNS

Schneider Downs Information Security Risk Advisory Services



Schneider Downs recommendations:

- Obtain product software and firmware only from official vendor download portals.
- Limit Admin credentials and review often.
- Minimize attack surfaces by segmenting via VLAN and segregating sensitive networks from general operational network via Firewall/ACL routers, starting with blocking all ports/IP addresses, then allow only what services/addresses that are needed to operate.
- Maintain timely data and system snapshots and back-ups. Test restoration from these back-ups.
- Analyze network traffic against known indicators of compromise (like beaconing to known controller IP addresses).
- Implement employee awareness training of malware vectors such as Phishing attacks.