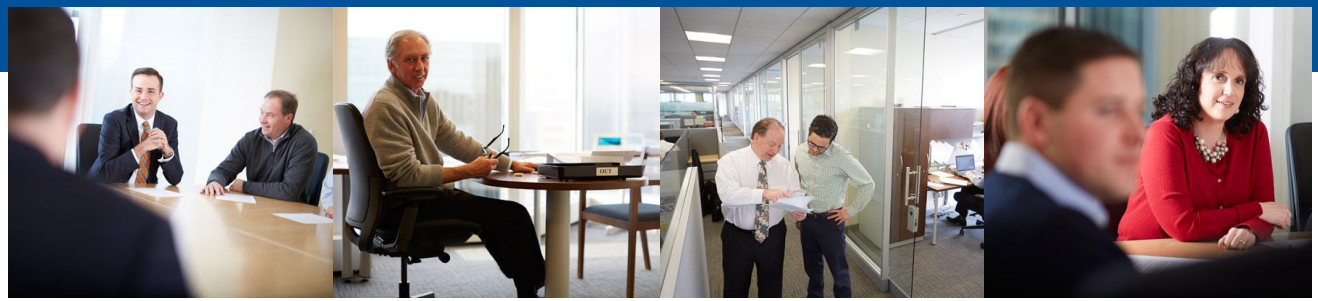
SCHNEIDER DOWNS

INFORMATION SECURITY RISK ADVISORY SERVICES

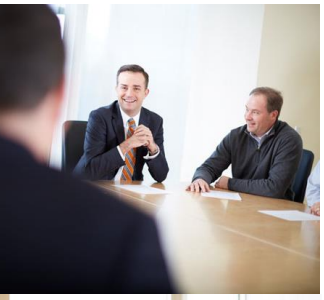
NEW SCADA Malware "SFG" used to attack European Power Plant
Pokémon GO Vulnerabilities
Major Windows Print Spooler Vulnerability
MEDJACK2—Hijacked Medical Devices



7/18/2016

Big Thinking. Personal Focus.

SCHNEIDER DOWNS



Schneider Downs Information Security Risk Advisory Services

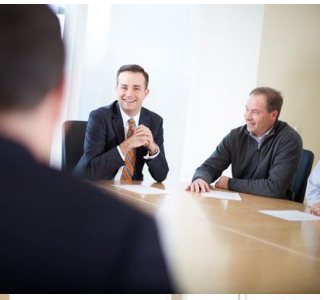
At least one European power plant was attacked this month with a new SCADA malware this month dubbed "SFG."

SFG:

- Believed to be derived from earlier SCADA malware "Furtim"
- Exploits older Windows vulnerabilities CVE-2014-4113 and CVE-2015-1701 that affect Microsoft servers.
- Highly sophisticated in its anti-virus and malware detection evasion.
- Suspected by some experts to be Eastern European state-sponsored.
- SFG can be utilized to deliver pay load and/or steal data.

SCHNEIDER DOWNS

Schneider Downs Information Security Risk Advisory Services

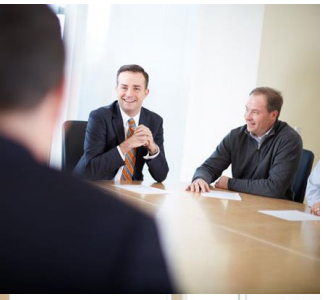



New Popular Pokémon GO Application May Open Children's Accounts to Hacking:

- Pokémon GO, Android & iOS based game is all the rave with pre-teens and young teens today. The game mixes real-world live interactive player GPS treasure mapping with aspects of Pokémon game.
- Pokémon GO App gives application access to take pictures, video, access location data, text messaging, find and use accounts on the phone.
- Multiple malicious Android versions on the Internet that contain Trojan, DroidJack, giving hackers full control of user's phone.
- Only trust Apps from the Apple App Store and Google Play.

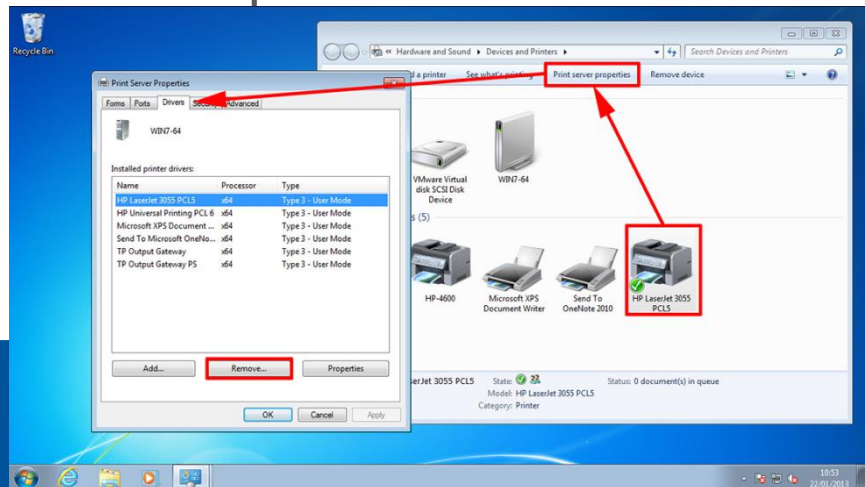
SCHNEIDER DOWNS

Schneider Downs Information Security Risk Advisory Services

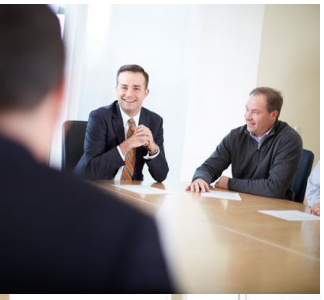


Critical Microsoft Print Spooler Bug can Allow Hackers to Infect All Versions of Windows:

- Microsoft in July launched a patch for a critical security flaw in Windows Print Spooler (CVE-2016-3238) that allows hackers to install Trojans on victims' devices when connecting to fake printers.
- All the Hacker has to do is get a victim to load the alleged hacker print driver by posing as a new network printer, or trick a user into loading it via web download or email attachment.
- Download and update all your Windows updates as of 7/12/16 to patch the bug.



SCHNEIDER DOWNS



Schneider Downs Information Security Risk Advisory Services

TrapX Security Company discovers three instances of medical device hacking in 2016.

- Many medical devices run on out-of-service software that is vulnerable to attack and three such attacks were reported this month.
- The affected hospitals had no idea they were attacked.
- One hack was of a respirator's PC running on old Windows XP.
- Another was a lab fluoroscope work station.
- The last was an X-ray machine running on Windows NT.
- Schneider Downs recommends that health care providers scan their networks for out-of-date vulnerable software running on their medical devices.
- All medical devices running expired end of life/end of service software such as Windows XP should be addressed by security professionals to mitigate patient and clinical risk.