Power & Utility Industry Threat Intelligence Spring 2015

Brent Huston

Security Evangelist & CEO

@lbhuston

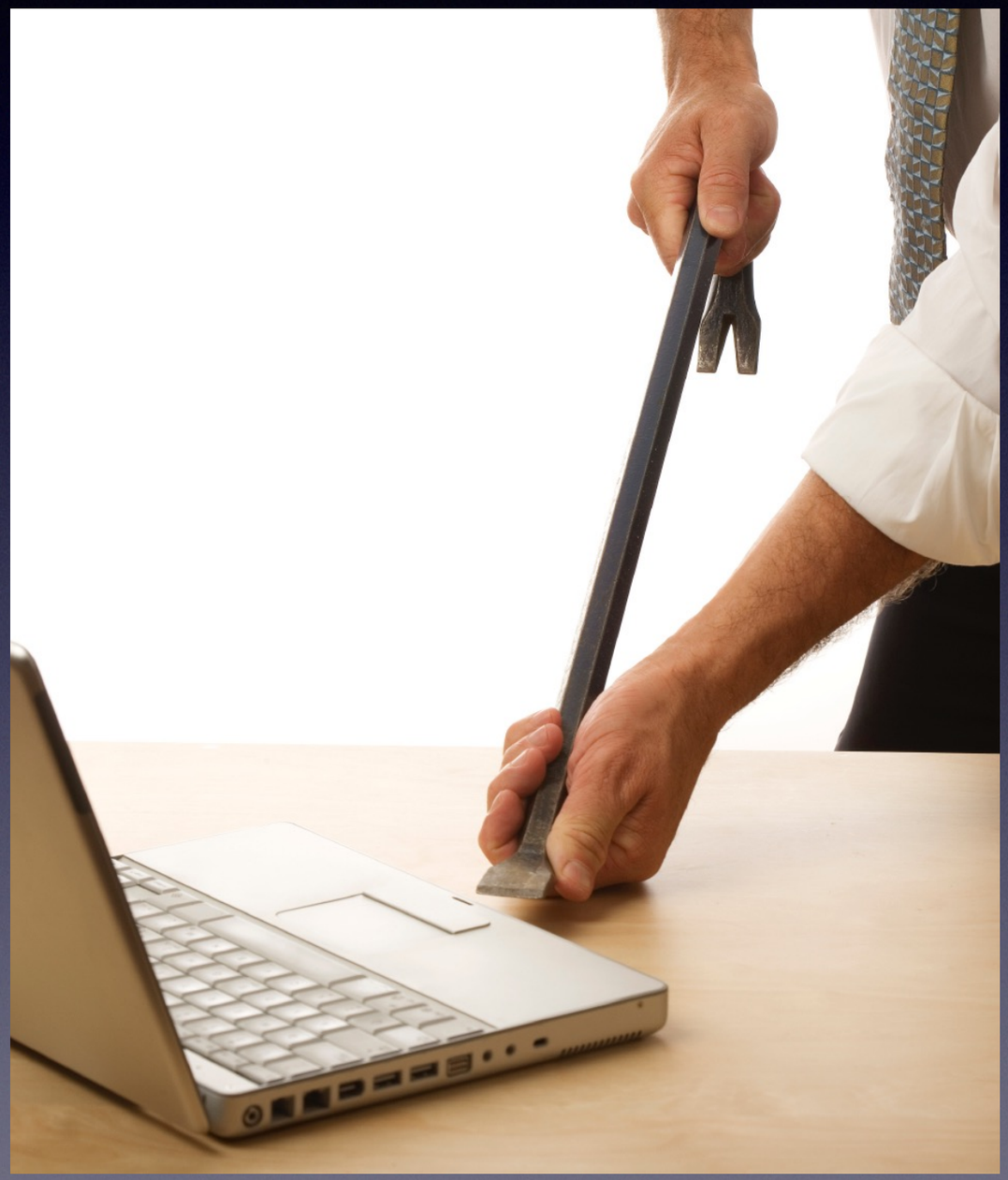
MICROSOLVED,INC.

Recent Campaigns & Research Issues

- Dragonfly makes old hotness new again
- Attack against Korea Hydro and Nuclear Power
- Defacement of gas station pump-monitoring systems
- Malware disguised as ICS/SCADA software
- Recent research on web vulnerabilities against embedded systems can cause physical damages

Threat Actors

- Nation-State affiliated groups
- Hacktivist organizations
- Organized crime



- Nothing new here, except that the underground markets for ICS data are maturing rapidly…
- The value chain is growing for ICS data theft, not just ICS access attacks

Threat Types & TTPs

- Threat types
  - Cyber espionage
  - Destructive attacks emerging
  - Damaging side effects from enumeration & scanning
- Commonly used TTPs
  - Spear phishing
  - Fake software updates/installers => RATs
  - Watering hole attacks
  - Malicious code embedded in common IT file formats shared with OT can be leveraged

BadUSB
Guess what? USB is bad for you! ;)

- USB controller chips' firmware can easily be reprogrammed
- Devices emulate keyboards and issue commands
- Infected USB drives can spoof network cards and change DNS settings
- Difficult for standard AV to detect infected USB device firmware
- **Be VERY careful about letting ANY digital media storage devices have physical access to ICS**
- **Look for this TTP style to be combined with issues like 'rowhammer' in the future**

But, Fix the Basics First!

- 50 shades of “grey out”
- Common wisdom of inventories vs actual deployment gaps
- Default configurations & authentication is everywhere
- Plain text protocols abound, making small access -> HUGE
- Many organizations pay little attention to relevant intellectual property & focus on control

More Information & Questions

- If you have questions, comments or feedback, please contact your account executive to schedule a discussion with one of our intelligence analysts

- Questions: info@microsolved.com
- More information: stateofsecurity.com & microsolved.com