INDUSTRIAL CYBERSECURITY: INNOVATION IN CYBERATTACK VERSUS INNOVATION IN PROTECTION

19th International Industrial Cybersecurity Experiences Congress – Madrid – 28.09.2022

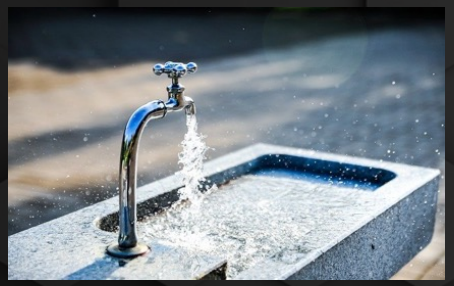
INTRODUCTION

- CEO, Owner, Ampere Industrial Security
- Former utility staff (telecommunications, water & electric)
- Drafter of NERC CIP standards and formal interpretations
- NERC CIP Supply Chain Working Group contributor
- First NERC CIP auditor
- Former Manager, CIP Audits and Investigations – WECC Region (NERC)
- Former Principal Investigator US DOE National Electric Sector Cybersecurity Organization
- EnergySec Founder, Former Director, Former Instructor and President Emeritus
- SANS ISC456 Instructor: Essentials for NERC Critical Infrastructure Protection
- US Coordinator, Centro de Ciberseguridad Industrial (CCI)
- Cybersecurity Advisory Team for State Solar, NARUC/NASEO
- National Telecommunications and Information Administration (NTIA) and Idaho National Lab (INL) Software Bill of Materials (SBOM) Energy POC Stakeholders
- DOE Solar Energy Technology Office (SETO) and National Renewable Energy Lab (NREL) Industry Advisory Board (IAB) for the Securing Solar for the Grid (S2G)
- Advisor to multiple industrial security hardware and software vendors
- GCIP, CISA, CRISC, CISSP-ISSAP, SSCP, NSA-IAM, CVI, TCP, SCP

OPERATIONAL TECHNOLOGY TODAY

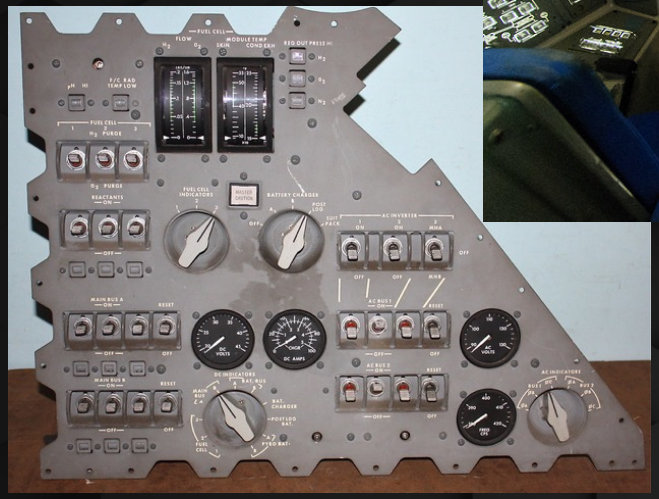








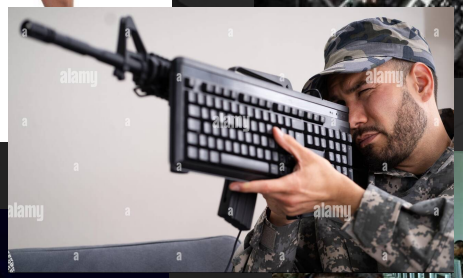

O.T. CHANGES OVER TIME



ATTACKERS OVER TIME







ICS ATTACK INNOVATION

Alert (AA22-083A) — More Alerts

Tactics, Techniques, and Procedures of Indicted State-Sponsored Russian Cyber Actors Targeting the Energy Sector

Original release date: March 24, 2022

Alert (AA20-049A)

Ransomware Impacting Pipeline Operations

Original release date: February 18, 2020 | Last revised: October 24, 2020

Alert (AA22-110A)

Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure

Original release date: April 20, 2022 | Last revised: May 09, 2022

Alert (AA21-201A)

Chinese Gas Pipeline Intrusion Campaign, 2011 to 2013

Original release date: July 20, 2021 | Last revised: July 21, 2021

Alert (AA21-287A)

Ongoing Cyber Threats to U.S. Water and Wastewater Systems

Original release date: October 14, 2021 | Last revised: October 25, 2021

Alert (TA17-163A)

CrashOverride Malware

Original release date: June 12, 2017 | Last revised: July 20, 2021

Alert (AA22-103A)

APT Cyber Tools Targeting ICS/SCADA Devices

Original release date: April 13, 2022 | Last revised: May 25, 2022

ICS Alert (IR-ALERT-H-16-056-01)

Cyber-Attack Against Ukrainian Critical Infrastructure

Original release date: February 25, 2016 | Last revised: July 20, 2021

ICS Joint Security Awareness Report (JSAR-12-241-01B)

Shamoon/DistTrack Malware (Update B)

Original release date: October 16, 2012 | Last revised: July 20, 2021

ICS Advisory (ICSA-14-178-01)

ICS Focused Malware

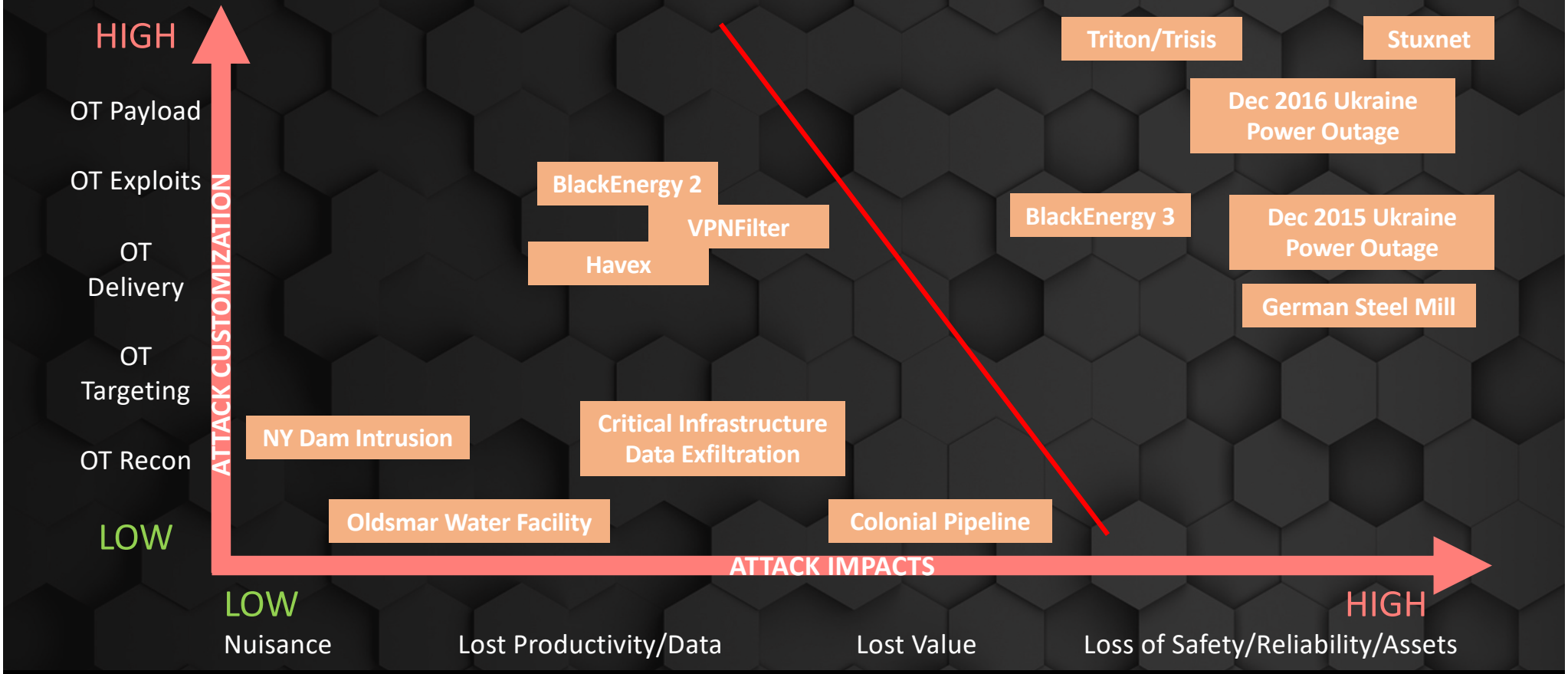
Original release date: June 30, 2014 | Last revised: July 20, 2021

ICS Alert (ICS-ALERT-14-281-01E)

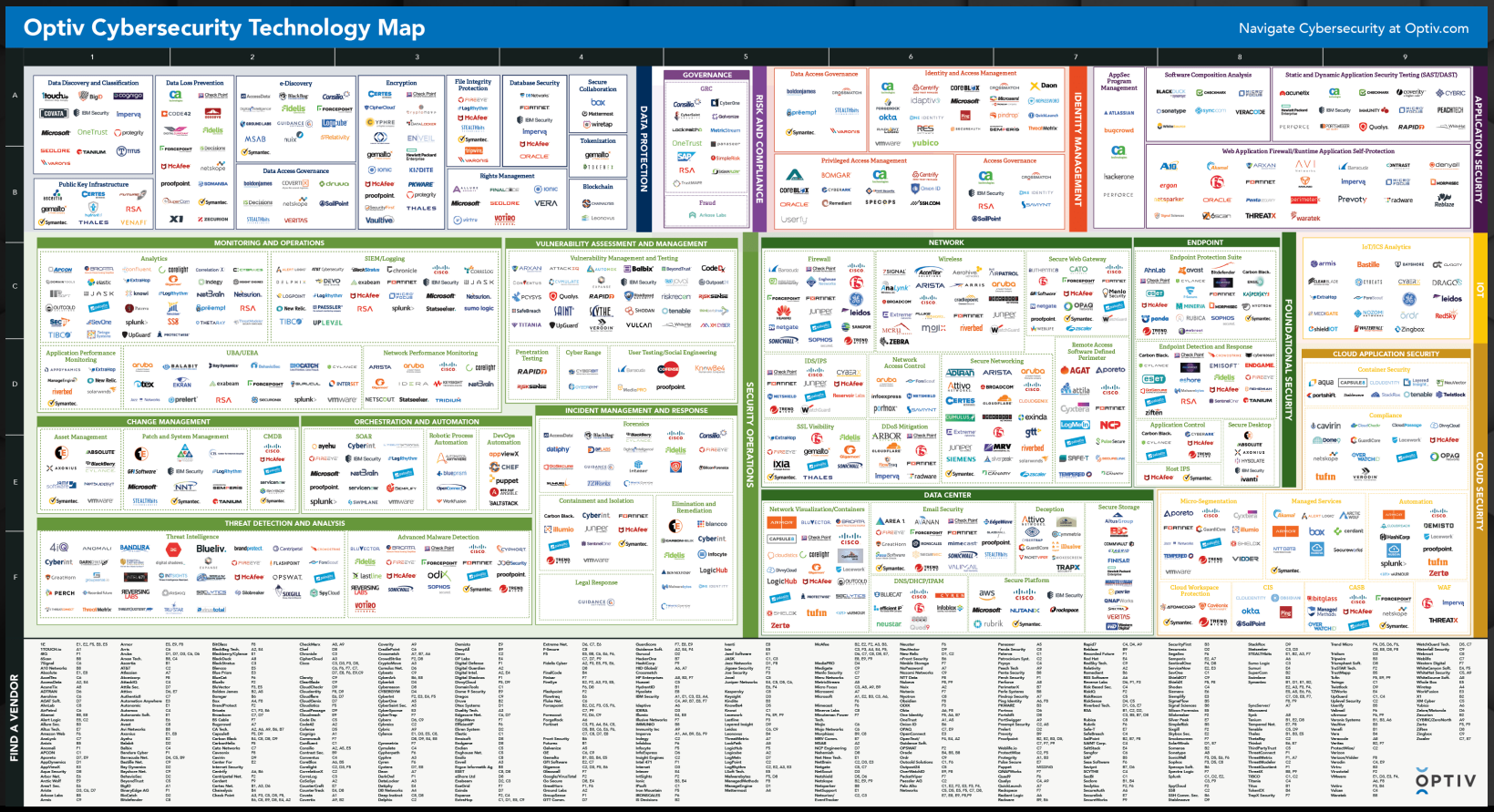
Ongoing Sophisticated Malware Campaign Compromising ICS (Update E)

Original release date: December 10, 2014 | Last revised: July 22, 2021

OT INCIDENTS AND CAMPAIGNS



MORE BLINKING LIGHTS



INNOVATION OR DISRUPTION?

INNOVATION IS A RACE

- Hackers are faster than laws, regulation, standards, norms
- You can not possibly know every zero day in advance
- You can not possibly know every new adversary tactic in advance
- If you bought/implemented every security tool available, would you be secure?
- If you were compliant to every regulation and standard, would you be secure?
- You can not stop humans from innovating…

…but you can use that to your advantage.

INNOVATION ENGINE

CONTACT ME


@PATRICKCMILLER


LINKEDIN.COM/IN/MILLERPATRICKC


PMILLER@AMPERESEC.COM


WWW.AMPERESEC.COM


+15032721414

All images sourced through Creative Commons and Pixabay