WEBCAST SERIES

Cyber Threats to the Electric Industry

HOSTED BY

Katie Nickels

GUEST SPEAKERS

Tim Conway & Robert M. Lee

Welcome to the SANS Threat Analysis Rundown

Our goal is to bring you the **inside scoop** on what you need to know about cyber threats. We'll bring you **different voices** from around the community to ensure you're **up-to-date** on what's happening in the threat landscape so you can take action.

Today's Agenda

- Rundown – (January Was Long)
- Deep-Dive – ("The" Electric System)
- Wrap-Up – (Defense is Doable)


SANS THREAT ANALYSIS RUNDOWN
Rundown

Rundown: February 12, 2020

- Recovering from a rough January
- A new indictment: Equifax
- Ransomware everywhere
- Staying vigilant on Iran

Deep-Dive

Cyber Threats to the Electric Industry

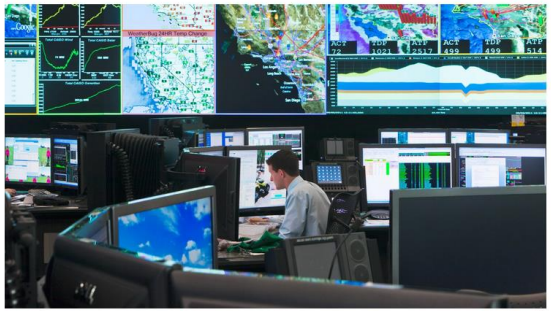
Tim Conway & Robert M. Lee

The Electric Grid is Under Attack!

In the worst-case scenario, Iranian hackers "could instantaneously shut down an entire power grid," Martini said. "It's not just the lights, it's also the internet which shuts down communication systems. Without shooting a single bullet or missile, you can shut down an entire county or nation." USA Today

Security News This Week: An Unprecedented Cyberattack Hit US Power Utilities

Exposed Facebook phone numbers, an XKCD breach, and more of the week's top security news.



PHOTOGRAPH: ULLSTEIN BILD/GETTY IMAGES

WIRED

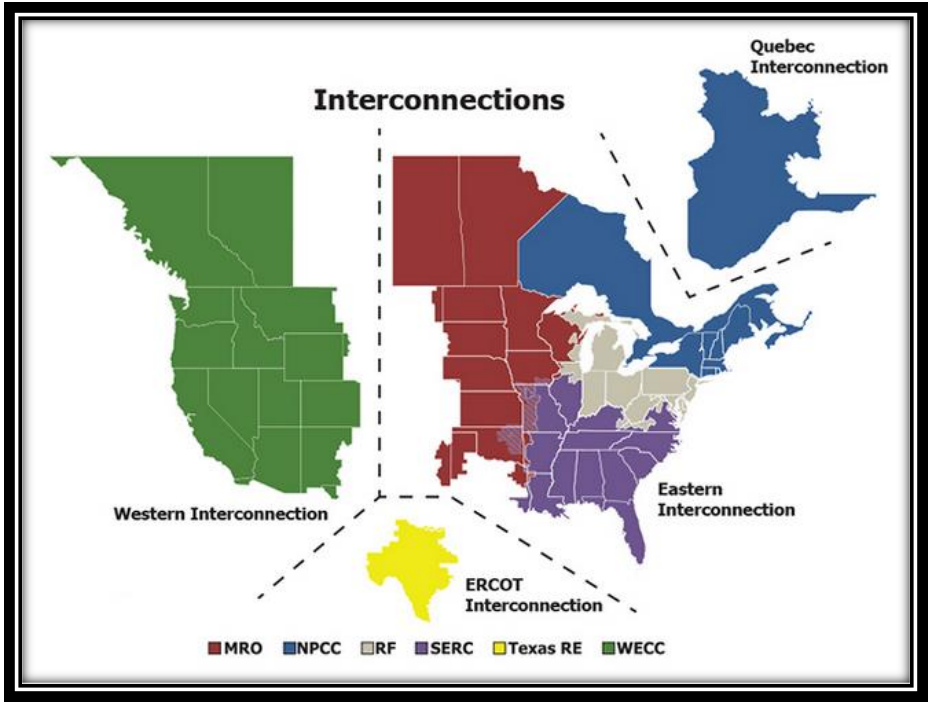
U.S. Government Makes Surprise Move To Secure Power Grid From Cyberattacks

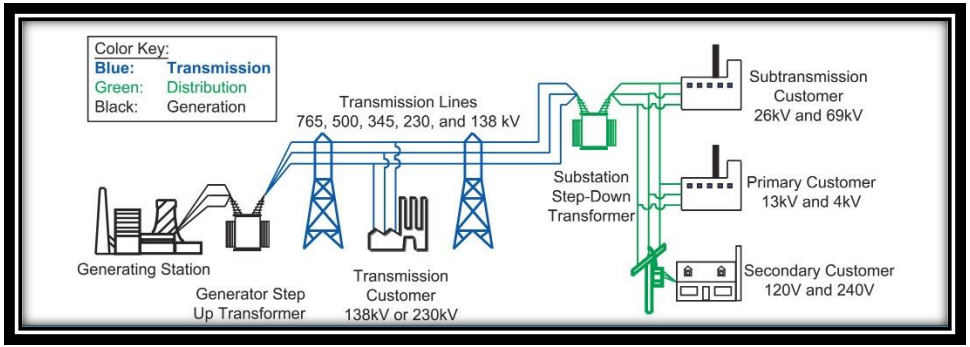
Kate O'Flaherty Senior Contributor
Cybersecurity
I'm a cybersecurity journalist.

Power lines in St. Charles Parish, Louisiana. Homeland Security officials say that Russian hackers... [+]
ASSOCIATED PRESS

Forbes

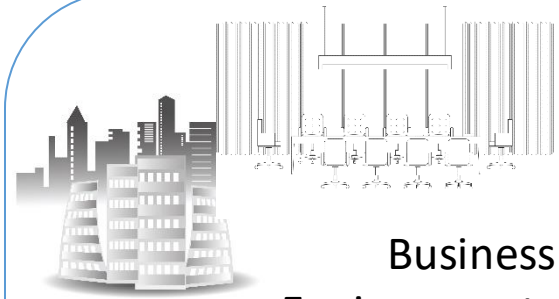
Nuance Matters



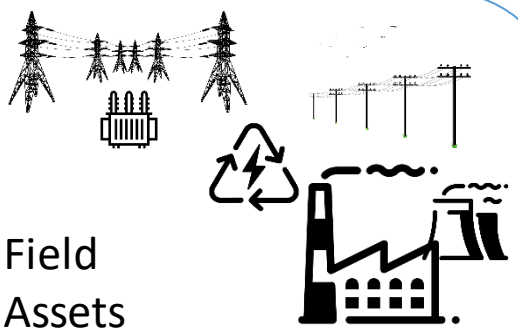


- Over 1,500 Registered Entities comprise the North American BES
- With thousands more distribution utilities

Context Specific Actionable Threat Intelligence



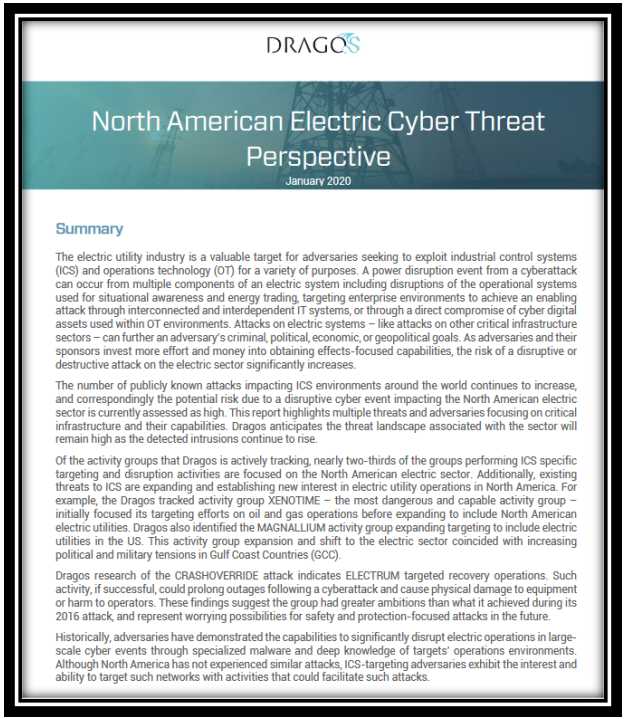
Business Environments



Field Assets

IT

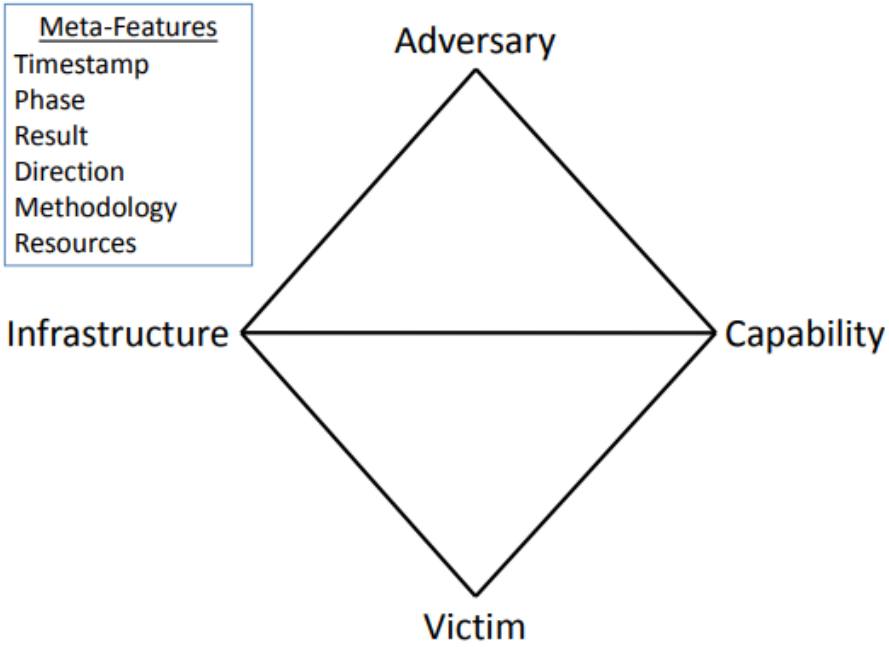
OT



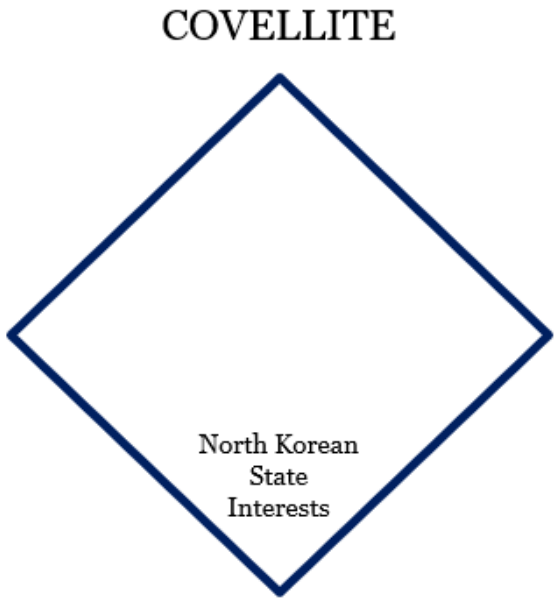
Know Thy Threats

- Activity Groups are clusters of intrusions to meet a requirement you have
- Intrusions are the individual events at organizations

- The Diamond Model (right) is used to express events
- Specific 2+ correlations equate an activity group



Covellite



- Legitimate infrastructure compromised by the adversary
- Specific university IPs for C2

- Sophisticated implant with secure communication channels
- Similar features to malware used against South Korean targets
- Specific session key used for payload and second encrypted layer
- 41 minute and 30 second sleep

- Electric utility companies in the United States

Collection Management Framework

	CONTROL CENTER	CONTROL CENTER	CONTROL CENTER	TRANSMISSION SUBSTATION	TRANSMISSION SUBSTATION
ASSET TYPE	Windows Human Machine Interface	Data Historian	Network Monitoring Appliance	Windows Human Machine Interface	Remote Terminal Units
DATA TYPE	Windows Event Logs	Alarms	Alerts	Windows Event Logs	Syslog
QUESTION TYPE (KILL CHAIN PHASES)	Exploration, Installation, Actions on Objectives	Actions on Objectives	Internal Reconnaissance, Command and Control, Delivery, Actions on Objectives	Exploitation, Installation, Actions on Objectives	Installation, Actions on Objectives
FOLLOW-ON COLLECTION	Registry Keys	Set Points and Tags	Packet Capture	Registry Keys	Controller Logic
DATA STORAGE LOCATION	Enterprise SIEM	Local	Enterprise SIEM	Local	Local
DATA STORAGE TIME	60 Days	120 Days	30 Days	30 Days	7 Days

Current CIP Standards

Version 6	Standard Name
CIP-002-5.1*	BES Cyber System Categorization
CIP-003-6	Security Management Controls
CIP-004-6	Personnel & Training
CIP-005-5*	Electronic Security Perimeter(s)
CIP-006-6	Physical Security of BES Cyber Systems
CIP-007-6	System Security Management
CIP-008-5*	Incident Reporting and Response Planning
CIP-009-6	Recovery Plans for BES Cyber Systems
CIP-010-2	Configuration Change Management and Vulnerability Assessments
CIP-011-2	Information Protection
CIP-014-2	Physical Security

Function Type of asset

- Generation resource, transmission substation, transmission line, control center, control room, blackstart asset

Risk Impact Rating Criteria

- Identified as High, Medium, Low, or non-BES

Cyber Programmable electronic devices

- Determine if there are cyber digital elements involved in operating the asset that could be used to impact the assets function

Accessibility Communications paths to the cyber devices

- Routable communications, serial communications, wireless, uni-directional communications, communications external to the electronic perimeter

Operationalize the Threat Intel

PARISITE

Leverages known VPN Vulnerabilities

XENOTIME

Demonstrated SIS manipulation

DYMALLOY

Long term persistence in IT and OT

Operationalize the Threat Intel

ELECTRUM

Demonstrated DPR manipulation

CHRYSENE

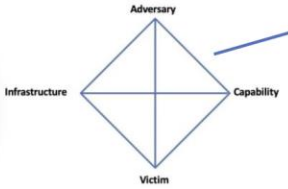
Demonstrated IT manipulation and OT targeting

ICS ATT&CK

MITRE | ATT&CK™ FOR ICS

- A key milestone in ICS cybersecurity
- A globally-accessible knowledge base of adversary tactics and techniques based on intelligence-driven insights

ICS ATT&CK and Activity Groups



Initial Access	Execution	Persistence	Evasion	Discovery	Lateral Movement	Collection	Command and Control	Inhibit Response Function	Impair Process Control	Impact
Data Historian Compromise	Change Program State	Hooking	Exploitation for Evasion	Control Device Identification	Default Credentials	Automated Collection	Commonly Used Port	Activate Firmware Update Mode	Brute Force I/O	Damage to Property
Drive-by Compromise	Command-Line Interface	Module Firmware	Indicator Removal on Host	I/O Module Discovery	Exploitation of Remote Services	Data from Information Repositories	Connection Proxy	Alarm Suppression	Change Program State	Denial of Control
Engineering Workstation Compromise	Execution through API	Program Download	Masquerading	Network Connection Enumeration	External Remote Services	Detect Operating Mode	Standard Application Layer Protocol	Block Command Message	Masquerading	Denial of View
Exploit Public-Facing Application	Graphical User Interface	Project File Infection	Rogue Master Device	Network Service Scanning	Program Organization Units	Detect Program State		Block Reporting Message	Modify Control Logic	Loss of Availability
External Remote Services	Man in the Middle	System Firmware	Rootkit	Network Sniffing	Remote File Copy	I/O Image		Block Serial COM	Modify Parameter	Loss of Control
Internet Accessible Device	Program Organization Units	Valid Accounts	Spoof Reporting Message	Remote System Discovery	Valid Accounts	Location Identification		Data Destruction	Module Firmware	Loss of Productivity and Revenue
Replication Through Removable Media	Project File Infection		Utilize/Change Operating Mode	Serial Connection Enumeration		Monitor Process State		Denial of Service	Program Download	Loss of Safety
Spearphishing Attachment	Scripting					Point & Tag Identification		Device Restart/Shutdown	Rogue Master Device	Loss of View
Supply Chain Compromise	User Execution					Program Upload		Manipulate I/O Image	Service Stop	Manipulation of Control
Wireless Compromise						Role Identification		Modify Alarm Settings	Spoof Reporting Message	Manipulation of View
						Screen Capture		Modify Control Logic	Unauthorized Command Message	Theft of Operational Information
								Program Download		
								Rootkit		
								System Firmware		
								Utilize/Change Operating Mode		

dex.php/Technique/T843


SANS THREAT ANALYSIS RUNDOWN
Wrap-Up

Takeaways and Action Items

- Be the voice of reason when you hear FUD
- Take a look at activity groups:

  https://www.activeresponse.org/wp-content/uploads/2013/07/diamond.pdf

  https://dragos.com/adversaries/

- Check out ATT&CK™ for ICS: https://attack.mitre.org/ics

References

- The Equifax indictment: https://www.justice.gov/opa/pr/chinese-military-personnel-charged-computer-fraud-economic-espionage-and-wire-fraud-hacking
- Ransomware
  - Snake/EKANS: https://twitter.com/VK_Intel/status/1214333066245812224
    https://dragos.com/blog/industry-news/ekans-ransomware-and-ics-operations/
    https://nakedsecurity.sophos.com/2020/01/13/snake-alert-this-ransomware-is-not-a-game/
  - RobbinHood: https://news.sophos.com/en-us/2020/02/06/living-off-another-land-ransomware-borrows-vulnerable-driver-to-remove-security-software/
  - MailTo: https://www.carbonblack.com/2020/02/07/threat-analysis-unit-tau-threat-intelligence-notification-mailto-netwalker-ransomware/

References

- Possible Iranian activity
  - https://www.fireeye.com/blog/threat-research/2020/02/information-operations-fabricated-personas-to-promote-iranian-interests.html
  - https://blog.certfa.com/posts/fake-interview-the-new-activity-of-charming-kitten/
  - https://www.reuters.com/article/us-iran-hackers-exclusive/exclusive-iran-linked-hackers-pose-as-journalists-in-email-scam-idUSKBN1ZZ1MS
  - https://www.recordedfuture.com/pupyrat-malware-analysis/
  - https://intezer.com/blog-new-iranian-campaign-tailored-to-us-companies-uses-updated-toolset/

References

- Resources to get started
  - https://dragos.com/adversaries
  - https://dragos.com/year-in-review/
  - https://dragos.com/resource/collection-management-frameworks-beyond-asset-inventories-for-preparing-for-and-responding-to-cyber-threats/
  - https://www.robertmlee.org/a-collection-of-resources-for-getting-started-in-icsscada-cybersecurity/
  - SANS ICS410, ICS456, ICS515, ICS612 – Do it!


SANS THREAT ANALYSIS RUNDOWN
Thank you for coming!
For the recording and slides, please visit
https://www.sans.org/webcasts/113035