Global Electric Cyber Threat Perspective

Pasquale Stirparo, Principal Adversary Hunter
Jason Christopher, Principal Cyber Risk Advisor
Dragos, Inc.

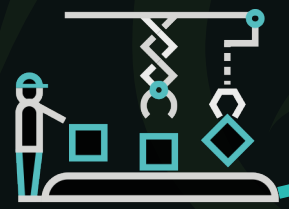
October 2021

Overview

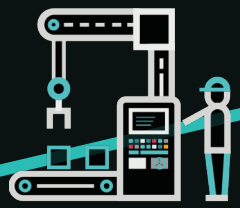
- Trends
- Biden Administration 100-Day Electric Plan
- Activity Groups
- Operational Segments Threat Perspective
- Threat Landscape
  - Ransomware
  - Supply Chain
  - Internet Exposed Asset
- Recommendations

INDUSTRY TRENDS

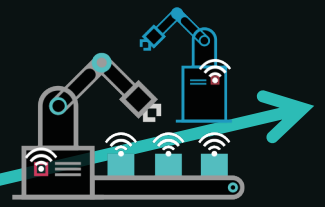
Growing investment in digital transformation and hyperconnectivity



STAND-ALONE



LOOSELY CONNECTED



HIGHLY CONNECTED

Greater exposure to malicious cyberthreats

“Threat groups are rising 3X faster than they’re declining…”

Source: Dragos 2020 YiR

Biden Administration 100-Day Electric Plan

The Directive

- Owners and operators to modernize cybersecurity defenses
- Improve visibility, detection, and response

Results

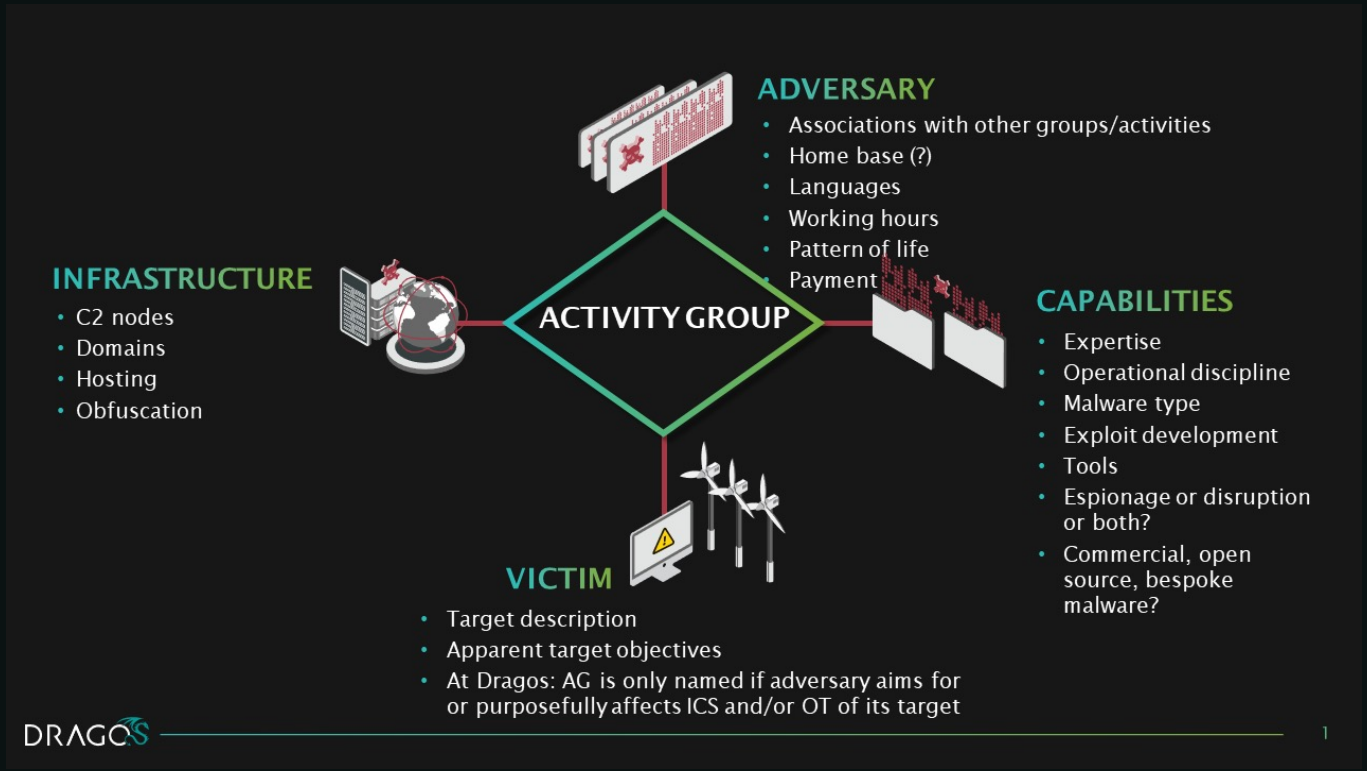
- As of August 16th, at least 150 electric utilities -- serving almost 90 million American electric customers -- have adopted or committed to adopting technologies

Public-Private Partnership

Activity Groups

What is an Activity Group (AG?)

At Dragos, an AG is *different* than just another name for an adversary



Known Activity Groups Targeting Electric

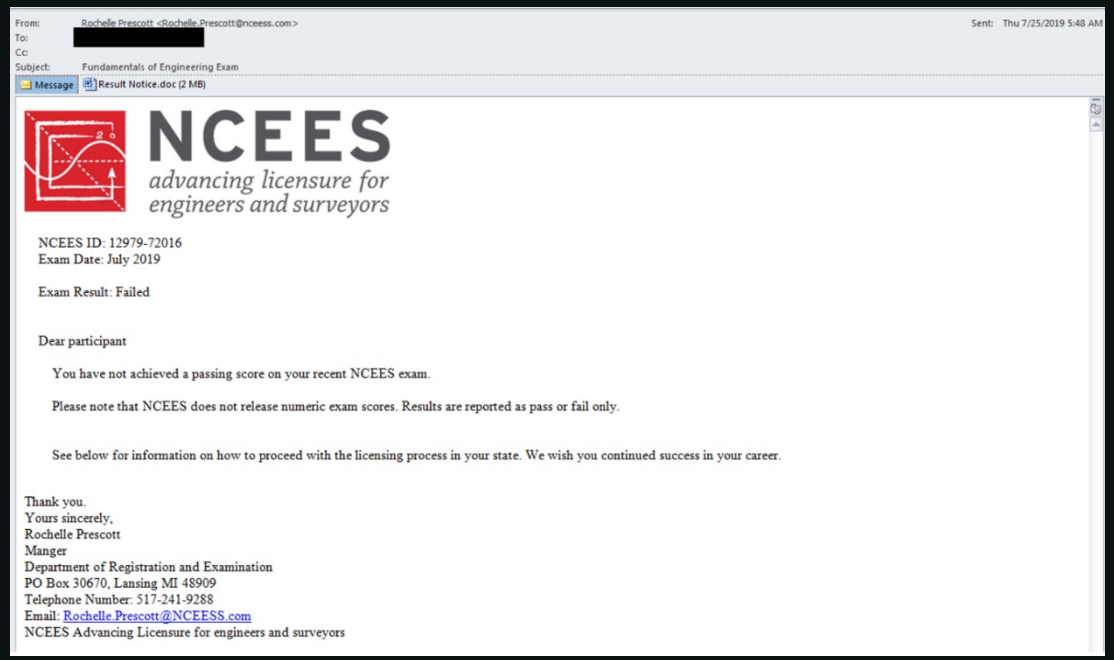
11 groups targeting Electric:

- ALLANITE
- CHRYSENE
- DYMALLOY
- ELECTRUM
- KAMACITE*
- MAGNALIUM
- PARISITE
- STIBNITE*
- TALONITE*
- WASSONITE
- XENOTIME

*New in 2020

Introducing TALONITE

- Dragos first learned of phishing campaigns in 2019
  - Impacted 17 organizations
  - Masqueraded as legitimate engineering, licensing and certification, and NERC
- New activity discovered in Q1 2021 focusing on US electric utilities likely for initial access and information gathering


From: Rochelle Prescott <Rochelle.Prescott@nceess.com> Sent: Thu 7/25/2019 5:48 AM
To: [redacted]
Cc:
Subject: Fundamentals of Engineering Exam
Message Result Notice.doc (2 MB)

NCEES
advancing licensure for engineers and surveyors

NCEES ID: 12979-72016
Exam Date: July 2019

Exam Result: Failed

Dear participant

You have not achieved a passing score on your recent NCEES exam.

Please note that NCEES does not release numeric exam scores. Results are reported as pass or fail only.

See below for information on how to proceed with the licensing process in your state. We wish you continued success in your career.

Thank you.
Yours sincerely,
Rochelle Prescott
Manger
Department of Registration and Examination
PO Box 30670, Lansing MI 48909
Telephone Number: 517-241-9288
Email: Rochelle.Prescott@NCEESS.com
NCEES Advancing Licensure for engineers and surveyors

Sample phishing email

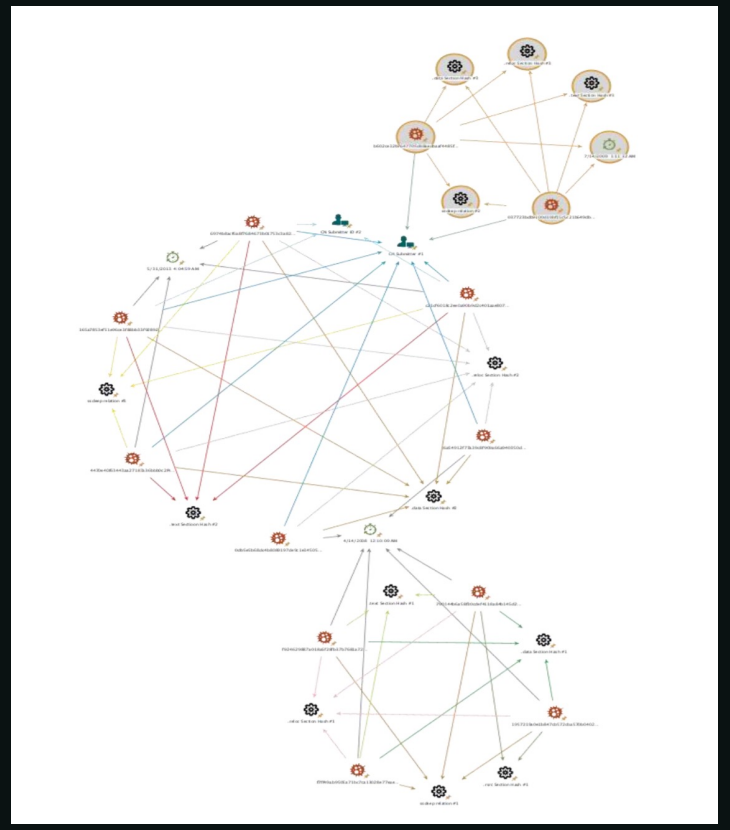
Introducing STIBNITE

- STIBNITE has been targeting wind turbine system companies in Azerbaijan since late 2019
- In 2021 targeting extended, remaining focused on Azerbaijan
  - State Oil Company of the Azerbaijan Republic (SOCAR) was used as a spearphishing lure to target the Azerbaijan Republic Ministry of Ecology and Natural Resources
  - Leveraged a new version of PoetRAT

Introducing KAMACITE

- Dragos assesses KAMACITE to be an Activity Group associated with developing access for other groups like ELECTRUM that then follow on with ICS-focused attacks

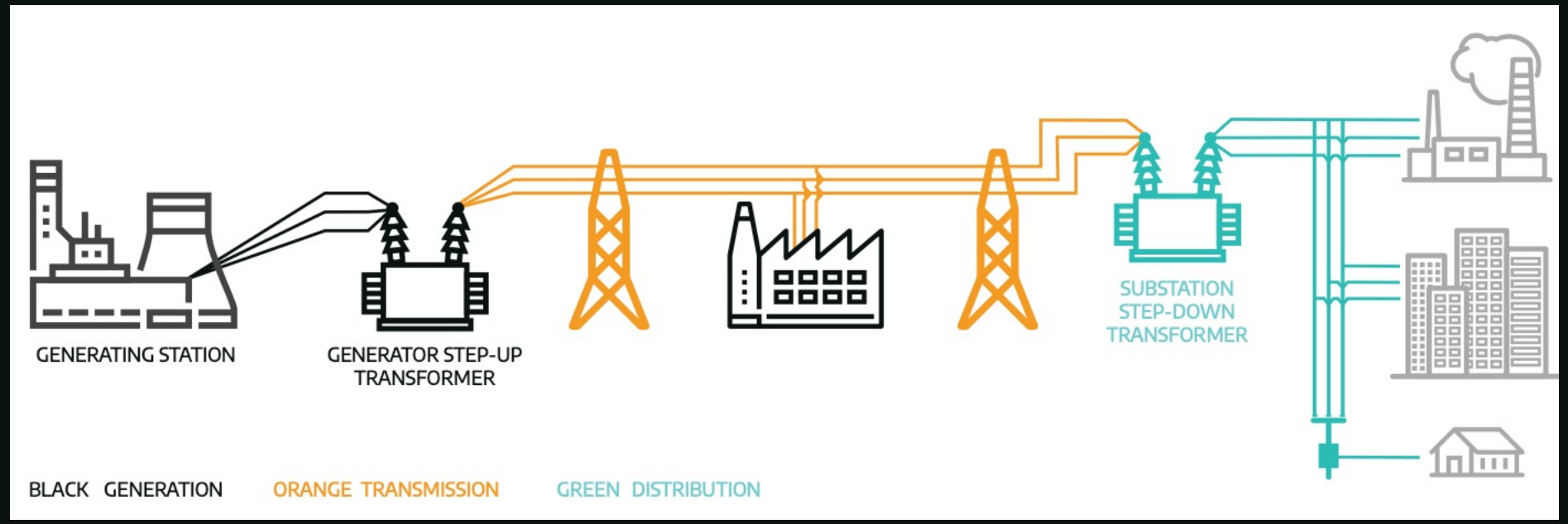
- In August 2021, Dragos identified and analyzed a sample of GREYENERGY, a modular malware seen as the successor to BLACKENERGY3.



Visual Representation of GREYENERGY file-based attribute clustering

Operational Segments Threat Perspective

Operational Segments



Generation

Threat Landscape and Assessment

At least five AGs have demonstrated intent or capabilities to infiltrate or disrupt Electric Power Generation

- XENOTIME
- DYMALLOY
- ALLANITE
- WASSONITE
- STIBNITE

ICS-targeting adversaries have not successfully disrupted electric power generation. The observed activities targeting this segment, including obtaining documentation on sensitive operations networks, could be used for espionage purposes or to facilitate a disruptive attack.

Transmission

Threat Landscape and Assessment

At least two AGs are a threat to transmission operations.

- ELECTRUM
- KAMACITE

CRASHOVERRIDE took place in Europe. Targeted breaker operations controlled by ABB devices adhering to the IEC 61850 standard and communicating using the Manufacturing Message Specification (MMS) protocol.

However, Dragos assesses with moderate confidence the attack can be leveraged to other equipment that adheres to these standards.

Distribution

Threat Landscape and Assessment

Only one attacks has disrupted electric distribution operations:

- First widespread outage caused by a cyberattack (Ukraine 2015), enabled by KAMACITE.
- Contrary to ELECTRUM, the adversary did not use ICS-specific malware. It controlled operations remotely via existing tools in the operations environment.

The behaviors and tools use exhibited could be deployed in distribution operations globally, depending on the adversary sponsor's focus.

However, disrupting electric power requires fundamental understanding of the enterprise and operational environments.

Ransomware

Ransomware

- Significant rise in the number of ransomware events affecting Utilities and Vendors.
  - Between 2018 and 2020, 10% of ransomware attacks that occurred on industrial and related entities targeted electric utilities[1]
- Most malware strains are IT-focused. But even if not affecting the OT network directly, those attacks have caused operations to halt.
  - Dragos identified multiple ransomware strains adopting ICS-aware functionality, including the ability to kill industrial focused computer processes, such as EKANS, MEGACORTEX, and CL0P.
- Almost all ransomware operators are increasingly incorporating data theft techniques into their campaigns to further ransom demands.

[1] https://www.dragos.com/resource/ransomware-in-ics-environments/

Ransomware Incidents in Electric

Dragos responded to several ransomware incidents in 2021

- Case Study: U.S. Power Company
  - Adversary stayed undetected for over a month before completing the operation
  - The ransomware attack itself took less than 1hour, halted company's operations

Supply Chain

The ICS OEM Nexus

- OEMs often have remote access to critical parts of customer networks
  - This means that hackers who breached an OEM could potentially use their credentials to control critical customer processes

- Compromising an OEM magnifies the potential risks to infrastructure
  - Infections in the critical infrastructure sector occurred on IT networks as well as on industrial control system networks that manage critical functions

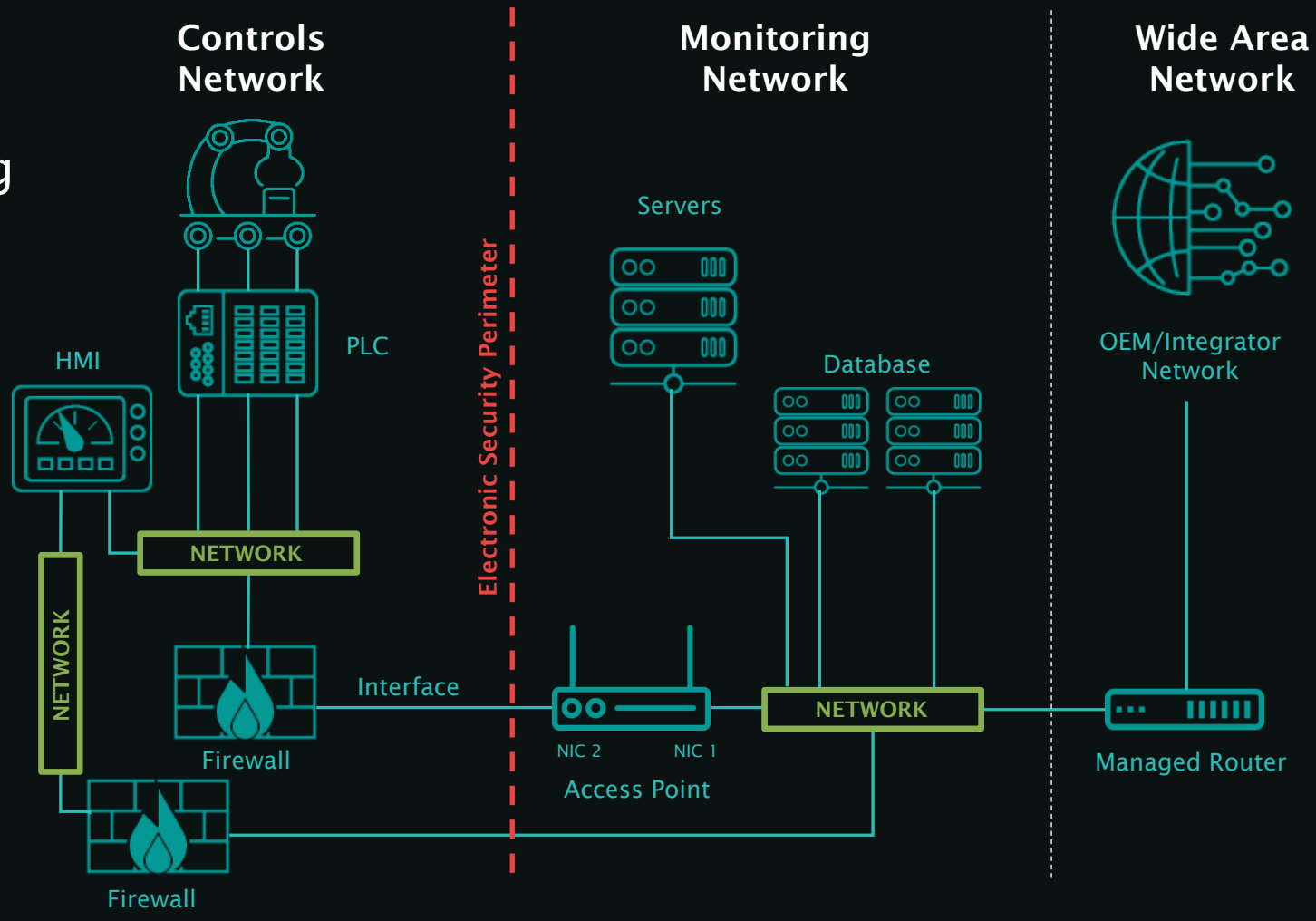
OT Exposure via Remote Access

Use cases:

- Monitoring and troubleshooting
- Patch distribution
- Staff augmentation

Examples:

- SolarWinds
- Numerous OEM compromises direct into DCS/SCADA networks of industrial companies



South Asian OT and ICS Provider Targeted

- In April 2021, Dragos discovered activity associated with an adversary targeting a South Asian based OT and ICS hardware manufacturer and service provider with direct access to customer networks
- The OEM has customers across the electric sector; OEM was notified, and response was inadequate
- Adversary re-established (or never left) access to same target triad in June-August 2021

Internet Exposed Assets

Internet Exposed Assets

Threat Landscape and Assessment

At least four AGs have demonstrated intent or capabilities to infiltrate or disrupt Electric Utilities, either in previous or active targeting

- PARISITE
- MAGNALLIUM
- ALLANITE
- XENOTIME

Adversary are quick to weaponize and exploit vulnerabilities in internet-facing services including Remote Desktop Protocol (RDP) and Virtual Private Network (VPN) services. Vulnerabilities discovered in the summer of 2020 impacted critical network infrastructure services including F5, Palo Alto Networks, Fortinet, Citrix and Juniper will likely be exploited by ICS-targeting adversaries, if they have not already.

Recommendations

Summary Recommendations

ACCESS RESTRICTIONS and ACCOUNT MANAGEMENT

Restrict administrative access within a domain, limit the number of domain administrators, and separate networking, server, workstation, and database administrators into separate Organizational Units (OUs)

RESPONSE PLANS

Develop, review, and practice cyberattack response plans and integrate cyber investigations into root-cause analysis for all events specific to OT

SEGMENTATION

Where possible, segment and isolate networks to limit lateral movement

THIRD-PARTIES

Ensure that third-party connections and OT interactions are monitored and logged, from a “trust, but verify” mindset

VISIBILITY

Take a comprehensive approach for visibility and threat detection into OT environments to ensure that there is no gap in monitoring

Thank You.
Any Questions?