**NCCIC** | NATIONAL CYBERSECURITY & COMMUNICATIONS INTEGRATION CENTER

# DEFENDING CRITICAL INFRASTRUCTURE: LESSONS LEARNED FROM THE FIELD

**Jonathan Homer**
Chief, Industrial Control Systems Team
Hunt and Incident Response Team (HIRT)

Homeland Security

## Overview

The NCCIC's mission is to reduce the likelihood and severity of incidents that may significantly compromise the security and resilience of the nation's critical infrastructure and communications networks.

NCCIC executes this mission by serving as a national hub for cyber and communications information, technical expertise, and operational integration, and by operating a 24x7 situational awareness, analysis, and incident response center.

"The cybersecurity functions of the [NCCIC] shall include… being a Federal civilian interface for the multi-directional and cross-sector sharing of information related to cybersecurity risks, incidents, analysis, and warnings… providing shared situational awareness… providing timely incident response capabilities to Federal and non-Federal entities…"

- NATIONAL CYBERSECURITY PROTECTION ACT OF 2014



## Core Functions

NCCIC performs a suite of functions that provide customers with comprehensive risk management capabilities, products, and services. These functions include:

- Information sharing
- Data synthesis and analysis
- Operational planning, training, and exercises
- Watch floor operations
- Risk and vulnerability assessments
- Hunt, incident response, and recovery

UNCLASSIFIED

## Hunt and Incident Response Team (HIRT)

**The NCCIC HIRT provides expert intrusion analysis and mitigation guidance to clients who lack in-house capability or require additional assistance with responding to a cyber incident**

- Federal agencies
- State and local governments
- Private sector (industry & critical infrastructure)
- Academia
- International organizations

**Uniquely Positioned for Comprehensive Analysis**

- Classified & unclassified TTPs
- Public & private sector partners
- Established relationship with law enforcement, intelligence community, and international partners

UNCLASSIFIED 4

UNCLASSIFIED

## APT Campaign Targeting Energy Sector

- Historically, cyber threat actors have targeted the energy sector with various results ranging from cyber espionage to the ability to disrupt energy systems in the event of a hostile conflict.
- Since at least May 2017, threat actors have targeted the energy sector and other entities, leveraging their capabilities to compromise victims' networks.
- This activity is assessed as a multi-stage intrusion campaign by threat actors.
- Targets low security and small networks to gain access and move laterally to networks of high-value asset owners within the energy sector.

UNCLASSIFIED 5

UNCLASSIFIED

## APT Campaign Targeting Energy Sector

- This campaign compromises two distinct categories of victims: staging and intended targets
- Initial victims (referred to as "staging targets") are peripheral organizations such as trusted third-party suppliers with less secure networks.
- The threat actor uses the staging target's network as a pivot point and malware repository when targeting their final intended target, with the ultimate objective of compromising the intended target's network.

UNCLASSIFIED 6

UNCLASSIFIED

## APT Campaign Targeting Energy Sector TTPs

The threat actors in this campaign employed a variety of TTPs, including:

- open-source reconnaissance,
- spear-phishing emails (from compromised legitimate accounts),
- watering-hole domains,
- host-based exploitation,
- industrial control system (ICS) infrastructure targeting, and
- ongoing credential gathering.



UNCLASSIFIED

## CrashOverride

- Highly capable Industrial Control Systems (ICS) attack platform in 2016. This attack targeted critical electric infrastructure in Ukraine.
- The platform fundamentally abuses the functionality of a targeted ICS system's legitimate control systems.
- General TTPs used in CrashOverride could be leveraged with modified technical implementations to affect U.S.-based critical infrastructure.



## Questions

CONTACT NCCIC:
NCCICCustomerService@hq.dhs.gov
888-282-0870
+1 703-235-5110


NCCIC