TLP:WHITE

NCCIC | NATIONAL CYBERSECURITY & COMMUNICATIONS INTEGRATION CENTER

AWARENESS BRIEFING:

RUSSIAN ACTIVITY AGAINST CRITICAL INFRASTRUCTURE

7/25/18

NCCIC

Audio Information:
Dial-In: 888-221-6227

DISCLAIMER

This report is provided “as is” for informational purposes only. The Department of Homeland Security (DHS) does not provide any warranties of any kind regarding any information contained within. The DHS does not endorse any commercial product or service, referenced in this bulletin or otherwise. This document is marked TLP:WHITE. Subject to standard copyright rules. TLP:WHITE information may be distributed without restriction. Sources may use TLP:WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release.

For more information on the Traffic Light Protocol,
see ***https://www.us-cert.gov/tlp***.

Welcome

AGENDA

Welcome

NCCIC Overview

Panel Presentations

NCCIC Resources

Q&A

Closing

TLP:WHITE

Housekeeping

Questions can be submitted in the chat box throughout the webinar and during the Q&A.

Please complete the short survey following the webinar.
We appreciate your feedback.

TLP:WHITE

NCCIC | NATIONAL CYBERSECURITY & COMMUNICATIONS INTEGRATION CENTER

NCCIC OVERVIEW

NCCIC

NCCIC Overview

Vision and Mission

Secure and robust cyber and communications infrastructure, resilient against attacks and disruption

Reduce the risk of systemic cybersecurity and communications challenges in our role as the Nation’s flagship of cyber defense, incident response and operational integration center

Mission Essential Functions (MEFs)

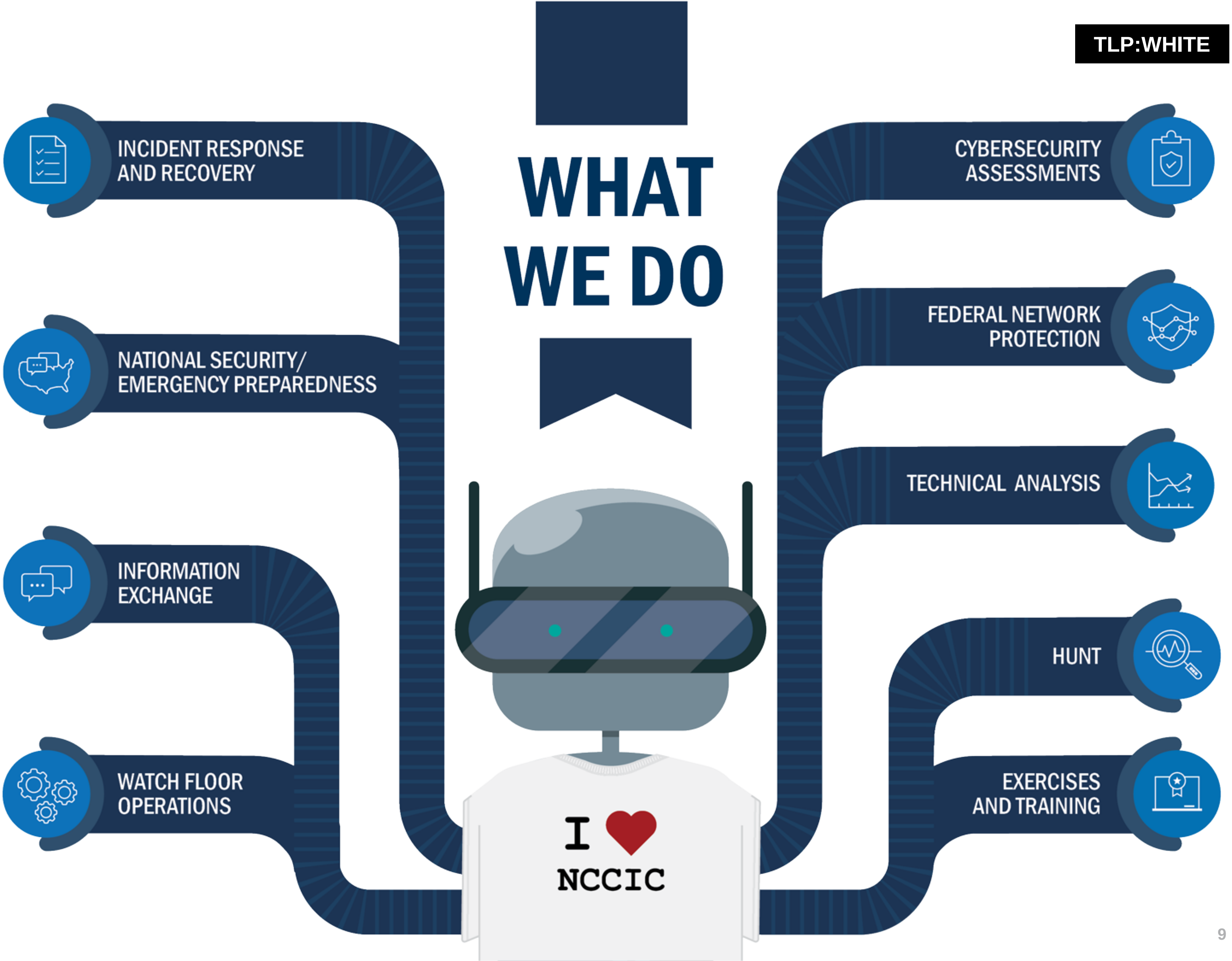
Incident Management: Manage cyber and communications incidents in real time to mitigate impacts and reduce risks to critical systems

Analysis: Conduct analyses to recognize threats and vulnerabilities, identify countermeasures, and develop situational awareness

Capacity Building: Build capacity across all levels of government and the private sector to improve management of cyber and communications risks

Information Sharing: Share information about cyber and communications risks to support stakeholder decisions and actions

WHAT WE DO



- INCIDENT RESPONSE AND RECOVERY
- NATIONAL SECURITY/ EMERGENCY PREPAREDNESS
- INFORMATION EXCHANGE
- WATCH FLOOR OPERATIONS
- CYBERSECURITY ASSESSMENTS
- FEDERAL NETWORK PROTECTION
- TECHNICAL ANALYSIS
- HUNT
- EXERCISES AND TRAINING

NCCIC | NATIONAL CYBERSECURITY &
COMMUNICATIONS INTEGRATION CENTER

HIRT | HUNT &
INCIDENT RESPONSE TEAM

RUSSIAN ACTIVITY AGAINST CRITICAL INFRASTRUCTURE

NCCIC

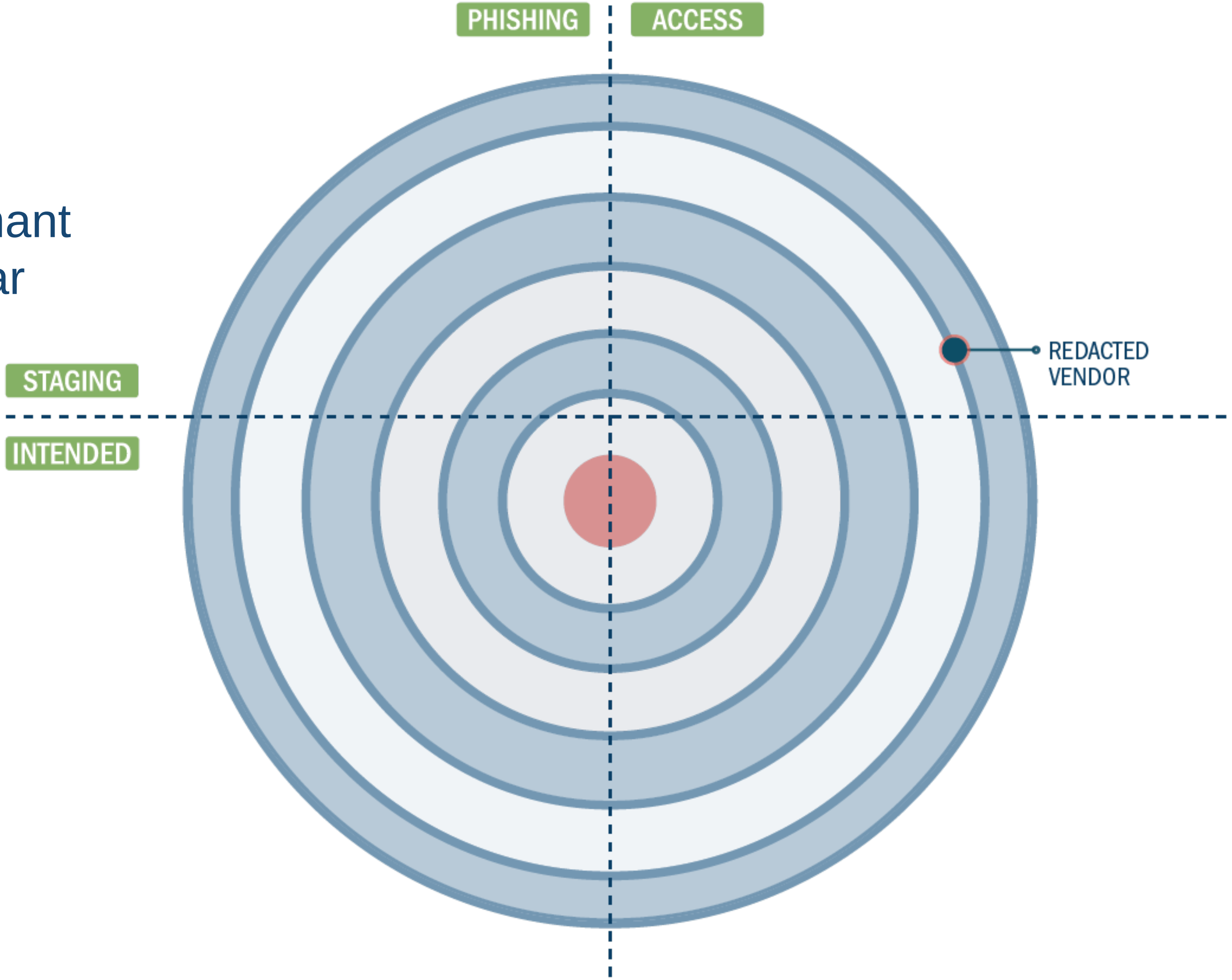
Campaign Summary

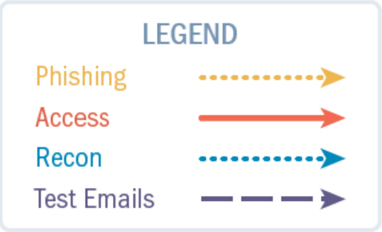
- **Advanced Persistent Threat** (APT) actors
- **Hundreds of victims** (targeted or affected)
  - Energy (focus area)
  - Nuclear
  - Aviation
  - Critical manufacturing
  - Government entities
- **Response effort** coordinated between multiple government organizations as well as industry organizations
- **Effect has been limited to access** so far, with no physical impact identified

TLP:WHITE

Campaign Timeline

- Vendor compromised in early 2016
- Remained dormant for over one year

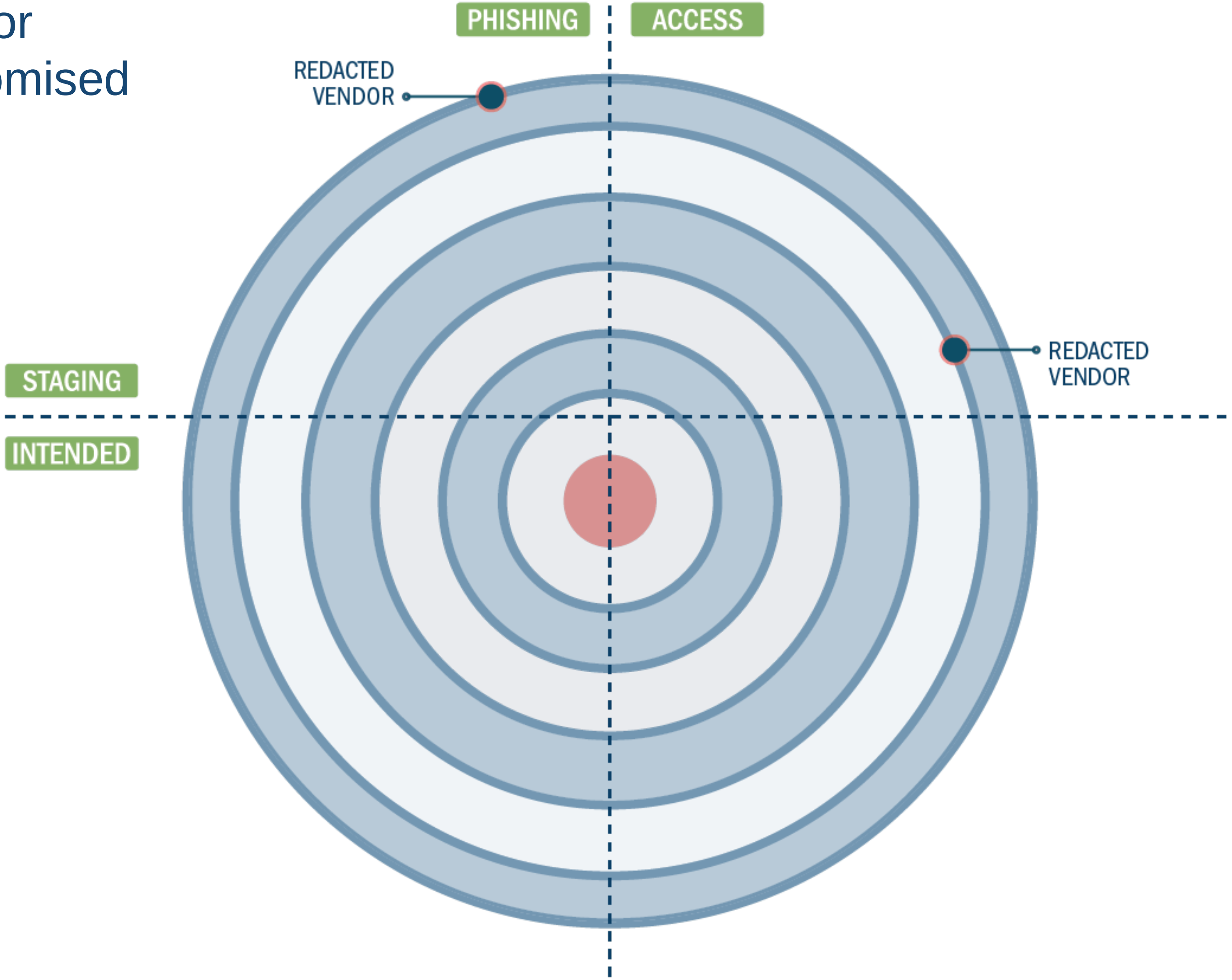


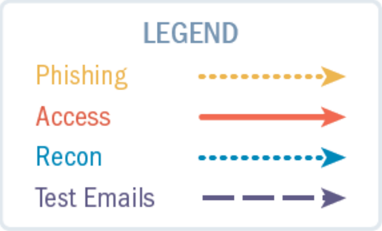


TLP:WHITE

Campaign Timeline

- Additional vendor network compromised in early 2017

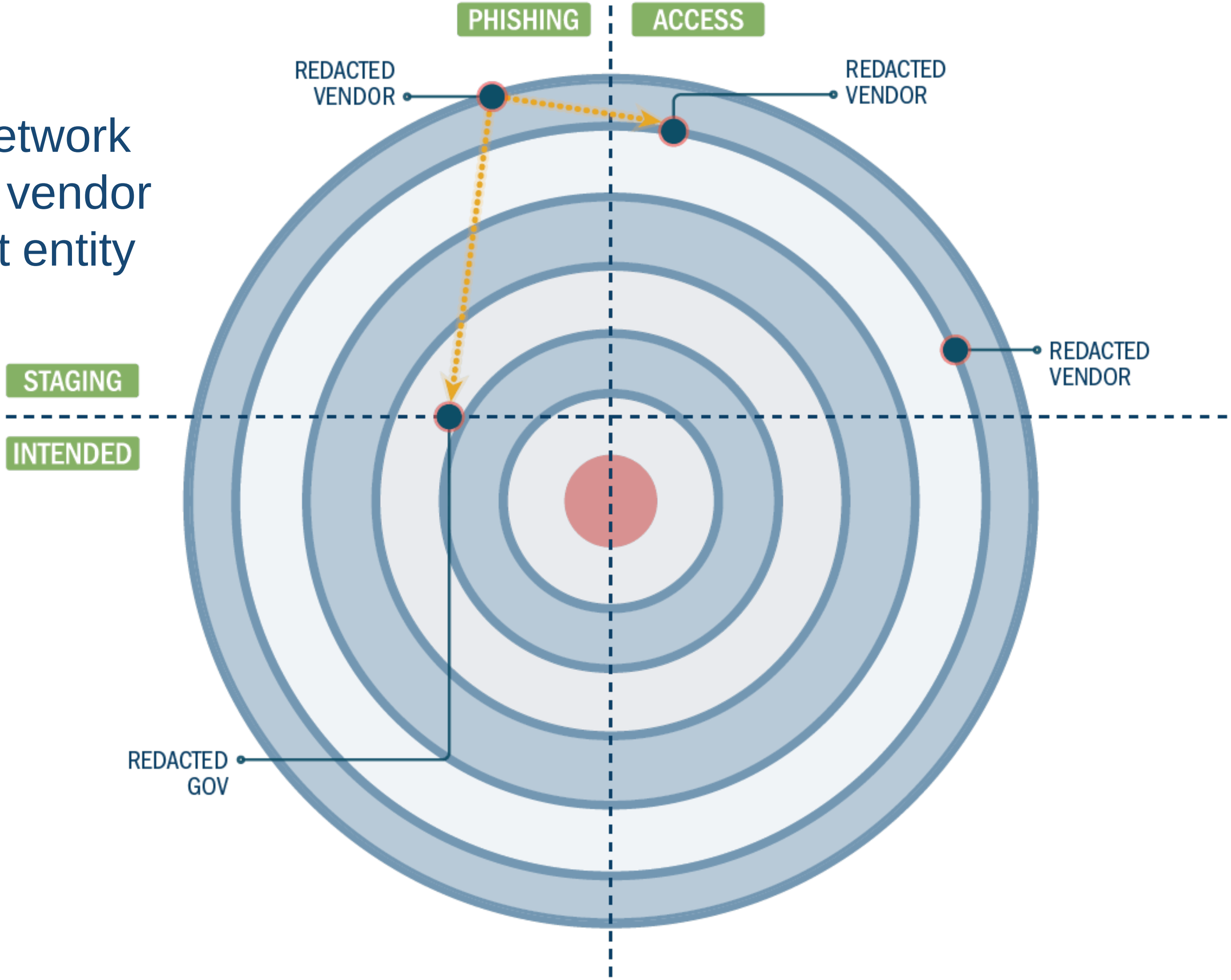




TLP:WHITE

Campaign Timeline

- Phishing attack originating from compromised network against another vendor and government entity



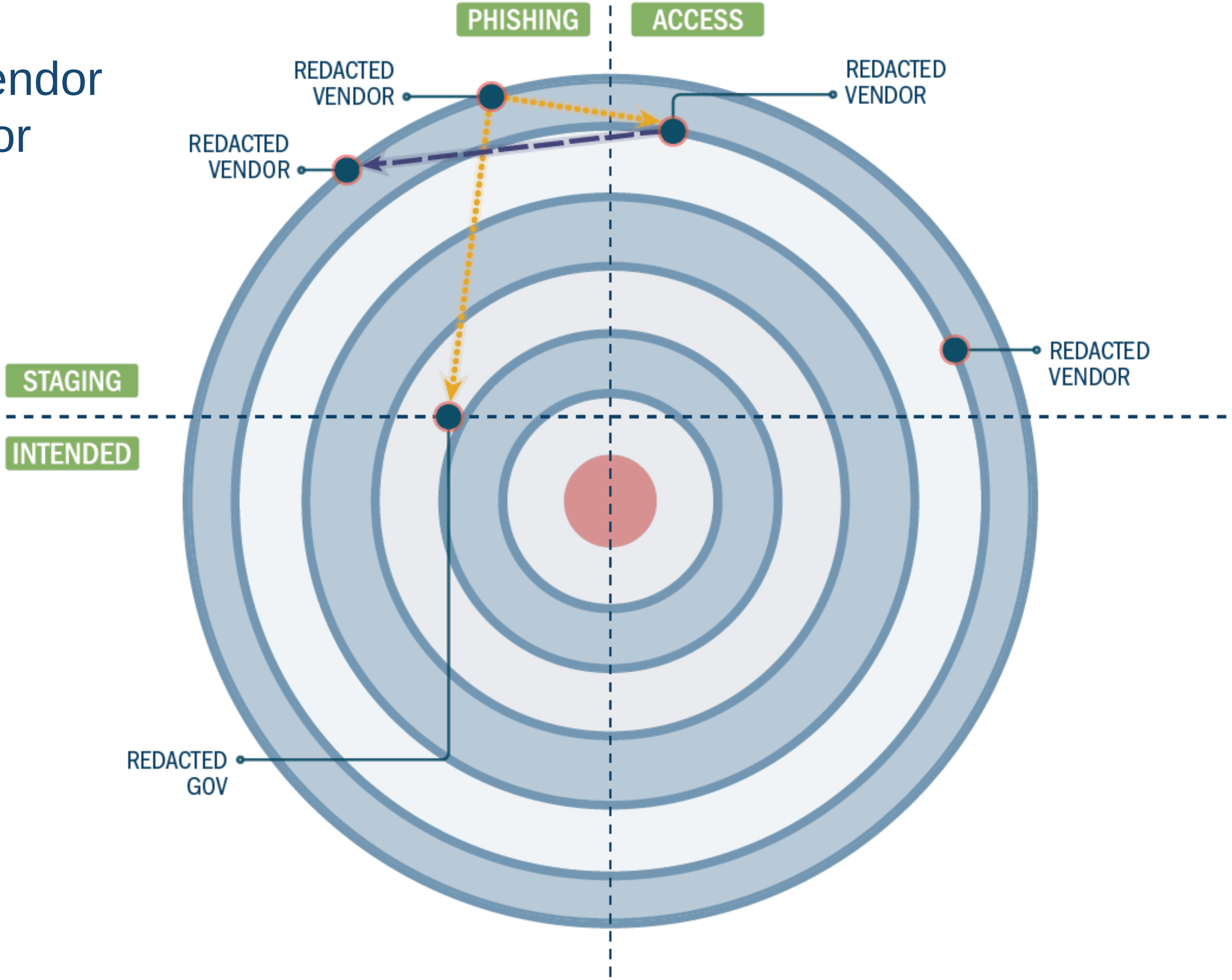
LEGEND

Phishing	••••••••••➤
Access	──────➤
Recon	••••••••••➤
Test Emails	─ ─ ─➤

TLP:WHITE

Campaign Timeline

- Intrusion from compromised vendor to another vendor



LEGEND

Phishing ·········➤

Access ━━━━➤

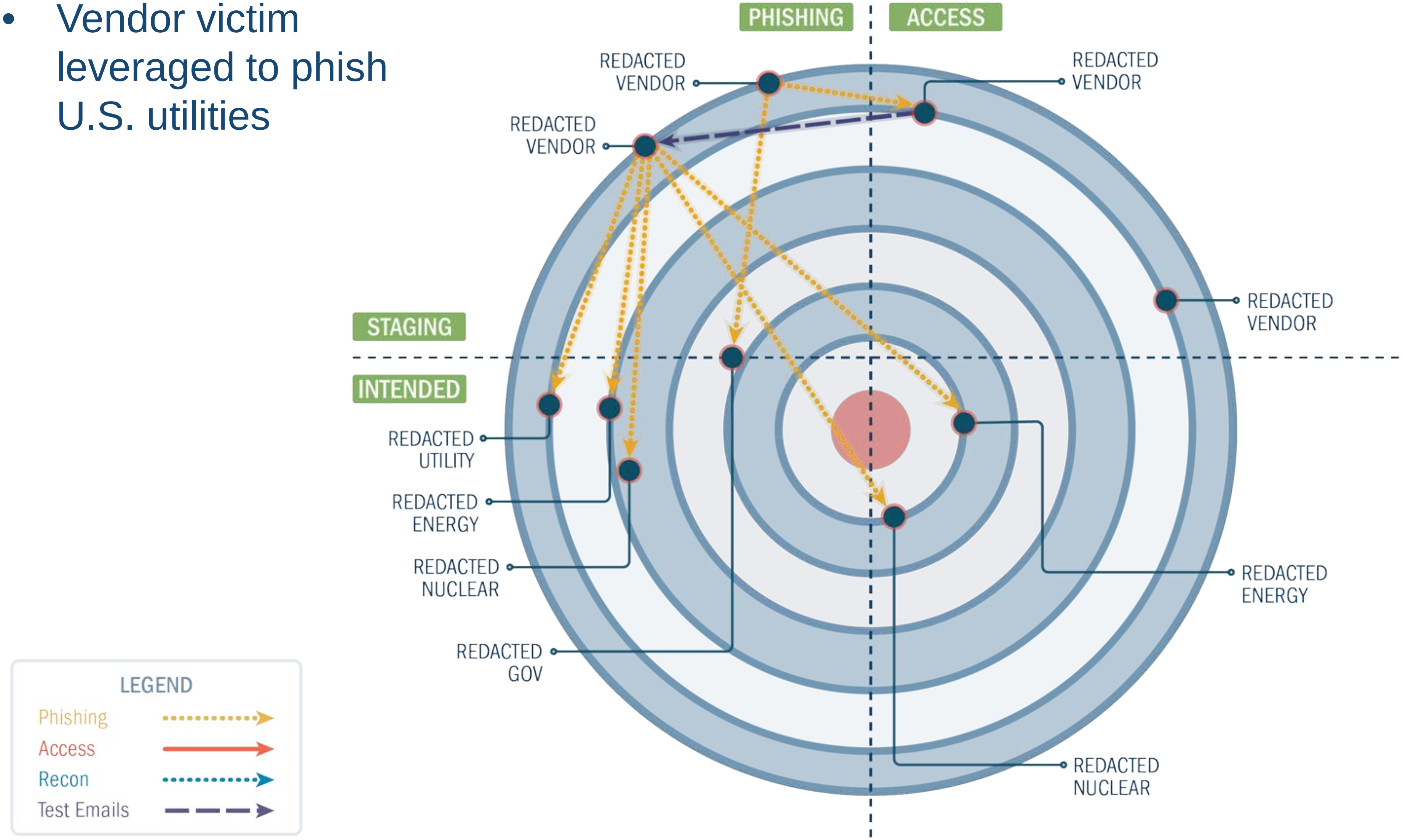
Recon ·········➤

Test Emails — — —➤

TLP:WHITE

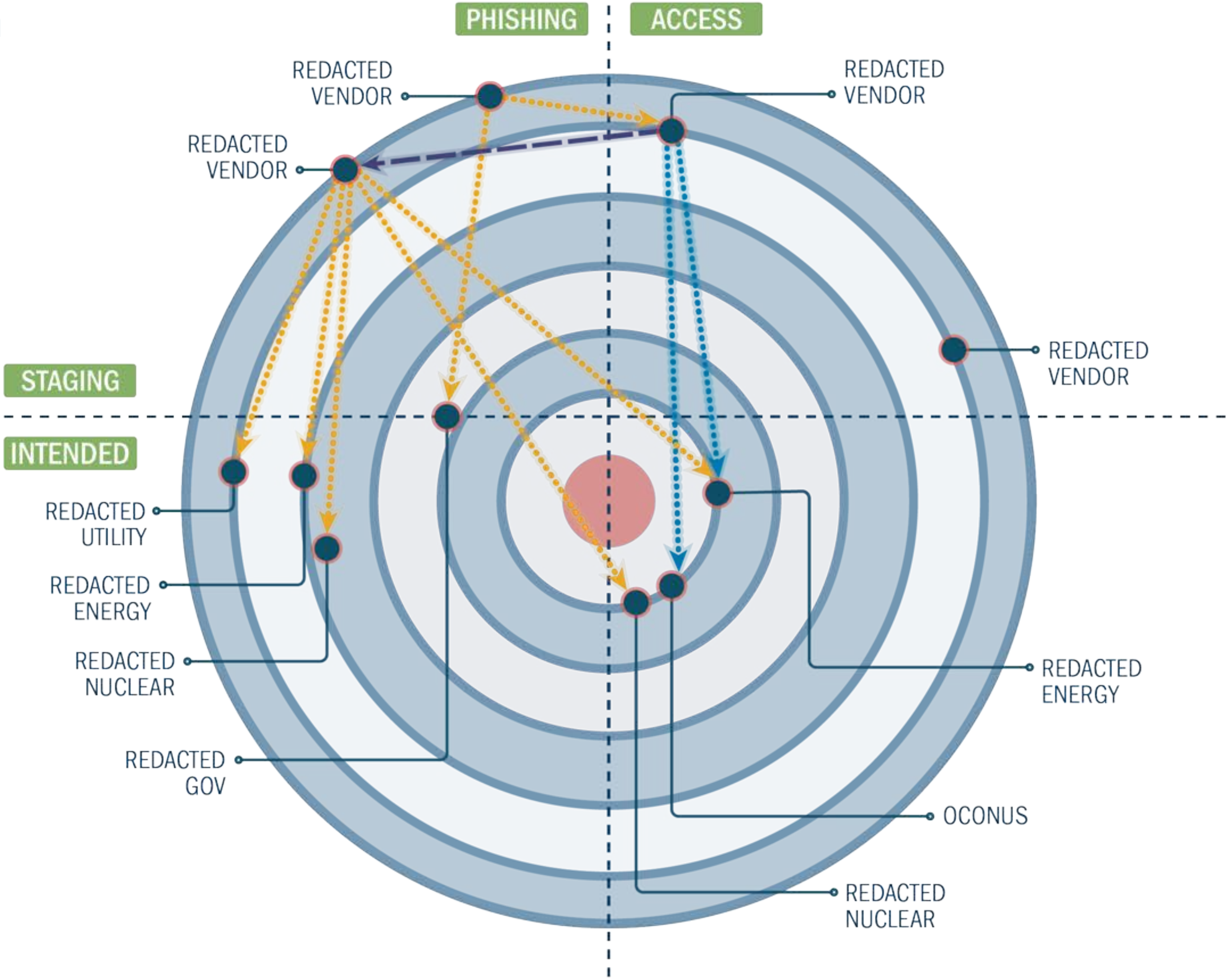
Campaign Timeline

- Vendor victim leveraged to phish U.S. utilities



Campaign Timeline

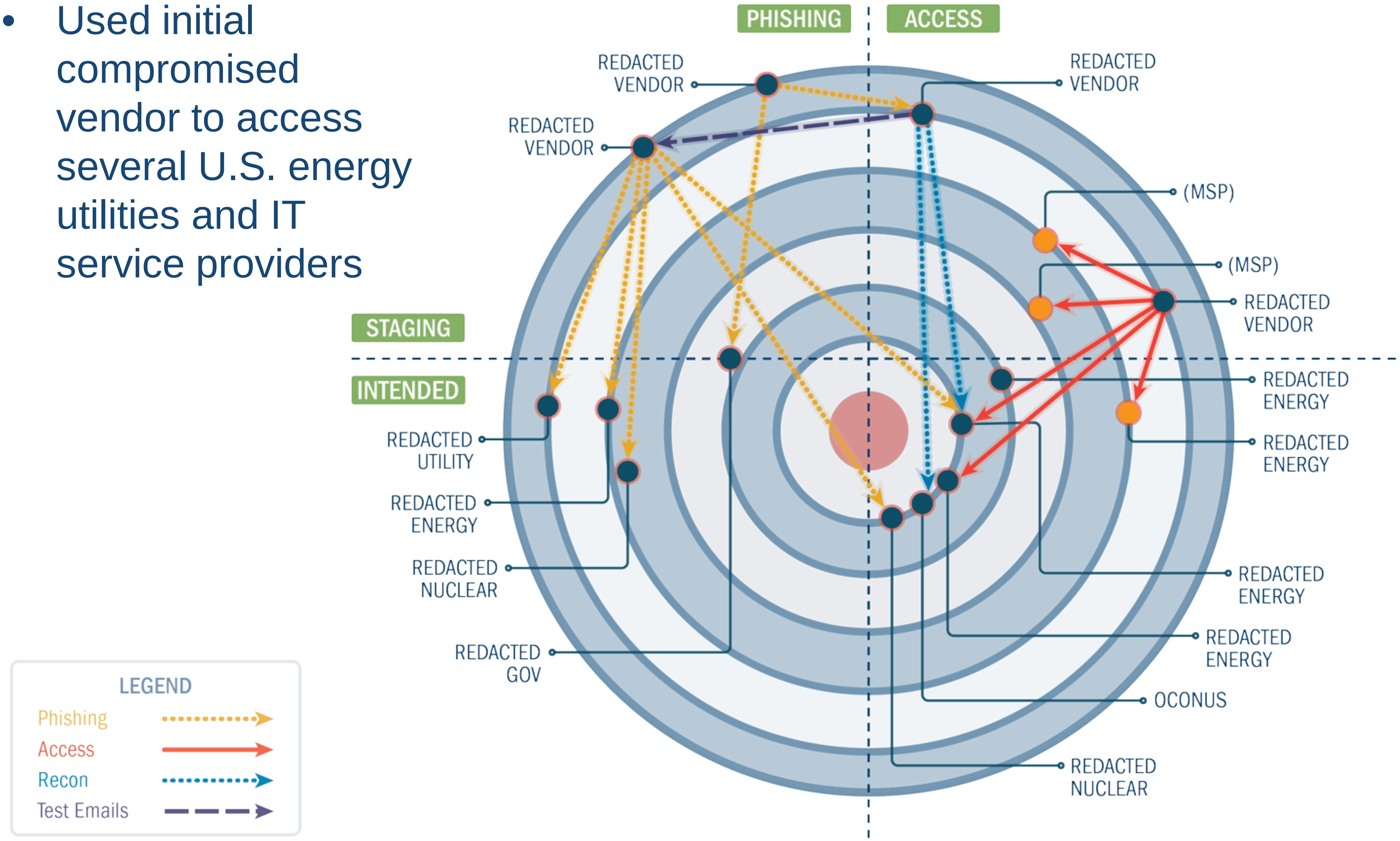
- Used new victim network to pivot and browse external content of an already-phished organization, as well as a non-U.S. organization



TLP:WHITE

Campaign Timeline

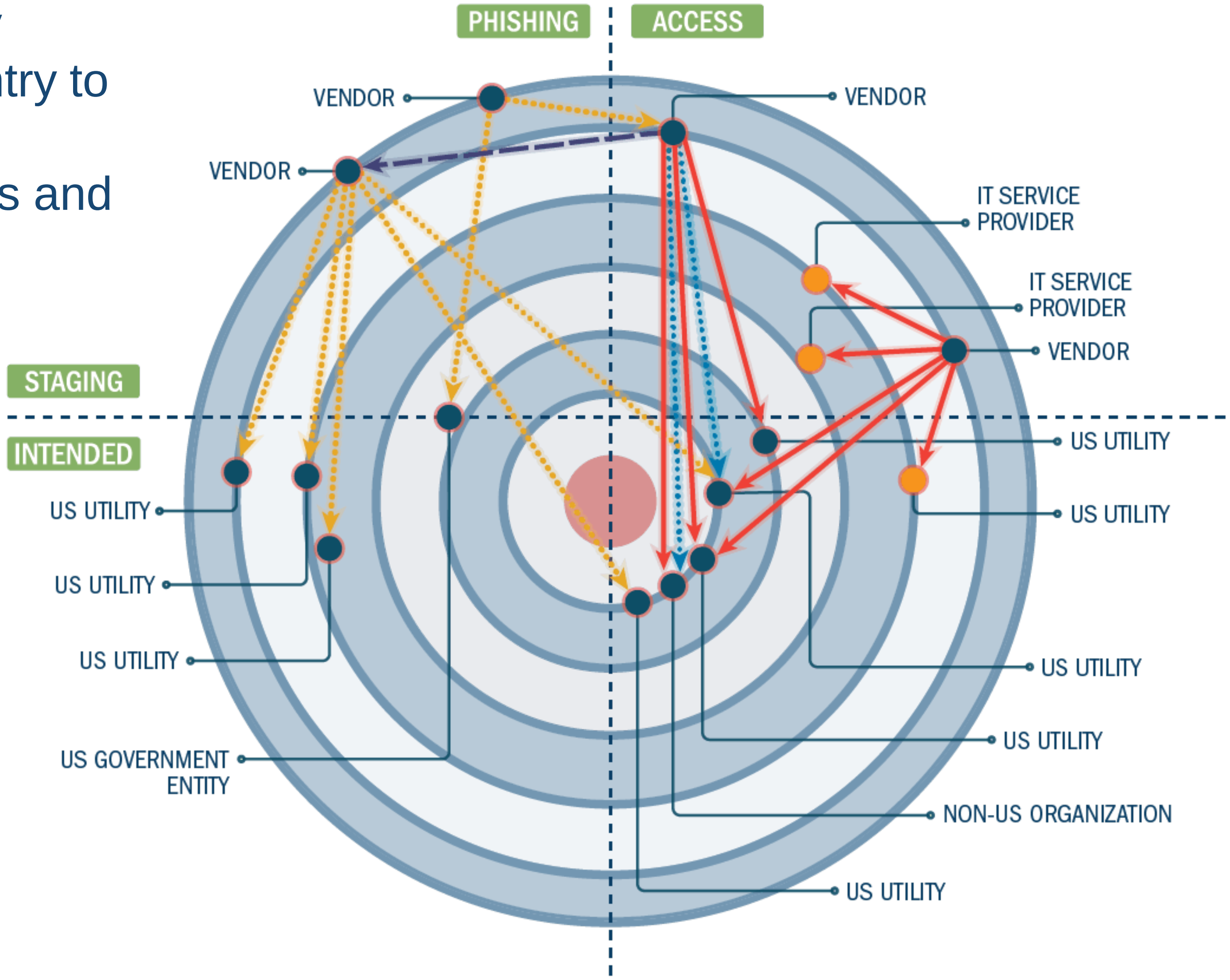
- Used initial compromised vendor to access several U.S. energy utilities and IT service providers



TLP:WHITE

Campaign Timeline

- Leveraged early victim to gain entry to two previously accessed utilities and one new victim



LEGEND

Phishing	·········➤
Access	⟶
Recon	·········➤
Test Emails	— — —➤

TLP:WHITE

Who is the Target?

Staging Targets

- **Smaller organizations** with less sophisticated networks
- **Pre-existing relationships** with intended targets
- **Deliberately selected**, not targets of opportunity
- Examples: **vendors, integrators, suppliers,** and **strategic R&D partners**
- Used for **staging tools** and **capabilities**

Intended Targets

- **Small, medium,** and **large organizations**
- U.S. targets focused within the **Energy Sector**, specifically power generation, transmission, and distribution
- **Sophisticated networks** with more defensive cyber tools

What We Will Present Today

Not a comprehensive overview of the attack

For full information, see:

- DHS Alert TA18-074A: Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors
- Third-party analysis reports

Focus of unique tactics and behaviors

Two areas of discussion

- Penetration of corporate networks
- Targeting of control systems

CORPORATE NETWORKS

Reconnaissance

Accessing the corporate websites of staging targets

Human-driven behaviors, not scripted

Lists of targets align to open-source lists (organized by subject-matter areas) published by third-party industry organizations

Downloading detailed photos of organization infrastructure published to public website by victim organization

CORPORATE NETWORKS

Credential Harvesting

Stage 1:
Request for file outbound over ports 137/139/445

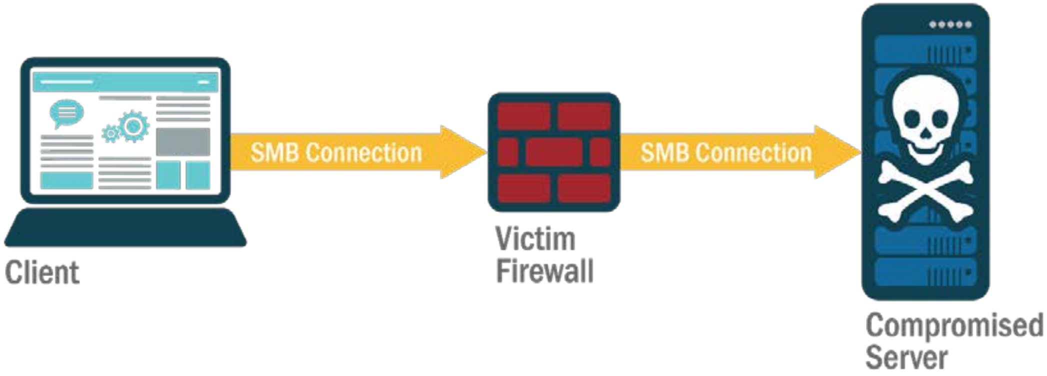
Stage 2:
Server requests credentials

Stage 3:
Victim provides user hash

Stage 4:
Server provides file

Tactic: Remote Server Message Block (SMB) server

- Spearphishing using a Microsoft Word file referencing a remote normal.dotm file
- Watering hole: Javascript leverages hidden iFrame to generate a “file://” connection to a remote server resulting in an SMB transfer of the user’s NT Local Area Network Manager (NTLM) hash



CORPORATE NETWORKS

Initial Network Access

- Primarily **leveraging captured legitimate credentials**

- All victims had **externally-facing, single-factor authenticated systems**

- Three known intrusion vectors
  - **Virtual private networks** (VPN)
  - **Outlook Web Access**
  - **Remote desktop** (both externally exposed and through VPN)

CORPORATE NETWORKS

Other Traditional TTPs

PERSISTENCE

- Legitimate credentials
- New account creation
- Scheduled tasks

COMMAND AND CONTROL

- Web Shells
- Remote Desktop

LATERAL MOVEMENT

- PsExec
- Batch Scripts
- Remote Desktop (RDP)
- Virtual Network Computing (VNC)
- Admin Shares

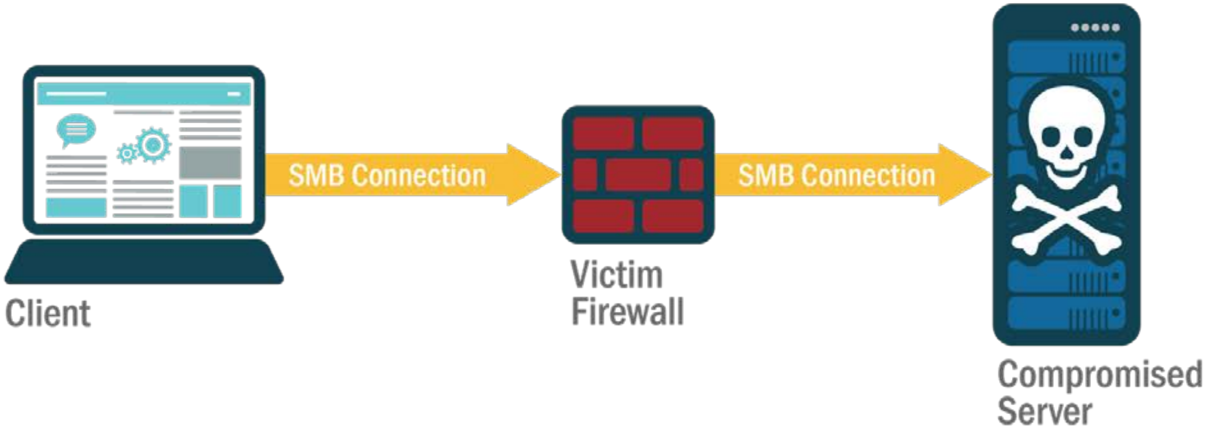
Tools leveraged were available on GitHub:

- Mimikatz
- CrackMapExec
- Angry IP
- SecretsDump
- Hydra
- Inveigh (and Inveigh-Relay)
- httrack

TLP:WHITE

CORPORATE NETWORKS

Persistence Using LNK files



Results

Active user’s credentials were obtained by the threat actor every time the directory was viewed.

Stage 1:
LNK file stored in common access directory

Stage 2:
LNK file icon file setting

Stage 3:
LNK file icon viewed using Windows Explorer

Stage 4:
Image request for file outbound over ports 137/139/445

Stage 5:
Server requests credentials

Stage 6:
Victim provided user hash

Stage 7:
Server provides image file

CONTROL SYSTEM NETWORKS

Recon and Initial Intrusions

- Threat actor conducted research using publicly available information specifically related to the control systems being operated by specific victims
- Many of the phishing emails were targeted against control systems operations and related to control system operations

TLP:WHITE

CONTROL SYSTEM NETWORKS

Tactics

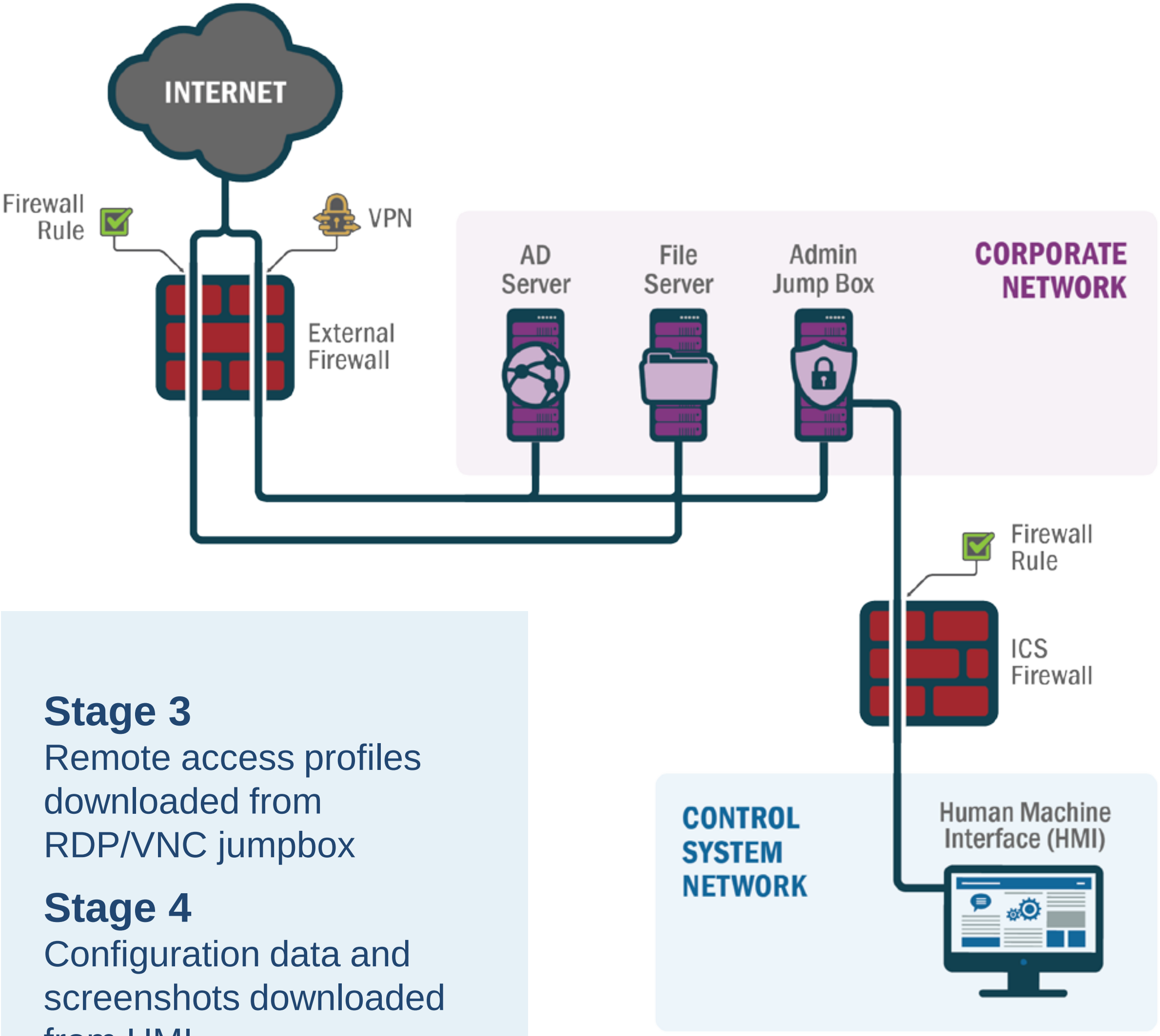
Stage 1
Access from threat actor to victim corporate network using RDP port forward already in place and/or compromised credentials through VPN

Stage 2
ICS data exfiltrated from corporate servers:

- Vendor Information
- Reference Documents
- ICS Architecture
- Layout Diagrams

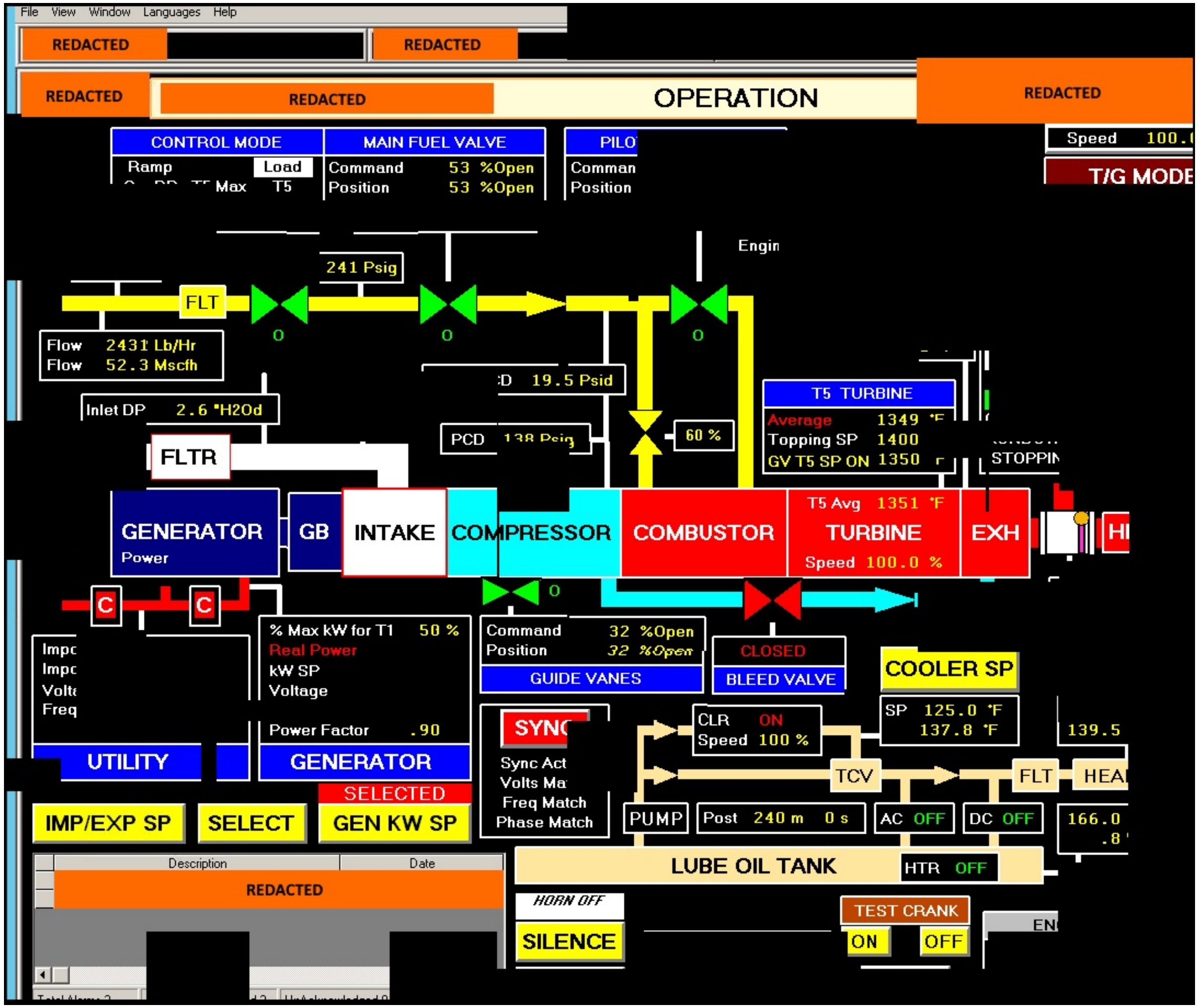
Stage 3
Remote access profiles downloaded from RDP/VNC jumpbox

Stage 4
Configuration data and screenshots downloaded from HMI



CONTROL SYSTEM NETWORKS

RDP Session of Threat Actor



Speed 100.
Ramp Load
Max T5
Command 53 %Open
Position 53 %Open
Comman
Position
241 Psig
Flow 2431 Lb/Hr
Flow 52.3 Mscfh
Inlet DP 2.6 "H2Od
:D 19.5 Psid
PCD 138 Psig
60 %
Average 1349 °F
Topping SP 1400
GV T5 SP ON 1350
T5 Avg 1351 °F
Speed 100.0 %
Generator Power
Impc
Impc
Volt
Freq
% Max kW for T1 50 %
Real Power
kW SP
Voltage
Power Factor .90
Command 32 %Open
Position 32 %Open
CLOSED
SP 125.0 °F
137.8 °F
139.5
CLR ON
Speed 100 %
Sync Act
Volts Ma
Freq Match
Phase Match
Post 240 m 0 s
AC OFF
DC OFF
166.0
.8
HTR OFF
HORN OFF

TLP:WHITE

Recommendations

Initial Triage

- Search for known indicators in historical logs (see DHS alert)
- Remain focused on behaviors (TTPs)
- Don’t whitelist network traffic with trusted partners

Continual Monitoring

- Behavior-based analysis
- Staging Targets: anticipate spearphishing and watering holes
- Intended Targets: anticipate spearphishing, C2 using legitimate credentials, and persistent scripts on workstations and servers

Related Mitigations

- Block all external SMB network traffic
- Require multi-factor authentication for all external interfaces

NCCIC

Current Focus Areas

NCCIC provides support for victims at all stages of compromise

Specifically interested in information from **victims, vendors,** and **cyber community** in the following areas:

1. Authentication by **threat actor** using **multi-factor authentication**
2. Any **direct access** or **information reconnaissance** pertaining to **control system networks**
3. **Non-interactive activities** by **threat actor** (actions other than those taken through RDP and VNC)

TLP:WHITE

NCCIC | NATIONAL CYBERSECURITY & COMMUNICATIONS INTEGRATION CENTER

NCCIC SERVICES

NCCIC

Information Sharing and Analysis

National Vulnerability Database (NVD)

Repository: Managed Automation

Automated Indicator Sharing (AIS)

Machine-to-machine: Indicators & Defensive Measures

Traffic Light Protocol (TLP)

TLP:RED

Sensitive Information to trusted Stakeholders

Cybersecurity Information Sharing & Collaboration Program (CISCP)

Voluntary: CI/Federal Government

Enhanced Cybersecurity Services (ECS)

Voluntary for System Protection

National Cyber Awareness System (NCAS)

Subscriptions for Products

NCCIC Portal

Secure Communications Platform

TLP:WHITE

NCCIC

24/7/365
OPERATIONS

Contact NCCIC

Email: nccicustomerservice@hq.dhs.gov

Phone: 1-888-282-0870

TLP:WHITE

Audience Q&A

Ask a question via the chat box.

Please complete the short survey following the webinar.
We appreciate your feedback.

NCCIC

TLP:WHITE

Thank you for joining us today!

U.S. DEPARTMENT OF HOMELAND SECURITY

NCCIC