NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Lesson Learned

Risk of Internet Accessible Cyber Assets

Primary Interest Groups
Transmission Operators (TOPs)
Transmission Owners (TOs)
Generation Operators (GOPs)
Generation Owners (GOs)
Distribution Provider (DPs)

Problem Statement
An electronic access point connected to the internet from a low-impact facility for remotely accessing a capacitor bank was compromised by unauthorized internet users for seven months prior to discovery.

Details
A registered entity discovered a compromised electronic access point connected to the internet from a low-impact facility. The access point was originally intended to be temporary and was installed by a SCADA Manager who subsequently left the entity without providing adequate documentation and turnover to the next SCADA Manager. The access point was misidentified as a remote terminal unit (RTU) with an end-of-life (EOL) operating system and left in place. Unauthorized personnel accessed the cyber asset for seven months before the registered entity became aware of the compromise. Because the device was identified as an EOL system, the compromised system was not maintained (patched, monitored, etc.) by the registered entity and was thus more susceptible to exploitable vulnerabilities.

The initial compromise resulted from an unauthorized internet user guessing via a "brute force"[1] method the weak password for the administrators' account, which permitted remote access. The compromised cyber asset was used over a seven-month period as a mail relaying (SMTP) and remote desktop (RDP) scanner.[2] Additionally, the IP address and credentials for the cyber asset were posted on a Russian-based media site, and the cyber asset was subsequently infected with ransomware.[3] The compromise was discovered after support staff could not remotely access the cyber asset. The purpose of the internet-connected access point was to remotely access and operate the capacitor banks to ensure the reliability of the system. Upon looking into the matter further, personnel discovered that the cyber asset was compromised with ransomware, so the registered entity immediately powered off the cyber asset.

[1] "Brute forcing" is an automated method of attempting authentication with many different passwords until the attacker is able to successfully login to the system
[2] A network scanner performs a scan on a network and collects an electronic inventory of the systems and the services for each device on the network. In this case, the server was used to scan for open SMTP (Simple Mail Transfer Protocol) servers and RDP (Remote Desktop Protocol) servers for potential compromise.
[3] See the NERC Alert dated 6/7/2016 "Ransomware Extortion Poses Increasing Risk"

Forensic analysis on the compromised system identified several different scanning tools designed to locate remotely accessible RDP or SMTP servers along with text files containing IP addresses for the scanners to target. Although the attackers likely conducted reconnaissance on the local network to identify other vulnerable devices, the primary focus of their activity appears to identify other remote systems to target for attacks.

Corrective Actions

The registered entity removed the compromised device from service and performed forensic analysis to identify all malware on the affected device and determine agent(s) of the compromise, time lines, and reveal (to the most possible extent) the underlying activities and motives of the compromise. A virus scan was also performed on all devices at the same site as well as a review of logs on all of the devices to look for anomalous activity. Other locations were also scanned to determine whether they had similar installations or issues.

Lesson Learned

Cyber assets at low-impact facilities capable of remote internet connectivity are susceptible to unauthorized access from the Internet or unsecured networks if not properly secured. These remote access points are typically used to provide communication paths for monitoring and control purposes to maintain BES reliability. Remote connectivity that can provide unauthorized and potentially malicious access to systems that supply auxiliary power, power quality, voltage support, fault monitoring, and breaker control is of particular concern. Failure to develop and follow appropriate policies and procedures to control the installation and maintenance of cyber assets may create exploitable vulnerabilities that could negatively impact BES reliability.

In this case, installation of, inaccurate identification of, and failing to provide adequate security protections for a device connected to a registered entity's network led to the compromise of the device. There may be several practical lessons learned that can be derived from this event that apply to low-impact cyber assets and constitute good cyber security practices in general.

Policy and Procedure:

- Train employees and contractors on cyber security awareness, policy, and practices.
- Catalog cyber assets at low-impact facilities to determine use and facilitate accurate records.
- Consult with and obtain authorization from responsible IT departments as well as compliance and risk management groups to evaluate potential risks and impacts of internet-facing and internetworked cyber assets at low-impact facilities.
- Have personnel (e.g., operations, maintenance) who perform periodic on-site visits conduct cyber device inventory checks as part of routine safety and maintenance inspections. Consider using a checklist.
- Periodically re-evaluate risks and potential impacts of the inventoried cyber assets as new threats and vulnerabilities are revealed or vendor support is discontinued.

- An entity's IT department could use tools such as Shodan[4] and nmap[5] on the entity's own public IP space on a regular basis to verify only authorized ports are open to the internet.
- When an employee or contractor leaves the company or is terminated, ensure appropriate turnover and Knowledge Transfer processes occur.

Cyber Security practices to consider for low-impact facilities:

- Identify and secure cyber assets at low-impact facilities capable of remote connectivity.
- Where possible, implement network access controls within the system to prevent the installation of unauthorized hardware.
- Implement network segmentation into trust zones.
- Change default passwords with strong passwords on user accounts and administrative accounts and restrict operational use of administrative accounts. Implement MFA (multi-factor authentication) for all internet-facing resources that support these technologies
- Provide for a patch management plan for evaluating security patching for cyber assets at low-impact facilities
- Whenever practical, monitor the network for anomalous behavior.

NERC's goal with publishing lessons learned is to provide industry with technical and understandable information that assists them with maintaining the reliability of the bulk power system. NERC requests that you provide input on this lesson learned by taking the short survey provided in the link below.

Click here for: Lesson Learned Comment Form

For more Information please contact:

NERC – Lessons Learned (via email)	WECC Event Analysis
Source of Lesson Learned:	Western Electric Coordinating Council
Lesson Learned #:	20180701
Date Published:	July 24, 2018
Category:	Transmission Facilities

This document is designed to convey lessons learned from NERC's various activities. It is not intended to establish new requirements under NERC's Reliability Standards or to modify the requirements in any existing Reliability Standards. Compliance will continue to be determined based on language in the NERC Reliability Standards as they may be amended from time to time. Implementation of this lesson learned is not a substitute for compliance with requirements in NERC's Reliability Standards.

[4] Shodan is an Internet site used to discover devices that are connected to the Internet, where they are located and who is using them.
[5] Nmap ("Network Mapper") is a free and open source (license) utility for network discovery and security auditing.