Ransomware Extortion Poses Increasing Risk

Ransomware is a special class of disruptive, malicious software designed to infiltrate networks and deny access to information and systems until the victim meets payment demands. In 2016, the Electricity Information Sharing and Analysis Center (E-ISAC) has noted a surge in both sector reporting and general media coverage indicating a significant increase in ransomware use tied to cyber extortion activity.

Why am I receiving this? >>
About NERC Alerts >>

Status: No Reporting is Required – For Information Only

PUBLIC: No Restrictions
More on handling >>

Instructions: NERC Advisories are designed to improve reliability by disseminating critical reliability information and are made available pursuant to Rule 810 of NERC’s Rules of Procedure, for such use as your organization deems appropriate. No particular response is necessary. This NERC Advisory is not the same as a Reliability Standard, and your organization will not be subject to penalties for a failure to implement any recommendations or practices provided in this Advisory. Additionally, issuance of this Advisory does not lower or otherwise alter the requirements of any approved Reliability Standard, or excuse the prior failure to follow the practices discussed in the Advisory if such failure constitutes a violation of a Reliability Standard.

Distribution: Initial Distribution: Balancing Authority, Distribution Provider, Generator Owner, Generator Operator, Interchange Authority, Load-Serving Entity, Reliability Coordinator, Transmission Owner, Transmission Operator, Transmission Planner, Transmission Service Provider
Who else will get this alert? >>
What are my responsibilities? >>

**Advisory:**

The E-ISAC is issuing this Advisory for broad awareness on destructive malicious software being used with the intent to extort a victim into paying money to regain access to data. A detailed E-ISAC Assessment was released on May 11, 2016 outlining the evolution of ransomware tactics. This assessment is available to E-ISAC members via the private portal. This advisory is an overview of the assessment. Further information can be attained by reviewing the assessment.

The E-ISAC assesses with medium confidence that extortion tactics will increase generally across all sectors and ransomware may become the financially motivated malware of choice, surpassing banking credential harvesting.

The increased accessibility of cryptocurrency (e.g., Bitcoin) and large botnets coupled with advancing ransomware capabilities and sophisticated extortion tactics provides criminals with a lower risk profile and higher potential reward. Additionally, the recent success of ransomware in the medical industry may incentivize attackers to move from broadly ransoming data on workstations and network shares to focusing further on ransoming servers and industries.

The E-ISAC is aware of at least one case where an industrial control systems (ICS) theme was used as a lure to deliver ransomware payloads. From an attacker’s perspective, a successful attack on critical operational technologies may improve the odds of a higher payoff.

The E-ISAC assesses with medium confidence that attackers will continue to increase opportunistic ransomware and also begin performing more targeted campaigns focused on direct disruption of businesses to increase the ransom and likelihood of payout. It is unknown whether the electricity subsector will become a key target of interest; however, the E-ISAC believes utilities may be seen as an attractive target.

**Background:**

*For further information, including mitigation measures, refer to the EISAC Assessment-20150511-01 report available at [https://www.eisac.com/collaboration#/document/4520](https://www.eisac.com/collaboration#/document/4520). An authorized Eisac.com username and password is required to access this.*

Currently, there are four known primary techniques involved with delivering ransomware into a victim’s environment. These delivery mechanisms include:

- Email phishing lures
- Malvertising and watering holes
- Internet-facing server exploitation
- Search Engine Optimization
Each of the nearly 100 known ransomware variants offers unique capabilities. Below is a range of capabilities when evaluating the risk of ransomware into any particular environment:

- Encryption of user files, includes local and externally-attached storage
- Encryption of network based files, includes both mapped and unmapped file shares accessible by the malware
- Manipulation of Master Boot Record to lock out computer startup process
- Destruction of Microsoft Windows Shadow Copy snapshots to prevent restoration

**Sharing Ransomware Activity with the E-ISAC**

Specific information to share about ransomware activity includes:

- If delivered via phishing, send a copy of the email in “msg” format. The emails can be delivered to the E-ISAC by zipping the file and password protecting the zip with the word “infected” in lower-case letters as the file password.
- Timeliness is critical when an adversary launches a new campaign. If the activity is recently observed, the E-ISAC recommends posting a Cyber Bulletin to the portal including the sender and subject line. This fast notification may allow all E-ISAC members to identify problematic activity not blocked by existing email security controls.
- Share any further analysis or insights when activity appears, such as actions:
  - Targeted toward a particular employee or employee function.
  - Using themes more tailored to the electricity subsector or organization.
  - Using previously unobserved tactics tools or procedures.

Generally, the E-ISAC continues to request:

- Member feedback when an indicator is potentially a false positive or low confidence.
- Additional details, including activity logs or forensic artifacts, such as binaries or network captures to derive stronger context or indicators that can be shared with members and partners.
- High-confidence indicators or signatures for both untargeted and targeted threats to the Electricity Sector.
With this information, the E-ISAC can provide updates allowing members to be more effective in detecting and scoping of this activity and other threats. We encourage members that have information regarding successful detections of threats, or updates involving suspected activity later determined benign, to share them on the E-ISAC portal (https://eisac.com).

Contact: Electricity ISAC
North American Electric Reliability Corporation
3353 Peachtree Road NE
Suite 600 – North Tower
Atlanta, GA 30326

operations@eisac.com

Alert ID: A-2016-06-07-01

You have received this message because you are listed as a primary compliance contact for your organization on the North American Electric Reliability Corporation’s compliance registry. If you believe that you have received this message in error, please notify the sender immediately and delete or otherwise dispose of all occurrences or references to this email. If you have questions about your membership in this list, please contact Bulk Power System Awareness at NERC by calling (404) 446-9797 or via email at nerc.alert@nerc.net.