Critical Broadcast Program

TLP:AMBER All-Points Bulletin 22-01
February 2, 2022

CBP APB 22-01 AWARENESS OF 'DOE ARES REPORT ON CYBERSECURITY CONSIDERATIONS DURING ONGOING TENSIONS' RELATED TO RUSSIA

Summary

The E-ISAC recommends North American electricity members and energy sector partners review the attached Department of Energy (DOE) Analysis of Risks in the Energy Sector (ARES) Report[1] to help evaluate the risk to your system from the identified threat vectors. As referenced by recent U.S.[2] and Canadian government[3] postings, if the government of the Russia believes the U.S. and its North Atlantic Treaty Organization (NATO) Allies are interfering in an escalating conflict in Eastern Europe, then it could target North American critical infrastructure in an attempt to undermine U.S. influence and deter further support for the Ukrainian government.

At the time of publication, the E-ISAC is not aware of any specific targeting of North American electricity industry members by Russia-linked adversaries. However, the E-ISAC assesses with **MODERATE** confidence (derived from other unclassified finished-intelligence products) that the threat to energy infrastructure from Russia-linked adversaries will likely increase if the conflict with Ukraine escalates. Members are encouraged to evaluate the threat vectors contained within this APB and the DOE ARES. Per the recommendations found in the ARES report, members should focus on the threat to the following:

- Jump Boxes
- Media Converters (e.g. serial-to-Ethernet)
- Protective Equipment and Safety Systems
- Third-Party Provided/Leased Communications Infrastructure Satellite Communications (e.g. Very Small Aperture Terminals (VSAT))

The E-ISAC also recently prepared a short "Preparedness Guide for Potential Russian State Sponsored Cyber Threats" that illustrates a conflict escalation ladder that may be used internally to guide potential internal thresholds for the activation of plans, and covers similar Russia-linked threats based on historical use cases.

Impact

Russia-linked adversaries demonstrated the capability and intent to use cyber means to attack critical infrastructure in the energy sector. As the U.S. Director of National Intelligence Worldwide Threat Assessment states, "Russia almost certainly considers cyber-attacks an acceptable option to deter

[1] U.S. Department of Energy, Analysis of Resilience in the Energy Sector (ARES) Report — attached
[2] U.S. Department of Homeland Security Cybersecurity and Infrastructure Security Agency (CISA), Alert (AA22-011A) "Understanding and Mitigating Russian State-Sponsored Cyber Threats to U.S. Critical Infrastructure" — https://www.cisa.gov/uscert/ncas/alerts/aa22-011a
[3] Canadian Centre for Cyber Security, "The Russian State-sponsored Cyber Threat to Canada's Critical Infrastructure" — https://www.eisac.com/portal-home/cyber-bulletin-detail?id=137201

TLP:AMBER – Limited disclosure, restricted to E-ISAC members and partners.

adversaries, control escalation, and prosecute conflicts."[4] If the current situation in Ukraine escalates, and NATO countries retaliate in some form threatening Russia's perceived interests, cyber-attacks could be used against North American critical infrastructure in an effort to influence NATO decision making. Furthermore, while an attack may not cause widespread outages, even small customer outages could be amplified through disinformation in an effort to sway North American political opinion away from supporting NATO or Ukraine—highlighting the need for unity of message between industry and government if an attack occurs.

What to Do

The DOE ARES report highlighted five areas to focus on for heightened preparedness to help counter threats from Russia-linked adversaries:

Jump Boxes

Jump boxes (or jump servers) represent attractive targets for adversary activity as these assets enable deeper access to the OT network and may provide high-privilege connections or activities.

- **Harden Jump Boxes:** Restrict the networks, subnets, and hosts the jump box can access, constraining adversary movement if compromised; enable multi-factor authentication if possible.
- **Increase and Segment Logging:** Monitor and log activity at jump boxes.
- **Consider a Disconnection Strategy:** Ensure that jump boxes can be disconnected without major impacts to operations, if needed; operations staff are well versed on disconnection strategies.

Media Converters

Media converters enable connections between two networks or networked devices, even if the communications paths are dissimilar (e.g., serial-to-Ethernet). Permanent loss of control could require replacement of affected media converters to restore functionality, as was the case in Ukraine 2015.

- **Decrease, Closely Monitor, and Tightly Control Remote Access Points:** Operationally necessary access should be time-limited and restricted to operators with multi-factor authentication.
- **Consider Prioritized Mitigation:** Many serial converters leverage older operating systems and have known vulnerabilities. Follow manufacturer and CISA guidance regarding patching schedules or alternative mitigations to ensure resilience to known vulnerabilities (CVEs in ARES).

Third-Party Provided/Leased Communications Infrastructure

Potential targeting of third party leased communications infrastructure may include, but is not limited to: fiber optics, dial-up, microwave, radio frequency, cellular, or satellite communications, including VSAT. VSAT communications are not encrypted by default and can disclose confidential information if not secured with additional protection methods. Remote exploitation of security vulnerabilities in VSAT systems could allow attackers entry into corporate or OT networks.

- **Identify Alternative Communications Infrastructure:** Implement alternative communications infrastructure to critical assets where possible. Test alternative voice communications channels.

[4] U.S. Director of National Intelligence, "2021 Worldwide Threat Assessment" — https://www.dni.gov/files/ODNI/documents/assessments/ATA-2021-Unclassified-Report.pdf

TLP:AMBER – Limited disclosure, restricted to E-ISAC members and partners.

- **Validate Cryptographic Integrity and Data Protection:** Ensure suitable cryptographic and access controls on data at-rest and in transit, as well as related metadata. Where possible, implement encrypted VPN tunnels for the transfer of sensitive or operational data.
- **Encrypt Network Communications:** Leased infrastructure may provide varying levels of cybersecurity protection based on parameters outside lessee control. Ensure that link encryption is used for third party infrastructure where cybersecurity risk cannot be fully evaluated.

Additionally, the E-ISAC further recommends (based off a recent National Security Agency advisory) the following VSAT security:

- Determine if VSAT technology is in use in enterprise or OT environments; review any applicable vendor or manufacturer advisories to determine the extent of susceptibility.
- Review and audit configurations for any default username and password entries. Secure VSAT communications with encryption technology such as Internet Protocol Security or Transport Layer Security virtual private networks.
- Additionally, the E-ISAC recommends Asset Owner and Operators audit historic inbound remote connections for suspicious traffic to all remote access solutions deployed.

Additional Notes

The E-ISAC will continue to monitor for related activity if observed in the electricity sector or closely related sectors, and will provide relevant updates to further the information as it becomes available. If you have any questions or comments, please contact operations@eisac.com or dial Watch Operations at **202-790-6000**. Members and partners are also encouraged to share information through these channels and posting vetted information on the E-ISAC Portal where appropriate.

References

DOE Geopolitical Awareness Webinar on previous Russian-linked cyber activity, December 17, 2021 — https://www.eisac.com/portal-home/cyber-bulletin-detail?id=136487

E-ISAC, "Preparedness Guide for Potential Russian State Sponsored Cyber Threats, January 12, 2021 — https://www.eisac.com/portal-home/cyber-bulletin-detail?id=136982

E-ISAC and the SANS Institute, "ICS Defense Use Case No. 6 – Modular ICS Malware," August 2, 2017 — https://www.eisac.com/cartella/Asset/00006542/TLP_WHITE_E-ISAC_SANS_Ukraine_DUC_6_Modular_ICS_Malware_Final.pdf?parent=64412

Mandiant, "Proactive Preparation and Hardening to Protect Against Destructive Attacks" — https://www.mandiant.com/media/14506/download

National Security Agency, Cybersecurity Advisory, "Protecting VSAT Communications" — https://media.defense.gov/2022/Jan/25/2002927101/-1/-1/0/CSA_PROTECTING_VSAT_COMMUNICATIONS_01252022.PDF

U.S. DEPARTMENT OF ENERGY | Office of Cybersecurity, Energy Security, and Emergency Response

ARES Report

Analysis of Risks in the Energy Sector (ARES)

REPORT TITLE:	Cybersecurity Considerations During Ongoing Geopolitical Tensions
REPORT DATE:	Wednesday, February 2, 2022
REPORT NUMBER:	ARES-22-0202-01

*The following Analysis of Risks in the Energy Sector (ARES) Report has been released by the U.S. Department of Energy (DOE) at **TLP:AMBER** to energy sector industry partners. Recipients may only share this information with members of their own organization with a need to know. This report may contain OFFICIAL USE ONLY information and is not intended for public disclosure or dissemination unless otherwise approved by the U.S. Department of Energy.*

OVERVIEW

The U.S. Department of Energy (DOE) is releasing this *Analysis of Risks in the Energy Sector* (ARES) Report as part of our continued efforts to share critical information about cybersecurity risks with energy industry partners. Increased geopolitical tensions in Eastern Europe highlight potential threats to U.S. critical energy infrastructure. This ARES Report provides information on cybersecurity threats and suggested mitigation measures to help reduce the risk presented by these threats to U.S. energy infrastructure across the electricity and oil and natural gas sectors. At this time of heightened tensions in Eastern Europe, energy sector entities must remain vigilant against potential cyber threats. **The targets and mitigations below are particularly relevant to the current geopolitical tensions and are an important area of focus.**

At this time, DOE is sharing the following cybersecurity risks to the energy sector:

- Jump Boxes
- Media Converters
- Protective Equipment and Safety Systems
- Third-Party Provided/Leased Communications Infrastructure

Additionally, DOE encourages energy sector asset owners and operators to lower the bar for sharing anomalous information to the government or your respective ISAC as an additional measure of collective defense.

EXPLOITS AND TECHNIQUES

In order for cyber adversaries to successfully attack critical infrastructure, they must develop both tools for access and the ability to cause impacts. These capabilities are often described as Stage I and Stage II capabilities, as referenced by the SANS ICS Cyber Kill Chain.[1] The time to develop a malicious cyber campaign can range from a few hours to several years. For example, Cisco Talos's analysis of WhisperGate assessed that attackers likely achieved access to victim networks months ahead of the mid-January 2022 attack against Ukrainian organizations.[2]

Cyber actors have been observed abusing federated authentication infrastructure to gain access to protected data and access legitimate credentials, challenging the identification of suspicious and malicious activity. For instance, actors have achieved initial access through the exploitation of public facing applications (T1190) through various brute force attacks.[3] NSA has warned about the theft of Security Assertion Markup Languages (SAML) or global administrator accounts to gain access to central or cloud resources.[4]

Cyberattacks directed against energy sector OT and enabling communications infrastructure could result in the following impacts:

- **Denial of view** (T0815) which temporary impacts operator visibility into the OT environment, potentially silencing error messages or statuses;[5]
- Temporary, sustained, or permanent **loss of view** (T0829) which results in a disruption to normal operating procedures, including electric grid operations and ONG-associated distribution;[6]
- **Loss of control** (T0827) resulting from destruction of critical control infrastructure, including configuration settings, registry, or point IDs tables.[7]
- **Loss of safety** (T0880) or the disruption of protection features through deliberate or unintended result of cyber manipulation.[8]

TARGETS AND MITIGATIONS

Jump Boxes

Jump boxes (or jump servers) represent attractive targets for adversary activity as these assets enable deeper access to the OT network and may provide high-privilege connections or activities. In some cases, these devices serve as a critical component for remote management of other assets, and within the OT environment, often enable the movement of data between networks or enclaves.

Recommended mitigations include:

- **Harden Jump Boxes:** Aim to create single-purpose jump boxes with limited applications available on the server. Restrict the networks, subnets, and hosts the jump box can access, constraining adversary movement in the event the server is compromised. Enable multi-factor authentication to jump boxes.
- **Increase and Segment Logging:** Monitor and log activity at jump boxes. Ensure these logs are replicated off the jump box to challenge adversary attempts at log destruction.
- **Consider a Disconnection Strategy:** Ensure that jump boxes can be disconnected without major impacts to operations, if needed. Further, ensure that relevant operations staff who manage jump boxes are well versed on disconnection strategies.

Media Converters

Media converters enable connections between two networks or networked devices, even if the communications paths are dissimilar (e.g., serial-to-Ethernet). Attacks directed against these devices could result in the temporary or permanent loss of information about the status of operational assets (view conditions). It is also possible that disruptions to, or destruction of, media converters could limit or eliminate remote control of serially connected field deployed equipment. Permanent loss of control could require replacement of affected media converters to restore functionality, as was the case in Ukraine following the December 2015 cyberattacks.[9]

Suggested mitigations include:

- **Decrease, Closely Monitor, and Tightly Control Remote Access Points:** Limiting remote access wherever possible within the OT networks decreases the potential technical targets from which a cyber-actor can conduct their operations. Operationally necessary access, such as administration capability, should be time limited, isolated from untrusted networks, and restricted to operators with multi-factor authentication.
- **Consider Prioritized Mitigation:** Many serial converters leverage older operating systems and have known vulnerabilities. Follow manufacturer and CISA guidance regarding patching schedules or alternative mitigations to ensure resilience to known vulnerabilities, for example as CVE-2016-4500,[10] CVE-2016-2309,[11] CVE-2018-8869,[12] CVE-2018-8865,[13] and CVE-2017-16272.[14]

Protective Equipment and Safety Systems

The cyberattack against the Ukrainian energy sector in 2016 identified the existence of malware designed to force protective relays into an unresponsive state, inhibiting their protective function.[15] During a 2017 cyber intrusion at a petrochemical facility, Russian state sponsored actors also demonstrated capabilities (Triton/Trisis/HatMan) designed to disrupt and modify safety instrumented systems.[16] Although use of these capabilities will not result in long-term outages without additional adversary action, pairing these capabilities with other operations could result in unsafe conditions and potential damage to energy equipment. Depending on the attack, recovery options can be as simple as manually restarting the equipment or as complex as replacing affected hardware.

Suggested mitigations include:

- **Ensure Out-of-Band Recovery Plans and Backup Information Exist:** Ensure critical energy equipment (e.g., workstations, servers, networking and automation devices) can be fully restored from backups, and that these backups and associated data are stored offline in non-networked assets or in enclave networks. Consider storing paper-based instruction and configuration settings for critical equipment. Brief personnel on communication plans and asset recovery activities in the event of a disruption.
- **Ability to Disable or Restrict Remote Access to Protection Equipment and Safety Systems:** Temporarily disable remote access to protection equipment where possible. In cases where remote access is operationally necessary, restrict to select users and enable temporary access only.

Third-Party Provided/Leased Communications Infrastructure

Deliberate targeting of third-party communications infrastructure can provide cyber actors with the necessary access to conduct initial reconnaissance or Stage 2 cyberattacks. Potential targeting of third party leased communications infrastructure may include, but is not limited to: fiber optics, dial-up, microwave, radio frequency (RF), cellular, or satellite communications, including very small aperture terminal (VSAT). In many cases, the links between sites are unencrypted, relying on the private nature of these infrastructures, frequency hopping, or frequency separation for security and anonymity.[17]

Further, previous cybersecurity alerts (CSA) have warned about the potential threat vectors introduced into 5G infrastructure, however, many of these risks are also prevalent in legacy cellular infrastructure as well.[18] Additional potential risks are introduced when cloud-based services rely on cellular systems.[19]

Suggested mitigations include:

- **Identify Alternative Communications Infrastructure:** Implement alternative communications infrastructure to critical assets where possible. Test alternative voice communications channels.

- **Validate Cryptographic Integrity and Data Protection:** Ensure suitable cryptographic and access controls on data at-rest and in transit, as well as related metadata. Where possible, implement encrypted VPN tunnels for the transfer of sensitive or operational data.
- **Encrypt Your Network Communications:** Leased infrastructure may provide varying levels of cybersecurity protection based on parameters outside lessee control. Ensure that link encryption is used for third party infrastructure where cybersecurity risk cannot be fully evaluated.[20]

Other Considerations

Additionally, these other mitigations are suggested:

- **Exercise Plans to Separate IT from OT Environments:** Where the capability exists, exercise plans for proactive separation of connections between IT and OT networks to minimize potential access vectors.
- **Limit Connectivity to IT and OT Networks:** Decrease connections between IT and OT networks where possible. Additionally, network administrators should consider blocking all inbound TOR traffic or traffic from public VPN services.
- **Lower Threshold for Anomaly Reporting:** Encourage increased vigilance and pay particular attention to suspicious or unexplainable observations. Share information relating to anomalies and cyber events with ISACs and threat information organizations
- **Refresh and re-distribute** cyber incident communication and response plans.

RELATED REPORTING

1. DHS-I&A; DHS-IB-2022-00927; (U) Warning of Potential for Cyber Attacks Targeting the United States in the Event of a Russian Invasion of Ukraine; 23 January 2022. https://hsin.dhs.gov/ci/iir/TSAintel/Intelligence%20Products/(U%20FOUO)%20IIB%20-%20Warning%20of%20Potential%20for%20Cyber%20Attacks%20Targeting%20-%2020220123.pdf
2. NSA; 172865-19; (U) Protecting VSAT Communications; 25 January 2022; https://media.defense.gov/2022/Jan/25/2002927101/-1/-1/0/CSA_PROTECTING_VSAT_COMMUNICATIONS_01252022.PDF.
3. CISA; ICS Alert (IR-ALERT-H-16-056-01); Cyber-Attack against Ukrainian Critical Infrastructure; 25 February 2016; https://www.cisa.gov/uscert/ics/alerts/IR-ALERT-H-16-056-01.
4. NSA/CISA/FBI/NCSC; U/OO/158036-21; "Russian GRU Conducting Global Brute Force Campaign to Compromise Enterprise and Cloud Environments"; July 2021; https://media.defense.gov/2021/Jul/01/2002753896/-1/-1/1/CSA_GRU_GLOBAL_BRUTE_FORCE_CAMPAIGN_UOO158036-21.PDF.
5. CISA; Alert (AA20-183A); "Defending against Malicious Cyber Activity Originating from TOR"; 1 July 2020; https://www.cisa.gov/uscert/ncas/alerts/aa20-183a.

ADDITIONAL INFORMATION AND FEEDBACK

DOE encourages recipients who identify the use of the indicators of compromise, tools, or techniques discussed in this document to report information to the relevant Information and Analysis and Sharing Center (ISAC):

- Downstream Natural Gas: analyst@dngisac.com
- Electricity: operations@eisac.com
- Oil & Natural Gas: soc@ongisac.org

For questions, comments, or concerns related to this report, please contact doeares@hq.doe.gov.

---

[1] (U); SANS; "The Industrial Control System Cyber Kill Chain"; 25 October 2015; https://www.sans.org/white-papers/36297/?msc=blog-ics-library.
[2] (U); Cisco Talos; "Ukraine Campaign Delivers Defacement and Wipers, in Continued Escalation;" 21 January 2022; https://blog.talosintelligence.com/2022/01/ukraine-campaign-delivers-defacement.html
[3] (U); NSA, CISA, FBI and NCSC; U/OO/158036-21; "Russian GRU Conducting Global Brute Force Campaign to Compromise Enterprise and Cloud Environments"; July 2021; https://media.defense.gov/2021/Jul/01/2002753896/-1/-1/1/CSA_GRU_GLOBAL_BRUTE_FORCE_CAMPAIGN_UOO158036-21.PDF.
[4] (U); NSA; U/OO/198854-20; "Detecting Abuse of Authentication Mechanisms"; Dec. 2020; media.defense.gov/2020/Dec/17/2002554125/-1/-1/0/AUTHENTICATION_MECHANISMS_CSA_U_OO_198854_20.PDF.
[5] (U); MITRE; "Denial of View"; https://collaborate.mitre.org/attackics/index.php/Technique/T0815.
[6] (U); MITRE; "Loss of View"; https://collaborate.mitre.org/attackics/index.php/Technique/T0829.
[7] (U); MITRE; "Loss of Control"; https://collaborate.mitre.org/attackics/index.php/Technique/T0827.
[8] (U); MITRE; "Loss of Safety"; https://collaborate.mitre.org/attackics/index.php/Technique/T0880.
[9] (U); Abir Shehod; MIT; "Ukraine Power Grid Cyberattack and US Susceptibility: Cybersecurity Implications if Smart Grid Advances in the U.S."; December 2016; https://web.mit.edu/smadnick/www/wp/2016-22.pdf.
[10] (U); CISA; ICS Advisory (ICSA-16-152-01): Moxa UC 7408-LX-Plus Firmware Overwrite Vulnerability; 31 May 2016; cisa.gov/uscert/ics/advisories/ICSA-16-152-01.
[11] (U) CISA; ICS Advisory (ICSA-16-138-01A); IRZ RUH2 3G Firmware Overwrite Vulnerability (Update A); 22 December 2016; cisa.gov/uscert/ics/advisories/ICSA-16-138-01.
[12] (U); CISA; ICS Advisory (ICSA-18-123-01); 3 May 2018; cisa.gov/uscert/ics/advisories/ICSA-18-123-01.
[13] (U); CISA; ICS Advisory (ICSA-18-123-01); 3 May 2018; cisa.gov/uscert/ics/advisories/ICSA-18-123-01.
[14] (U); CISA; ICS Advisory (ICSA-17-355-01); 21December 2017; cisa.gov/uscert/ics/advisories/ICSA-17-355-01.
[15] (U); ESET; "WIN32/INDUSTROYER: A New Threat for Industrial Control Systems"; 12 June 2017; welivesecurity.com/wp-content/uploads/2017/06/Win32_Industroyer.pdf.
[16] (U); CISA; Alert (A22-011A); (U) Understanding and Mitigating Russian State-Sponsored Cyber Threats to Critical Infrastructure; 11 January 2022; cisa.gov/uscert/ncas/alerts/aa22-011a.
[17] (U); NSA; 172865-19; (U) Protecting VSAT Communications; 25 January 2022; media.defense.gov/2022/Jan/25/2002927101/-1/-1/0/CSA_PROTECTING_VSAT_COMMUNICATIONS_01252022.PDF.
[18] (U); NSA/CISA/FBI; "Potential Threat Vectors to 5G Infrastructures"; TLP:WHITE; 2021; media.defense.gov/2021/May/10/2002637751/-1/-1/0/POTENTIAL%20THREAT%20VECTORS%20TO%205G%20INFRASTRUCTURE.PDF.
[19] (U); CISA/NSA; Security Guidance for 5G Cloud Infrastructures; 2021; media.defense.gov/2021/Oct/28/2002881720/-1/-10/SECURITY_GUIDANCE_FOR_5G_CLOUD_INFRASTRUCTURES_PART_I_20211028.PDF.
[20] (U//FOUO) NSA; 172865-19; (U) Protecting VSAT Communications; 25 January 2022.