JOINT
CYBERSECURITY
ADVISORY

Product ID: AA25-343A

December 9, 2025

Co-Authored by:

EUROPOL
EC3 European Cybercrime Centre

EUROJUST
European Union Agency for Criminal Justice Cooperation

Australian Government
Australian Signals Directorate
ASD Australian Signals Directorate
ACSC Australian Cyber Security Centre

Communications Security Establishment Canada
Centre de la sécurité des télécommunications Canada
Canadian Centre for Cyber Security
Centre canadien pour la cybersécurité

Canadian Security Intelligence Service
Service canadien du renseignement de sécurité

NÚKIB

UNCyber

JUNALCO

Federal Office for Information Security

POLICIJA

National Cyber Security Centre
NEW ZEALAND

POLICIA NACIONAL

Polisen

National Cyber Security Centre
a part of GCHQ

Pro-Russia Hacktivists Conduct Opportunistic Attacks Against US and Global Critical Infrastructure

To report suspicious or criminal activity related to information found in this joint Cybersecurity Advisory, contact your local FBI field office or CISA's 24/7 Operations Center at contact@cisa.dhs.gov or 1-844-Say-CISA (1-844-729-2472). When available, please include the following information regarding the incident: date, time, and location of the incident; type of activity; number of people affected; type of equipment used for the activity; the name of the submitting company or organization; and a designated point of contact.

This document is marked TLP:CLEAR. Disclosure is not limited. Sources may use TLP:CLEAR when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:CLEAR information may be distributed without restriction. For more information on the Traffic Light Protocol, see Traffic Light Protocol (TLP) Definitions and Usage.

Actions for Operational Technology Owners and Operators to Take Today to Mitigate Cyber Threats Related to Pro-Russia Hacktivists Activity

- **Reduce** exposure of operational technology (OT) assets to the public-facing internet.
- **Adopt** mature asset management processes, including mapping data flows and access points.
- **Ensure** that OT assets are using robust authentication procedures.

Summary

Note: This joint Cybersecurity Advisory is being published as an addition to the Cybersecurity and Infrastructure Security Agency (CISA) May 6, 2025, joint fact sheet Primary Mitigations to Reduce Cyber Threats to Operational Technology and European Cybercrime Centre's (EC3) Operation Eastwood, in which CISA, Federal Bureau of Investigation (FBI), Department of Energy (DOE), Environmental Protection Agency (EPA), and EC3 shared information about cyber incidents affecting the operational technology (OT) and industrial control systems (ICS) of critical infrastructure entities in the United States and globally.

FBI, CISA, National Security Agency (NSA), and the following partners—hereafter referred to as "the authoring organizations"—are releasing this joint advisory on the targeting of critical infrastructure by pro-Russia hacktivists:

- U.S. Department of Energy (DOE)
- U.S. Environmental Protection Agency (EPA)
- U.S. Department of Defense Cyber Crime Center (DC3)
- Europol European Cybercrime Centre (EC3)
- EUROJUST – European Union Agency for Criminal Justice Cooperation
- Australian Signals Directorate's Australian Cyber Security Centre (ASD's ACSC)
- Canadian Centre for Cyber Security (Cyber Centre)
- Canadian Security Intelligence Service (CSIS)
- Czech Republic Military Intelligence (VZ)
- Czech Republic National Cyber and Information Security Agency (NÚKIB)
- Czech Republic National Centre Against Terrorism, Extremism, and Cyber Crime (NCTEKK)
- French National Cybercrime Unit – Gendarmerie Nationale (UNC)
- French National Jurisdiction for the Fight Against Organized Crime (JUNALCO)
- German Federal Office for Information Security (BSI)
- Italian State Police (PS)
- Latvian State Police (VP)
- Lithuanian Criminal Police Bureau (LKPB)
- New Zealand National Cyber Security Centre (NCSC-NZ)

- Romanian National Police (PR)
- Spanish Civil Guard (GC)
- Spanish National Police (CNP)
- Swedish Polisen (SC3)
- United Kingdom National Cyber Security Centre (NCSC-UK)

The authoring organizations assess pro-Russia hacktivist groups are conducting less sophisticated, lower-impact attacks against critical infrastructure entities, compared to advanced persistent threat (APT) groups. These attacks use minimally secured, internet-facing virtual network computing (VNC) connections to infiltrate (or gain access to) OT control devices within critical infrastructure systems. Pro-Russia hacktivist groups—Cyber Army of Russia Reborn (CARR), Z-Pentest, NoName057(16), Sector16, and affiliated groups—are capitalizing on the widespread prevalence of accessible VNC devices to execute attacks against critical infrastructure entities, resulting in varying degrees of impact, including physical damage. Targeted sectors include Water and Wastewater Systems, Food and Agriculture, and Energy.

The authoring organizations encourage critical infrastructure organizations to implement the recommendations in the **Mitigations** section of this advisory to reduce the likelihood and impact of pro-Russia hacktivist-related incidents. For additional information on Russian state-sponsored malicious cyber activity, see CISA’s Russia Threat Overview and Advisories webpage.

Table of Contents

Background and Development of Pro-Russia Hacktivist Groups

Over the past several years, the authoring organizations have observed pro-Russia hacktivist groups conducting cyber operations against numerous organizations and critical infrastructure sectors worldwide. The escalation of the Russia-Ukraine conflict in 2022 significantly increased the number of these pro-Russia groups. Consisting of individuals who support Russia's agenda but lack direct governmental ties, most of these groups target Ukrainian and allied infrastructure. However, among the increasing number of groups, some appear to have associations with the Russian state through direct or indirect support.

Cyber Army of Russia Reborn

The authoring organizations assess that the Russian General Staff Main Intelligence Directorate (GRU) Main Center for Special Technologies (GTsST) military unit 74455—tracked in the cybersecurity community under several names (see **Appendix B: Additional Designators Used for Cited Groups**)—is likely responsible for supporting the creation of CARR —also known as "The People's Cyber Army of Russia"—in late February or early March of 2022. Actors suspected to be from GRU unit 74455 likely funded the tools CARR threat actors used to conduct distributed denial-of-service (DDoS) attacks through at least September 2024.

In April 2022, the group began using a new Telegram channel featuring the name "CyberArmyofRussia_Reborn" to organize and plan group actions. The channel creators recruited actors to use CARR as an unattributable platform for conducting cyber activities beneath the level of an APT, aimed at deterring anti-Russia rhetoric. CARR threat actors presented themselves as a group of pro-Russia hacktivists supporting Russia's stance on the Ukrainian conflict, and they soon began claiming responsibility for DDoS attacks against the U.S. and Europe for supporting Ukraine.

CARR documented these actions through embellished images and videos shared on their social media channels, promoting Russian ideology, disseminating talking points, and publicizing leaked information from hacks attributed to Russian state threat actors.

In late 2023, CARR expanded their operations to include attacks on industrial control systems (ICS), claiming an intrusion against a European wastewater treatment facility in October 2023. In November 2023, CARR targeted human-machine interface (HMI) devices, claiming intrusions at two U.S. dairy farms.

The authoring organizations assess that by late September 2024, CARR channel administrators became dissatisfied with the level of support and funding provided by the GRU. This dissatisfaction led CARR administrators and an administrator from another hacktivist group, NoName057(16), to create the Z-Pentest group, employing the same tactics, techniques, and procedures (TTPs) as CARR but separate from GRU involvement.

NoName057(16)

The authoring organizations assess that the Center for the Study and Network Monitoring of the Youth Environment (CISM), established on behalf of the Kremlin, created NoName057(16) as a covert project within the organization. Senior executives and employees within CISM developed and customized the NoName057(16) proprietary DDoS tool `DDoSia`, paid for the group's network infrastructure, served as administrators on NoName057(16) Telegram channels, and selected DDoS targets.

Active since March 2022, NoName057(16) has conducted frequent DDoS attacks against government and private sector entities in North Atlantic Treaty Organization (NATO) member states and other European countries perceived as hostile to Russian geopolitical interests. The group operates primarily through Telegram channels and used GitHub, alongside various websites and repositories, to host `DDoSia` and share materials and TTPs with their followers.

In 2024, NoName057(16) began collaborating closely with other pro-Russia hacktivist groups, operating a joint chat with CARR by mid-2024. In July 2024, NoName057(16) jointly claimed responsibility with CARR for an alleged intrusion against OT assets in the U.S. The high degree of cooperation with CARR likely contributed to the formation of Z-Pentest, which is composed of actors and administrators from both teams, in September 2024.

Z-Pentest

Established in September 2024, Z-Pentest is composed of members from CARR and NoName057(16). The group specializes in OT intrusion operations targeting globally dispersed critical infrastructure entities. Additionally, the group uses “hack and leak” operations and defacement attacks to draw attention to their pro-Russia messaging. Unlike other pro-Russia hacktivist groups, Z-Pentest largely avoids DDoS activities, claiming OT intrusions as attempts to garner more attention from the media.

Shortly after Z-Pentest’s inception, the group announced alliances with CARR and NoName057(16), possibly to leverage the other groups’ subscribers to grow the new channel. In March 2025, Z-Pentest posted evidence claiming OT device intrusions to their channel using a NoName057(16) cyberattack campaign hashtag. Similarly, in April 2025, Z-Pentest shared a video purporting defacement of an HMI by changing system names to NoName057(16) and CARR references. Z-Pentest continues to create new alliances with other groups, like Sector16, to continue growing their subscriber base and incidentally propagate TTPs with new partners.

Sector16

Formed in January 2025, Sector16 is a novice pro-Russia hacktivist group that emerged through collaboration with Z-Pentest. Sector16 actively maintains an online presence, including a public Telegram channel where they share videos, statements, and claims of compromising U.S. energy infrastructure. These communications often align with pro-Russia narratives and reflect their self-proclaimed support for Russian geopolitical objectives.

Members of Sector16 may have received indirect support from the Russian government in exchange for conducting specific cyber operations that further Russian strategic goals. This aligns with broader Russian cyber strategies that involve leveraging non-state threat actors for certain cyber activities, adding a layer of deniability.

Technical Details

Note: This advisory uses the MITRE ATT&CK® Matrix for Enterprise framework, version 18. See the **MITRE ATT&CK Tactics and Techniques** section of this advisory for a table of the threat actors' activity mapped to MITRE ATT&CK tactics and techniques.

TTP Overview

Pro-Russia hacktivist groups employ easily disseminated and replicated TTPs across various entities, increasing the likelihood of widespread adoption and escalating the frequency of intrusions. These groups have limited capabilities, frequently misunderstanding the processes they aim to disrupt. Their apparent low level of technical knowledge results in haphazard attacks where actors intend to cause physical damage but cannot accurately anticipate actual impact. Despite these limitations, the authoring organizations have observed these groups willfully cause actual harm to vulnerable critical infrastructure.

Pro-Russia hacktivist groups use the TTPs in this Cybersecurity Advisory to target virtual network computing (VNC)-connected HMI devices. These groups are primarily seeking notoriety with their actions. While they have caused damage in some instances, they regularly make false or exaggerated claims about their attacks on critical infrastructure to garner more attention. They frequently misrepresent their capabilities and the impacts of their actions, portraying minor incursions as significant breaches, but such incursions can still lead to lost time and resources for operators remediating systems.

Additionally, pro-Russia hacktivists use an opportunistic targeting methodology. They leverage superficial criteria, such as victim availability and existing vulnerabilities, rather than focusing on strategically significant entities. Their lack of strategic focus can lead to a broad array of targets, ranging from water treatment facilities to oil well systems. Pro-Russia hacktivists have demonstrated a pattern of frequently taking advantage of the widespread availability of vulnerable VNC connections. While system owners typically use VNC connections for legitimate remote system access functions, threat actors can maliciously use these connections to broadly target numerous platforms and services. Consequently, these groups can indiscriminately compromise critical infrastructure entities, including those in the Water and Wastewater, Food and Agriculture, and Energy Sectors.

Pro-Russia hacktivist groups have successfully targeted supervisory control and data acquisition (SCADA) networks using basic methods, and in some cases, performed simultaneous DDoS attacks against targeted networks to facilitate SCADA intrusions. As recently as April 2025, threat actors used the following unsophisticated TTPs to access networks and conduct SCADA intrusions:

- Scan for vulnerable devices on the internet [T0883] with open VNC ports [T1595.002].
- Initiate temporary virtual private server (VPS) [T1583.003] to execute password brute force software.
- Use VNC software to access hosts [T1021.005].
- Confirm connection to the vulnerable device [T0886].
- Brute force the password, if required [T1110.003].
- Gain access to HMI devices [T0883], typically with default [T0812], weak, or no passwords [T0859].

  - Log the confirmed vulnerable device IP address, port, and password.
  - Using the HMI graphical interface [T0823], capture screen recordings or intermittent screenshots while conducting the following actions, intending to affect productivity and cause additional costs [T0828]:
    - Modify usernames/passwords [T0892];
    - Modify parameters [T0836];
    - Modify device name [T0892];
    - Modify instrument settings [T0831];
    - Disable alarms [T0878];
    - Create loss of view (a technique that mandates local hands-on operator intervention) [T0829]; and/or
    - Device restart or shutdown [T0816].
  - Disconnect from the device, ending the VNC connection.
  - Research the compromised device company after the intrusion [T1591].

Propagation

To reach a wider audience, pro-Russia hacktivist groups work together, amplify each other's posts, create additional groups to amplify their own posts, and likely share TTPs. For example, Z-Pentest jointly claimed intrusion of a U.S. system with Sector16. Sector16 later began posting additional intrusions for which the group claimed sole responsibility. It is likely that these and similar groups will continue to iterate and share these methods to disrupt critical infrastructure organizations.

Reconnaissance and Initial Access

The threat actors' intrusion methodology is relatively unsophisticated, inexpensive to execute, and easy to replicate. These pro-Russia hacktivist groups abuse popular internet-scraping tools, such as `Nmap` or `OPENVAS`, to search for visible VNC services and use brute force password spraying tools to access devices via known default or otherwise weak credentials. Threat actors typically search for these services on the default port `5900` or other nearby ports (`5901-5910`). Their goal is to gain remote access to HMI devices connected to live control networks.

Once threat actors obtain access, they manipulate available settings from the graphical user interface (GUI) on the HMI devices, such as arbitrary physical parameter and setpoint changes, or conduct defacement activities. Because pro-Russia hacktivist groups seem to lack sector-specific expertise or cyber-physical engineering knowledge, they currently cannot reliably estimate the true impact of their actions. Regardless of outcome, pro-Russia hacktivist groups often post images and screen recordings to their social media platforms, boasting the compromises and exaggerating impacts to garner attention from their peers and the media.

Impact

While pro-Russia hacktivist groups currently demonstrate limited ability to consistently cause significant impact, there is a risk that their continued attacks will result in further harm or grievous physical consequences. Attacks have not yet caused injury; however, the attacks against occupied factories and community facilities demonstrate a lack of consideration for human safety.

Victim organizations reported that the most common operational impact caused by these threat actors is a temporary loss of view, necessitating manual intervention to manage processes. However, any modifications to programmatic and systematic procedures can result in damage or disruption, including substantial labor costs from hiring a programmable logic controller programmer to restore operations, costs associated with operational downtime, and potential costs for network remediation.

MITRE ATT&CK Tactics and Techniques

See **Table 1** to **Table 10** for all referenced threat actor tactics and techniques in this advisory. For assistance with mapping malicious cyber activity to the MITRE ATT&CK framework, see CISA and MITRE ATT&CK's Best Practices for MITRE ATT&CK Mapping and CISA's Decider Tool.

Table 1. Reconnaissance

Technique Title	ID	Use
Gather Victim Organization Information	T1591	Threat actors use information available on the internet to determine what systems they believe they have compromised and post the information on their social media. This methodology frequently leads to the threat actors misidentifying their claimed victims.
Active Scanning: Vulnerability Scanning	T1595.002	Threat actors use open source tools to look for IP addresses in target countries with visible VNC services on common ports.

Table 2. Resource Development

Technique Title	ID	Use
Acquire Infrastructure: Virtual Private Server	T1583.003	Threat actors use virtual infrastructure to obfuscate identifiers.

Table 3. Initial Access

Technique Title	ID	Use
Internet Accessible Device	T0883	Threat actors gain access through less secure HMI devices exposed to the internet.

Table 4. Persistence

Technique Title	ID	Use
Valid Accounts	T0859	Threat actors use password guessing tools to access legitimate accounts on the HMI devices.

Table 5. Credential Access

Technique Title	ID	Use
Brute Force: Password Spraying	T1110.003	Threat actors use tools to rapidly guess common or simple passwords.

Table 6. Lateral Movement

Technique Title	ID	Use
Default Credentials	T0812	Threat actors seek and build libraries of known default passwords for control devices to access legitimate user accounts.
Remote Services	T0886	Threat actors leverage VNC services to access system HMI devices.
Remote Services: VNC	T1021.005	Threat actors hunt VNC-enabled devices visible on the internet and connect with remote viewer software.

Table 7. Execution

Technique Title	ID	Use
Graphical User Interface	T0823	Threat actors interact with HMI devices via GUIs, attempting to modify control devices.

Table 8. Inhibit Response Function

Technique Title	ID	Use
Device Restart/Shutdown	T0816	While threat actors claim to turn off HMIs, it is possible that operators (not the threat actors) turn the devices off during incident response.
Alarm Suppression	T0878	Threat actors use HMI interfaces to clear alarms caused by their activity and alarms already present on the system at the time of their intrusion.

Technique Title	ID	Use
Change Credential	T0892	Threat actors change the usernames and passwords of HMI devices in operator lockout attempts, usually resulting in a loss of view and operators switching to manual operations.

Table 9. Impair Process Control

Technique Title	ID	Use
Modify Parameter	T0836	Threat actors attempt to change upper and lower limits of operational devices as available from the HMI.
Unauthorized Command Message	T0855	Threat actors attempt to send unauthorized command messages to instruct control system assets to perform actions outside of their intended functionality, causing possible impact.

Table 10. Impact

Technique Title	ID	Use
Loss of Productivity and Revenue	T0828	Threat actors purposefully attempt to impact productivity and create additional costs for the affected entities.
Loss of View	T0829	Threat actors change credentials on HMI devices, preventing operators from modifying processes remotely.
Manipulation of Control	T0831	Threat actors change setpoints in processes, impacting the efficiency of operations for those specific processes.

Incident Response

If organizations find exposed systems with weak or default passwords, they should assume threat actors compromised the system and begin the following incident response protocols:

1. **Determine which hosts were compromised and isolate them** by quarantining or taking them offline.
2. **Initiate threat hunting activities to scope the intrusion.** Collect and review artifacts, such as running processes/services, unusual authentications, and recent network connections.
3. **Reimage compromised hosts.**
4. **Provision new account credentials.**
5. **Report the compromise to CISA, FBI, and/or NSA.** See the **Contact Information** section of this advisory.
6. **Harden the network to prevent additional malicious activity.** See the **Mitigations** section of this advisory for guidance.

Mitigations

OT Asset Owners and Operators

The authoring organizations recommend organizations implement the mitigations below to improve your organization's cybersecurity posture based on the threat actors' activity. These mitigations align with the Cross-Sector Cybersecurity Performance Goals (CPGs) developed by CISA and the National Institute of Standards and Technology (NIST). The CPGs provide a minimum set of practices and protections that CISA and NIST recommend all organizations implement. CISA and NIST based the CPGs on existing cybersecurity frameworks and guidance to protect against the most common and impactful threats, tactics, techniques, and procedures. Visit CISA's CPGs webpage for more information on the CPGs, including additional recommended baseline protections.

- **Reduce exposure of OT assets to the public-facing internet.** When connected to the internet, OT devices are easy targets for malicious cyber threat actors. Many devices can be found by searching for open ports on public IP ranges with search engine tools to target victims with OT components [CPG 3.S].
  - **Asset owners should use attack surface management services** and web-based search platforms to scan the internet. This mitigation can help identify if there are VNC systems exposed within the IP ranges they own, especially for connections set up by third parties. **Note:** For more information on attack surface management, see CISA's Internet Exposure Reduction Guidance, CISA's Cyber Hygiene Services for U.S. critical infrastructure, and NSA's Attack Surface Management for the U.S. Defense Industrial Base.
  - **Implement network segmentation between IT and OT networks.** Segmenting critical systems and introducing a demilitarized zone (DMZ) for passing control data to enterprise logistics reduces the potential impact of cyber threats and the risk of disruptions to essential OT operations [CPG 3.I].
  - **Consider implementing a firewall and/or virtual private network** if exposure to the internet is necessary for controlling access to devices.
    - Consider disabling public exposure by default and implementing time-limited remote access to reduce the amount of time systems are exposed.
    - Restrict and monitor both inbound and outbound traffic at OT perimeter firewalls. Configure OT perimeter firewalls to enforce a default-deny policy for all traffic. Asset owners should explicitly permit authorized destinations and protocols based on operational requirements.
    - Implement strict egress filtering to prevent unauthorized data exfiltration or command-and-control callbacks.
    - Regularly audit firewall rulesets and monitor outbound traffic patterns for anomalies indicative of threat actor activity, such as beaconing or unexpected protocol usage.
- **Adopt mature asset management processes**, including mapping data flows and access points. Generating a complete picture of both OT and IT assets provides visibility to operators and management, allowing organizations to monitor and assess deviations for criticality [CPG 2.A].

  - **Keep remote access services updated** with the latest version available and ensure all systems and software are up to date with patches and necessary security updates.
    - Keep VNC systems updated with the latest version available.
  - **Refer to the joint** [Foundations for OT Cybersecurity: Asset Inventory Guidance for Owners and Operators] to help with reducing cybersecurity risk by identifying which assets within their environment should be secured and protected.
- **Ensure OT assets use robust authentication procedures.**
  - Many devices lack robust authentication and authorization. Devices with weak authentication are vulnerable targets to threat actors using credential theft techniques.
  - Implement MFA where possible. Where MFA is not feasible, use strong, unique passwords. Apply password standards for operator-accessible services on underlying OT assets, as well as network devices protecting those services. This is especially important for services that require internet accessibility [CPG 3.A] [CPG 3.B] [CPG 3.C] [CPG 3.F].
  - Establish an allowlist that permits only authorized device IP addresses and/or media access control addresses. The allowlist can be refined to operator working hours to further obstruct malicious threat actor activity; organizations are encouraged to establish monitoring and alerting for access attempts not meeting these criteria [CPG 3.E].
  - Disable any unused authentication methods, logic, or features, such as default authentication keys and default passwords. Block all unused high ephemeral ports and monitor for attempted connections using standard protocols on non-standard ports [CPG 3.R].
  - Authenticate all access to field controllers before authorizing access to, or modification of, a device's state, logic, program, or filesystems.
- **Enable control system security features** that can separate and audit view and control functions. Limiting remotely accessible or default user accounts to "view-only" removes the potential for impact without exploiting a vulnerability [CPG 3.G].
- **Implement and practice business recovery/disaster recovery plans.** Plans should also take into consideration redundancy, fail-safe mechanisms, islanding capabilities, backup restoration, and manual operation.
  - Include scenarios that necessitate switching to manual operations. Maintaining the capability of an organization to revert to manual controls to quickly restore operations is vital in the immediate aftermath of a cyber incident [CPG 6.A].
  - Create backups of the engineering logic, configurations, and firmware of HMIs to enable fast recovery. Organizations should routinely test backups and standby systems to ensure safe manual operations in the event of an incident [CPG 3.O].
- **Collect and monitor the traffic of OT assets and networking devices.** This includes unusual logins or unexpected protocols communicating over the internet, and functions of ICS management protocols that change an asset's operating mode or modify programs.
- **Review configurations for setpoint ranges or tag values** to stay within safe ranges and establish alerting for deviations.

- **Take a proactive approach in the procurement process** by following the guidance outlined in the joint guide Secure by Demand: Priority Considerations for Operational Technology Owners and Operators when Selecting Digital Products.

OT Device Manufacturers

Although critical infrastructure organizations can take steps to mitigate risks, it is ultimately the responsibility of OT device manufacturers to build products that are secure by design. The authoring organizations urge device manufacturers to take ownership of the security outcomes of their customers in line with the joint guide Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Secure by Design Software.

- **Eliminate default credentials and require strong passwords.** The use of default credentials is a top weakness threat actors exploit to gain access to systems.
- **Mandate MFA for privileged users.** Changes to engineering logic or configurations are safety-impacting events in critical infrastructure. MFA should be available for safety critical components at no additional cost.
- **Practice secure by default principles.** OT components were initially designed without public internet connectivity in mind. When internet connection becomes necessary, implementing additional security measures is essential to safeguard these systems. Manufacturers should recognize insecure states and promptly inform users so they can make informed risk decisions.
    - **Include logging at no additional charge.** Change and access control logs allow operators to track safety-impacting events in their critical infrastructure. These logs should be available for no cost and use open standard logging formats.
- **Publish Software Bill of Materials (SBOMs).** Vulnerabilities in underlying software libraries can affect a wide range of devices. Without an SBOM, it is nearly impossible for a critical infrastructure system owner to measure and mitigate the impact of a vulnerability on their existing systems. See CISA's SBOM webpage for more information.

Additionally, see CISA's Secure by Design Alert on how software manufacturers can shield web management interfaces from malicious cyber activity. By using secure by design tactics, software manufacturers can make their product lines secure "out of the box" without requiring customers to spend additional resources making configuration changes, purchasing tiered security software and logs, monitoring, and making routine updates.

For more information on secure by design, see CISA's Secure by Design webpage.

Validate Security Controls

In addition to applying mitigations, the authoring organizations recommend exercising, testing, and validating your organization's security program against the threat behaviors mapped to the MITRE ATT&CK Matrix for Enterprise framework in this advisory. The authoring organizations recommend testing your existing security controls inventory to assess how it performs against the ATT&CK techniques described in this advisory.

To start:

1. Select an ATT&CK technique described in this advisory (see **Table 1** to **Table 10**).
2. Align your security technologies against the technique.
3. Test your technologies against the technique.
4. Analyze your detection and prevention technologies' performance.
5. Repeat the process for all security technologies to obtain a set of comprehensive performance data.
6. Tune your security program, including people, processes, and technologies, based on the data generated by this process.

The authoring organizations recommend continually testing your security program, at scale, in a production environment to ensure optimal performance against the MITRE ATT&CK techniques identified in this advisory.

Resources

Entities requiring additional support for implementing any of the mitigations in this advisory should contact their regional CISA Cybersecurity Advisor for assistance. Key resources organizations should reference include:

- CISA, EPA, NSA, FBI, ASD's ACSC, Cyber Centre, BSI, NCSC-NL, and NCSC-NZ's Foundations for OT Cybersecurity: Asset Inventory Guidance for Owners and Operators offers best practices to assist organizations in identifying and prioritizing which assets should be secured and protected.
- CISA, FBI, NSA, EPA, DOE, USDA, FDA, MS-ISAC, Cyber Centre, and NCSC-UK's guidance on Defending OT Operations Against Ongoing Pro-Russia Hacktivist Activity that can help organizations protect OT systems from pro-Russia hacktivist activity.
- NSA and CISA's guidance on Control System Defense: Know the Opponent helps organizations defend OT and ICS assets against malicious cyber activity.
- CISA and EPA's resource page on Water and Wastewater Cybersecurity to help organizations reduce risks posed by malicious cyber actors targeting water and wastewater systems.
  - For additional guidance, see CISA, EPA, and FBI's fact sheet on Top Cyber Actions for Securing Water Systems.
- The Food and Ag-ISAC's best practices on Food and Ag Cybersecurity: A Guide for Small & Medium Enterprises provides recommendations to help mitigate against cyber threats.
- DOE and National Association of Regulatory Utility Commissioners Cybersecurity Baselines for Electric Distribution Systems and Distributed Energy (DER) webpage provides resources for state public utility commissions and utilities, as well as DER operators and aggregators to help mitigate cybersecurity risks.

Additional resources that apply to this advisory include:

- EPA's Cybersecurity for the Water Sector resource page provides organizations with guidance on implementing basic cyber hygiene practices.

- CISA's Cross-Sector Cybersecurity Performance Goals enables critical infrastructure organizations to reduce the likelihood and impact of known risks and adversary techniques.
- CISA's Require Strong Passwords webpage supports small and medium-sized businesses mitigating against malicious cyber activity that targets weak passwords.
- CISA, NSA, FBI, EPA, TSA, and international partners' guidance Secure by Demand: Priority Considerations for Operational Technology Owners and Operators when Selecting Digital Products.
- DOE's guidance on Cyber-Informed Engineering recommends considering cyber-enabled risks during the conception, design, and development phases when manufacturing physical systems.
- CISA's Cyber Hygiene Services help enable critical infrastructure organizations to reduce their exposure to threats by taking a proactive approach to monitoring and mitigating attack vectors.
- CISA, NSA, FBI, and international partners' guidance on Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Secure by Design Software urges software manufacturers to provide customers with products that are safer and more secure.
    - See more information in these Secure by Design Alerts: How Manufacturers Can Protect Customers by Eliminating Default Passwords and How Software Manufacturers Can Shield Web Management Interfaces From Malicious Cyber Activity.

Contact Information

U.S. organizations are encouraged to report suspicious or criminal activity related to information in this advisory to CISA, FBI, and/or NSA:

- Contact CISA via CISA's 24/7 Operations Center at contact@cisa.dhs.gov or 1-844-Say-CISA (1-844-729-2472) or your local FBI field office. When available, please include the following information regarding the incident: date, time, and location of the incident; type of activity; number of people affected; type of equipment used for the activity; the name of the submitting company or organization; and a designated point of contact.
- For NSA cybersecurity guidance inquiries, contact CybersecurityReports@nsa.gov.

Australian organizations: Visit cyber.gov.au or call 1300 292 371 (1300 CYBER 1) to report cybersecurity incidents and access alerts and advisories.

Canadian organizations: Report incidents by emailing Cyber Centre at contact@cyber.gc.ca.

New Zealand organizations: Report cyber security incidents to incidents@ncsc.govt.nz or call 04 498 7654.

United Kingdom organizations: Report a significant cyber security incident: report.ncsc.gov.uk (monitored 24 hours) or, for urgent assistance, call 03000 200 973.

Disclaimer

The information in this report is being provided "as is" for informational purposes only. The authoring organizations do not endorse any commercial entity, product, company, or service, including any entities, products, or services linked within this document. Any reference to specific commercial entities, products, processes, or services by service mark, trademark, manufacturer, or otherwise, does not constitute or imply endorsement, recommendation, or favoring by FBI and co-sealers.

Acknowledgements

Schneider Electric, Nozomi Networks, Eversource Energy, Electricity Information Sharing and Analysis Center, Chevron, BP, and Dragos contributed to this advisory.

Version History

December 09, 2025: Initial version.

Appendix A: Targeting Methodologies for Pro-Russia Hacktivist Groups

For further information on targeting methodologies for pro-Russia hacktivist groups, see:

- CISA's alert Unsophisticated Cyber Threat Actor(s) Targeting Operational Technology;
- The joint fact sheet Primary Mitigations to Reduce Cyber Threats to Operational Technology; and
- CISA's Russia Cyber Threat webpage.

Appendix B: Additional Designators Used for Cited Groups

The cybersecurity industry and cyber actor groups often use various names to reference actor groups. While not exhaustive, the following are the most notable names used within the cybersecurity community to reference the groups in this advisory.

Note: Cybersecurity organizations have different methods of tracking and attributing cyber actors, and this may not be a 1:1 correlation to the authoring organizations' understanding for all activity related to these groupings.

- GRU military unit 74455
  - Sandworm Team
  - Voodoo Bear
  - Seashell Blizzard
  - APT44
- Cyber Army of Russia Reborn (CARR)
  - CyberArmy of Russia
  - Народная CyberАрмия (НКА)
  - People's CyberArmy of Russia (PCA)
  - Russian CyberArmy Team (RCAT)
- NoName057(16)
  - NoName057(16) Spain
  - NoName057(16) Italy
  - NoName057(16) France
- Z-Pentest
  - Z-Pentest Beograd
  - Z-Pentest Alliance
  - Z-Alliance