CYBERSECURITY ADVISORY

Pro-Russia Hacktivists Conduct Opportunistic Attacks Against Critical Infrastructure

Executive Summary

This advisory addresses an escalating threat from pro-Russia hacktivist groups conducting unsophisticated but impactful attacks against critical infrastructure entities in the United States and globally. Key findings indicate:

- **Threat Actors:** Cyber Army of Russia Reborn (CARR), NoName057(16), Z-Pentest, Sector16, and affiliated groups
- **Attack Method:** Exploitation of internet-accessible Virtual Network Computing (VNC) connections using weak or default credentials
- **Impact:** Physical damage to operational technology (OT) assets and critical infrastructure systems
- **Targeted Sectors:** Water and Wastewater Systems, Ports, Food and Agriculture, and Energy, Telecommunication, Aviation
- **Geographic Scope:** United States and global critical infrastructure

Despite limited technical sophistication, these groups have demonstrated a willingness to cause actual harm to vulnerable infrastructure while often making false or exaggerated claims about their capabilities.

Threat Overview

Threat Actor Profiles

Cyber Army of Russia Reborn (CARR)

CARR was likely established by Russia's General Staff Main Intelligence Directorate (GRU) military unit 74455 in February-March 2022. The group:

Head Office: Level 34, 1 Eagle Street (Waterfront Place), Brisbane, QLD 4000, Australia **ABN:** 33 601 684 119 **P:** +61 7 3184 9114 **Int P:** 1300 292 376
Branch Office: Level 2 / 4 318 Lambton Quay Wellington 6011, New Zealand **P:** +64 4333 0395

- Initially focused on DDoS attacks against U.S. and European targets
- Expanded operations in late 2023 to include attacks on Industrial Control Systems (ICS)
- Claimed intrusions against European wastewater treatment facilities and U.S. dairy farms
- Became dissatisfied with GRU support levels by September 2024, leading to creation of Z-Pentest

NoName057(16)

Established as a covert project under the Kremlin-affiliated Center for the Study and Network Monitoring of the Youth Environment (CISM), NoName057(16) has:

- Been active since March 2022
- Conducted frequent DDoS attacks against NATO member states and allied nations
- Developed the proprietary DDoS tool "DDoSia"
- Begun collaborating closely with CARR in 2024
- Jointly targeted U.S. OT assets with CARR in July 2024

Z-Pentest

Formed in September 2024 from members of CARR and NoName057(16), Z-Pentest:

- Specializes in OT intrusion operations against globally dispersed critical infrastructure
- Avoids DDoS activities, focusing instead on intrusions and "hack and leak" operations
- Claims OT intrusions to gain media attention
- Has formed alliances with Sector16 and other emerging groups
- Continues to propagate TTPs to new partner organizations

Sector16

This novice pro-Russia hacktivist group:

- Emerged in January 2025 through collaboration with Z-Pentest
- Maintains active public Telegram presence

Head Office: Level 34, 1 Eagle Street (Waterfront Place), Brisbane, QLD 4000, Australia **ABN:** 33 601 684 119 **P:** +61 7 3184 9114 **Int P:** 1300 292 376
Branch Office: Level 2 / 4 318 Lambton Quay Wellington 6011, New Zealand **P:** +64 4333 0395

- Shares videos and statements claiming compromise of U.S. energy infrastructure
- May receive indirect support from the Russian government for cyber operations
- Reflects broader Russian strategies leveraging non-state actors for deniability

Technical Analysis

Attack Methodology

Pro-Russia hacktivist groups employ highly replicable, low-cost TTPs that exploit fundamental security weaknesses:

a. Reconnaissance and Initial Access

1. **Internet Scanning:** Attackers use open-source tools (Nmap, OPENVAS) to search for exposed VNC services on default port 5900 or nearby ports (5901-5910)
2. **Vulnerability Identification:** They identify targets based on availability rather than strategic significance
3. **VNC Connection Exploitation:** Target internet-facing Human-Machine Interface (HMI) devices lacking adequate access controls
4. **Credential Attacks:** Employ brute force password spraying against weak or default credentials

b. Compromise and Exploitation

Once access is obtained, attackers:

1. Establish temporary Virtual Private Servers (VPS) for executing password brute force software
2. Connect to HMI devices using VNC software
3. Confirm connections and authenticate (often with default credentials)
4. Log compromised device IP address, port, and password
5. Access HMI graphical interfaces to capture evidence

c. Impact Activities

Attackers manipulate HMI settings to cause operational disruption:

Head Office: Level 34, 1 Eagle Street (Waterfront Place), Brisbane, QLD 4000, Australia ABN: 33 601 684 119 P: +61 7 3184 9114 Int P: 1300 292 376
Branch Office: Level 2 / 4 318 Lambton Quay Wellington 6011, New Zealand P: +64 4333 0395

- Modify usernames and passwords (causing operator lockout)
- Change operational parameters and setpoints
- Modify device names and instrument settings
- Disable alarms on affected systems
- Create "loss of view" conditions (forcing manual intervention)
- Restart or shutdown devices
- Capture screenshots/video evidence for social media posting

d. Lack of Technical Sophistication

A critical characteristic of these threat actors:

- **Limited Engineering Knowledge:** Actors frequently lack sector-specific expertise or cyber-physical engineering knowledge
- **Unpredictable Impact:** Cannot reliably estimate true consequences of their actions
- **False Claims:** Regularly make exaggerated or false claims about attack impacts to garner media attention
- **Opportunistic Targeting:** Focus on easily accessible targets rather than strategically significant assets
- **Misidentification:** Often misidentify their claimed victims based on superficial internet searches

Operational Impact Assessment

a. Actual Consequences

While direct injury has not yet occurred, reported impacts include:

- **Temporary Loss of View:** Most common operational impact, requiring manual operator intervention
- **Physical Damage:** Documented damage to critical infrastructure systems
- **Operational Downtime:** Extended periods requiring system restoration

Head Office: Level 34, 1 Eagle Street (Waterfront Place), Brisbane, QLD 4000, Australia **ABN:** 33 601 684 119 **P:** +61 7 3184 9114 **Int P:** 1300 292 376
Branch Office: Level 2 / 4 318 Lambton Quay Wellington 6011, New Zealand **P:** +64 4333 0395

- **Financial Costs:** Significant labor costs from hiring specialized programmers (PLC programmers) to restore operations; remediation costs; downtime-related revenue loss
- **Safety Risk:** Attacks demonstrate lack of consideration for human safety, particularly against occupied facilities and community infrastructure

b. Risk Assessment

Although current technical capabilities are limited, continuing attacks pose escalating risks:

- Increased frequency of intrusions through easily replicated TTPs
- Potential for grievous physical consequences as attacks continue
- Broad applicability across critical infrastructure sectors
- Rapid dissemination of methods among affiliated groups

MITRE ATT&CK Framework Mapping

The following table maps MITRE ATT&CK Techniques Used by Pro-Russia Hacktivist Groups to establish cybersecurity frameworks:

Tactic/Technique	MITRE ATT&CK ID
Gather Victim Organization Information	T1591
Active Scanning: Vulnerability Scanning	T1595.002
Acquire Infrastructure: Virtual Private Server	T1583.003
Internet Accessible Device	T0883
Valid Accounts	T0859
Brute Force: Password Spraying	T1110.003
Default Credentials	T0812
Remote Services	T0886
Remote Services: VNC	T1021.005
Graphical User Interface	T0823

Head Office: Level 34, 1 Eagle Street (Waterfront Place), Brisbane, QLD 4000, Australia **ABN:** 33 601 684 119 **P:** +61 7 3184 9114 **Int P:** 1300 292 376
Branch Office: Level 2 / 4 318 Lambton Quay Wellington 6011, New Zealand **P:** +64 4333 0395

Device Restart/Shutdown	T0816
Alarm Suppression	T0878
Change Credential	T0892
Modify Parameter	T0836
Loss of Productivity and Revenue	T0828
Loss of View	T0829
Manipulation of Control	T0831

Recommended Incident Response Procedures

If your organization discovers exposed systems with weak or default passwords, implement the following incident response protocols immediately:

1. **System Isolation:** Determine which hosts were compromised and immediately quarantine or take them offline
2. **Threat Hunting:** Initiate comprehensive threat hunting activities to scope the intrusion extent
    - Collect and review running processes/services
    - Analyze unusual authentications and suspicious user activities
    - Review recent network connections
3. **System Remediation:** Reimage all compromised hosts with clean system images
4. **Credential Rotation:** Provision entirely new account credentials across affected systems
5. **Formal Reporting:** Report the compromise to CISA, FBI, and/or NSA (contact information provided below)
6. **Network Hardening:** Implement defensive measures outlined in the Mitigation Strategies section

Head Office: Level 34, 1 Eagle Street (Waterfront Place), Brisbane, QLD 4000, Australia **ABN:** 33 601 684 119 **P:** +61 7 3184 9114 **Int P:** 1300 292 376
Branch Office: Level 2 / 4 318 Lambton Quay Wellington 6011, New Zealand **P:** +64 4333 0395

Critical Mitigation Strategies

For Operational Technology Asset Owners and Operators

a. Priority 1: Reduce Internet Exposure

- **Scan for Exposure:** Use attack surface management services and web-based search platforms to identify exposed VNC systems within your IP ranges
- **Network Segmentation:** Implement network segmentation between IT and OT networks; establish demilitarized zones (DMZs) for control data passage
- **Access Controls:** If internet exposure is necessary:
  - Implement firewalls and/or virtual private networks (VPNs)
  - Disable public exposure by default
  - Implement time-limited remote access to minimize exposure duration
- **Firewall Configuration:**
  - Enforce default-deny policy for all traffic
  - Explicitly permit only authorized destinations and protocols
  - Implement strict egress filtering to prevent unauthorized exfiltration
  - Monitor outbound traffic patterns for anomalies (beaconing, unexpected protocols)

b. Priority 2: Implement Robust Asset Management

- **Comprehensive Asset Inventory:** Maintain complete mapping of OT and IT assets, data flows, and access points
- **Software Updates:** Keep all systems, software, and remote access services (particularly VNC systems) updated with latest versions and patches
- **Refer to Guidance:** Consult "Foundations for OT Cybersecurity: Asset Inventory Guidance for Owners and Operators" for asset identification best practices

c. Priority 3: Enforce Strong Authentication

- **Multi-Factor Authentication (MFA):** Implement MFA where technically feasible
- **Strong Password Requirements:** Where MFA is not feasible, implement:
  - Strong, unique passwords across all systems

Head Office: Level 34, 1 Eagle Street (Waterfront Place), Brisbane, QLD 4000, Australia **ABN:** 33 601 684 119 **P:** +61 7 3184 9114 **Int P:** 1300 292 376
Branch Office: Level 2 / 4 318 Lambton Quay Wellington 6011, New Zealand **P:** +64 4333 0395

- Password standards for operator-accessible services
- Elimination of default credentials and authentication keys
- Blocking of unused high ephemeral ports

- **Access Controls:**
  - Establish allowlists permitting only authorized device IP addresses/MAC addresses
  - Restrict allowlists to operator working hours where possible
  - Monitor and alert on access attempts outside these parameters
  - Authenticate all access to field controllers before authorizing state/logic/program modifications

d. Priority 4: Implement Protective Controls

- **Control Function Separation:** Enable control system security features separating and auditing view and control functions
  - Limit remotely accessible or default accounts to "view-only" mode
  - Remove potential for malicious impact without requiring vulnerability exploitation
- **Business Continuity Planning:**
  - Develop comprehensive recovery/disaster recovery plans including manual operation scenarios
  - Implement redundancy, fail-safe mechanisms, and islanding capabilities
  - Create backups of engineering logic, configurations, and firmware
  - Routinely test backups and standby systems to ensure safe manual operation capability
- **Monitoring and Detection:**
  - Collect and monitor traffic from OT assets and networking devices
  - Track unusual logins, unexpected protocols communicating over internet
  - Monitor ICS management protocol changes affecting asset operating mode or program modifications
  - Review setpoint configurations for safe operational ranges
  - Establish alerting for deviations from safe operating parameters

e. Priority 5: Procurement Strategy

- **Secure by Demand Approach:** Apply guidance from "Secure by Demand: Priority Considerations for Operational Technology Owners and Operators when Selecting Digital Products"
- **Vendor Requirements:** Request that OT device manufacturers implement secure-by-design principles

For Operational Technology Device Manufacturers

Manufacturers must prioritize security in product design to reduce customer vulnerability:

a. Eliminate Default Credentials

- Remove all pre-configured default passwords
- This is a critical weakness exploited by attackers to gain initial access

b. Mandate Multi-Factor Authentication

- Implement MFA for privileged users as baseline functionality
- Make MFA available for safety-critical components at no additional cost
- Recognize that engineering logic and configuration changes are safety-impacting events

c. Implement Secure by Default Principles

- Acknowledge that OT components may require internet connectivity despite original design assumptions
- Implement additional security measures as default configurations
- Inform users of insecure states to enable informed risk decision-making

d. Provide Comprehensive Logging

- Include change and access control logging at no additional charge
- Enable tracking of safety-impacting events in critical infrastructure
- Use open standard logging formats

e. Publish Software Bill of Materials (SBOM)

- Publicly document all underlying software libraries and dependencies

Head Office: Level 34, 1 Eagle Street (Waterfront Place), Brisbane, QLD 4000, Australia **ABN:** 33 601 684 119 **P:** +61 7 3184 9114 **Int P:** 1300 292 376
Branch Office: Level 2 / 4 318 Lambton Quay Wellington 6011, New Zealand **P:** +64 4333 0395

- Enable critical infrastructure owners to measure and mitigate vulnerability impacts
- Consult CISA's SBOM webpage for implementation guidance

Incident Response Contact Information

United States Organizations

- **Australia:** cyber.gov.au or 1300 292 371
- **Canada:** Cyber Centre at contact@cyber.gc.ca
- **New Zealand:** incidents@ncsc.govt.nz or 04 498 7654
- **United Kingdom:** report.ncsc.gov.uk (24-hour monitoring) or 03000 200 973 (urgent)
- **CISA:** contact@cisa.dhs.gov or 1-844-SAY-CISA (1-844-729-2472)
- **Local FBI Field Office:** Contact your regional office
- **NSA Cyber Security:** CybersecurityReports@nsa.gov

Include the following information when reporting:

- Date, time, and location of incident
- Type of attack/activity
- Number of people affected
- Equipment used for attack
- Organization name
- Designated point of contact

Recommendations for Your Organization

Immediate Actions (Next 30 Days)

1. **Conduct VNC Exposure Audit:** Use attack surface management tools to identify exposed VNC systems in your IP ranges

Head Office: Level 34, 1 Eagle Street (Waterfront Place), Brisbane, QLD 4000, Australia **ABN:** 33 601 684 119 **P:** +61 7 3184 9114 **Int P:** 1300 292 376
Branch Office: Level 2 / 4 318 Lambton Quay Wellington 6011, New Zealand **P:** +64 4333 0395

2. **Change Default Credentials:** Immediately change all default passwords on OT assets
3. **Enable Logging:** Activate change and access control logging across all critical systems
4. **Document Baseline:** Establish baselines for normal operational parameters and setpoints

Short-Term Actions (30-90 Days)

1. **Implement Network Segmentation:** Separate IT and OT networks with firewalls and DMZs
2. **Deploy MFA:** Implement multi-factor authentication on critical systems
3. **Inventory Assets:** Complete comprehensive mapping of OT assets and data flows
4. **Test Incident Response:** Exercise incident response procedures against the documented TTPs

Long-Term Actions (90+ Days)

1. **Vendor Assessment:** Evaluate OT device manufacturers' security posture and capabilities
2. **Business Continuity:** Develop and regularly test recovery procedures including manual operations
3. **Continuous Monitoring:** Implement 24/7 monitoring for suspicious activities
4. **Workforce Training:** Conduct regular security awareness training for operations staff

Conclusion

Pro-Russia hacktivist groups represent a persistent but opportunistic threat to critical infrastructure globally. While individual actors lack sophisticated technical capabilities, their easy-to-replicate TTPs and willingness to cause actual harm create substantial risk. The widespread prevalence of internet-accessible VNC connections with weak credentials provides abundant attack surface.

Organizations must immediately prioritize:

1. Eliminating exposed OT assets from the public internet
2. Eliminating weak and default credentials
3. Implementing network segmentation and access controls

Head Office: Level 34, 1 Eagle Street (Waterfront Place), Brisbane, QLD 4000, Australia **ABN:** 33 601 684 119 **P:** +61 7 3184 9114 **Int P:** 1300 292 376
Branch Office: Level 2 / 4 318 Lambton Quay Wellington 6011, New Zealand **P:** +64 4333 0395

4. Establishing comprehensive monitoring and logging

OT device manufacturers must shift responsibility toward secure-by-design principles, eliminating default credentials and implementing mandatory security controls at baseline.

By implementing these recommendations, organizations can significantly reduce their likelihood of victimization by these threat actors while improving overall cybersecurity posture against broader threats.

Head Office: Level 34, 1 Eagle Street (Waterfront Place), Brisbane, QLD 4000, Australia **ABN:** 33 601 684 119 **P:** +61 7 3184 9114 **Int P:** 1300 292 376
Branch Office: Level 2 / 4 318 Lambton Quay Wellington 6011, New Zealand **P:** +64 4333 0395