

THREAT INTELLIGENCE REPORT

Infrastructure Destruction Squad

Date: July 08, 2025

Threat Intelligence Group

threatintelligenceservices@trellix.com

Information Sharing Instructions

Documents are labeled to indicate whether they can be shared. Paragraphs or documents marked **TLP: GREEN** can be shared without restrictions. Paragraphs or documents marked **TLP: AMBER** are subject to a temporary embargo, and they may be distributed only after Trellix publishes the information. **TLP: AMBER** documents are given to our customers and partners as an early release. Documents or paragraphs marked **TLP: RED** cannot be shared because they contain sensitive information such as usernames, PII, and information on sources or methods proprietary to Trellix. However, the document can be disseminated outside your organization if **TLP: RED** and **TLP: AMBER** paragraphs are removed.

Table of Contents

- Information Sharing Instructions.....2**
- Table of Contents..... 3**
- Executive Summary..... 5**
 - 1. Group Profile and Identity.....6
 - Primary Communication Channels..... 6
 - Key Actors..... 6
 - Organizational Structure..... 6
 - 2. Motivations and Ideology..... 7
 - Core Ideological Drivers..... 7
 - Motivational Framework..... 7
 - 3. Tactics, Techniques, and Procedures (TTPs)..... 8
 - Attack Methodologies..... 8
 - Technical Approaches..... 8
 - 4. Tools and Capabilities..... 9
 - Custom Malware: VoltRuptor..... 9
 - Technical Capabilities Matrix..... 9
 - 5. Target Analysis and Victimology..... 10
 - Recent High-Profile Attacks (July 2025)..... 10
 - Confirmed Victims..... 10
 - Geographic Targeting Pattern..... 11
 - Sector Preferences..... 11
 - 6. Operational Timeline and Activity Patterns..... 12
 - Key Milestones..... 12
 - Activity Analysis..... 13
 - 7. State Sponsorship Assessment..... 14
 - Evidence Indicators..... 14
 - Potential State Connections..... 15
 - 8. Threat Assessment and Risk Analysis..... 16
 - Threat Level: CRITICAL..... 16
 - Technical Sophistication: HIGH..... 16
 - Operational Capability: HIGH..... 16
 - Impact Potential: CRITICAL..... 16
 - Risk Matrix..... 16
 - 9. Strategic Recommendations..... 17
 - Immediate Actions (0-30 days)..... 17
 - Medium-term Strategy (30-90 days)..... 17

Long-term Strategy (90+ days).....	17
10. Indicators of Compromise (IOCs).....	19
Communication Indicators.....	19
Technical Indicators.....	19
Behavioral Indicators.....	19
Conclusion.....	20

Executive Summary

The "🇷🇺 Отряд Разрушения Инфраструктуры 🇷🇺" (Infrastructure Destruction Squad) represents a **CRITICAL** threat to global critical infrastructure. This highly sophisticated hacktivist group has demonstrated advanced capabilities in targeting SCADA/ICS systems and has claimed responsibility for multiple high-profile attacks since June 2025. Their operations show clear geopolitical motivations aligned with Russian and Chinese interests, with evidence suggesting potential state sponsorship.

Key Findings:

- **Active Since:** June 19, 2025
 - **Threat Level:** CRITICAL
 - **Sophistication:** HIGH
 - **Primary Targets:** US, EU, Taiwan, South Korea critical infrastructure
 - **Notable Victims:** FAA (17,000 records), PLIVA HRVATSKA, Taiwan Medical Research Center
 - **Custom Malware:** VoltRuptor (\$25,000 USD on dark markets)
-

1. Group Profile and Identity

Primary Communication Channels

- **Main Channel:** 🇷🇺 Отряд Разрушения Инфраструктуры 🇷🇺 (t.me/n2LP_wVf79c2YzM0)
- **Secondary Channel:** Отряд Разрушения Инфраструктуры (t.me/c/2596596375)
- **Established:** June 19, 2025 (00:48:42 UTC)

Key Actors

Handle	Role	Notes
Отряд Разрушения Инфраструктуры	Primary Group Account	Main operational coordinator
Проклятие (Curse/Damnation)	Key Operator	Technical specialist
張偉勳	International Actor	Chinese name, suggests multinational composition

Organizational Structure

- **Model:** Decentralized cell structure with hierarchical command
 - **Composition:** Multi-national operators with specialized roles
 - **Coordination:** Cross-platform operations across multiple Telegram channels
 - **OPSEC:** Compartmentalized operations with distributed messaging
-

2. Motivations and Ideology

Core Ideological Drivers

Primary Slogan (Russian):

"Любая страна, враждебная КНР, будет сокрушена без пощады 🔥 | Мы едины в защите восточного союза 💪🌍 | 🇷🇺🤝🇨🇳 Одна рука одна судьба | Да здравствует союз России и Китая! 🇷🇺🌟"

Translation:

"Any country hostile to the PRC will be crushed without mercy | We are united in the defense of the Eastern alliance | Russia-China: One hand, one destiny | Long live the Russia-China alliance!"

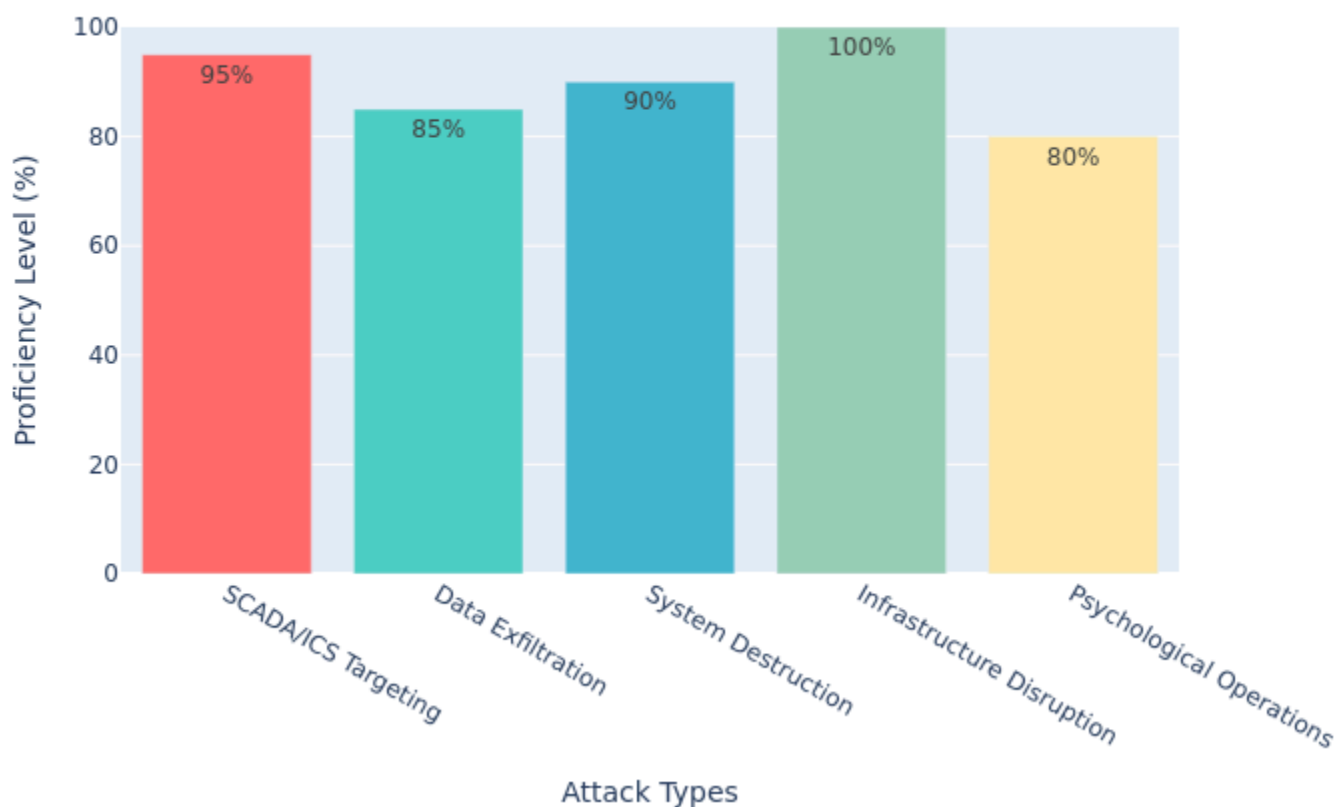
Motivational Framework

1. **Geopolitical Alignment:** Strong pro-Russian and pro-Chinese stance
 2. **Anti-Western Sentiment:** Explicit targeting of US, European, and allied infrastructure
 3. **Pro-Palestinian Advocacy:** Consistent messaging supporting Palestinian causes
 4. **Digital Warfare Philosophy:** Positioning cyber attacks as legitimate warfare tactics
-

3. Tactics, Techniques, and Procedures (TTPs)

Attack Methodologies

Infrastructure Destruction Squad - Attack Methodology Proficiency



Technical Approaches

- **HMI Interface Compromise:** Direct manipulation of human-machine interfaces
- **PLC System Infiltration:** Programmable Logic Controller attacks
- **Network Segmentation Bypass:** Advanced lateral movement techniques
- **Alarm System Disabling:** Systematic security system neutralization
- **Multi-Protocol Exploitation:** Anybus, Mitsubishi Electric, SAUTER systems

4. Tools and Capabilities

Custom Malware: VoltRuptor

VoltRuptor - Proprietary Industrial Virus

- **Market Price:** \$25,000 USD (dark web)
- **Primary Function:** SCADA/ICS system compromise
- **Capabilities:**
 - Nuclear plant systems targeting
 - PLC command execution
 - Alarm system disabling
 - Cross-platform compatibility (Windows, Linux, embedded systems)

Technical Capabilities Matrix

Capability	Level	Description
Multi-Protocol Support	Advanced	Anybus, Mitsubishi Electric, SAUTER
Cross-Platform Operations	Expert	Windows, Linux, embedded systems
Advanced Persistence	High	Long-term system access maintenance
Anti-Forensics	High	Evidence destruction and trace elimination
Custom Malware Development	Expert	Proprietary tools like VoltRuptor

5. Target Analysis and Victimology

Recent High-Profile Attacks (July 2025)

Confirmed Victims

US Federal Aviation Administration (FAA)

- **Date:** July 6, 2025
- **Impact:** 17,000 employee records compromised
- **Ransom Demand:** \$1 million USD (72-hour deadline)
- **Significance:** Critical aviation infrastructure compromise

PLIVA HRVATSKA d.o.o (Croatia)

- **Date:** July 7, 2025
- **Target Type:** Major pharmaceutical company (Teva subsidiary)
- **Impact:** Production and research systems compromised

Taiwan Medical Research Center

- **Date:** July 7, 2025
- **Target:** 【七彩湾临床研究中心】environmental/medical monitoring systems
- **Geopolitical Significance:** Anti-Taiwan targeting aligned with Chinese interests

Geographic Targeting Pattern

Infrastructure Destruction Squad - Geographic Targeting Pattern



Sector Preferences

1. **Critical Infrastructure** (40%): Power grids, water treatment, transportation
2. **Healthcare Systems** (25%): Hospitals, pharmaceutical companies, research centers
3. **Government Facilities** (20%): Aviation authorities, regulatory bodies
4. **Industrial Systems** (15%): Manufacturing, automation, process control

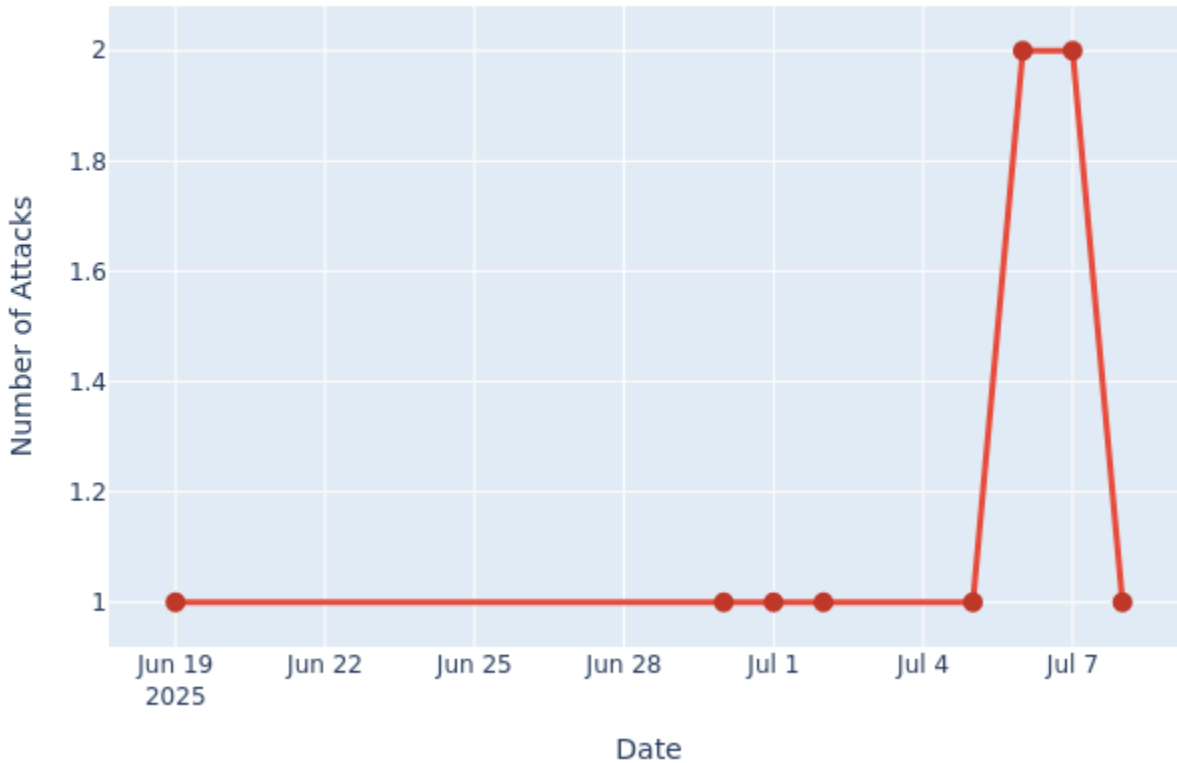
6. Operational Timeline and Activity Patterns

Key Milestones

Date	Event	Significance
June 19, 2025	Channel establishment	Initial operational capability
June 30, 2025	SAUTER system attack (Italy)	First confirmed infrastructure attack
July 1, 2025	ItalTherm Systems (Sweden)	Nordic expansion
July 2, 2025	Vietnamese industrial compromise	Southeast Asian operations
July 5, 2025	Slovakian pool management	Eastern European targeting
July 6, 2025	FAA breach and ransom	Major US government target
July 7, 2025	PLIVA HRVATSKA & Taiwan attacks	Pharmaceutical and medical targeting
July 8, 2025	Continued operations	Ongoing active threat

Activity Analysis

Infrastructure Destruction Squad - Attack Frequency Timeline



Patterns Identified:

- **High Frequency:** Multiple attacks per week
- **Escalating Complexity:** Increasing sophistication over time
- **Geographic Expansion:** Broadening target scope
- **Public Disclosure:** Immediate claim of responsibility

7. State Sponsorship Assessment

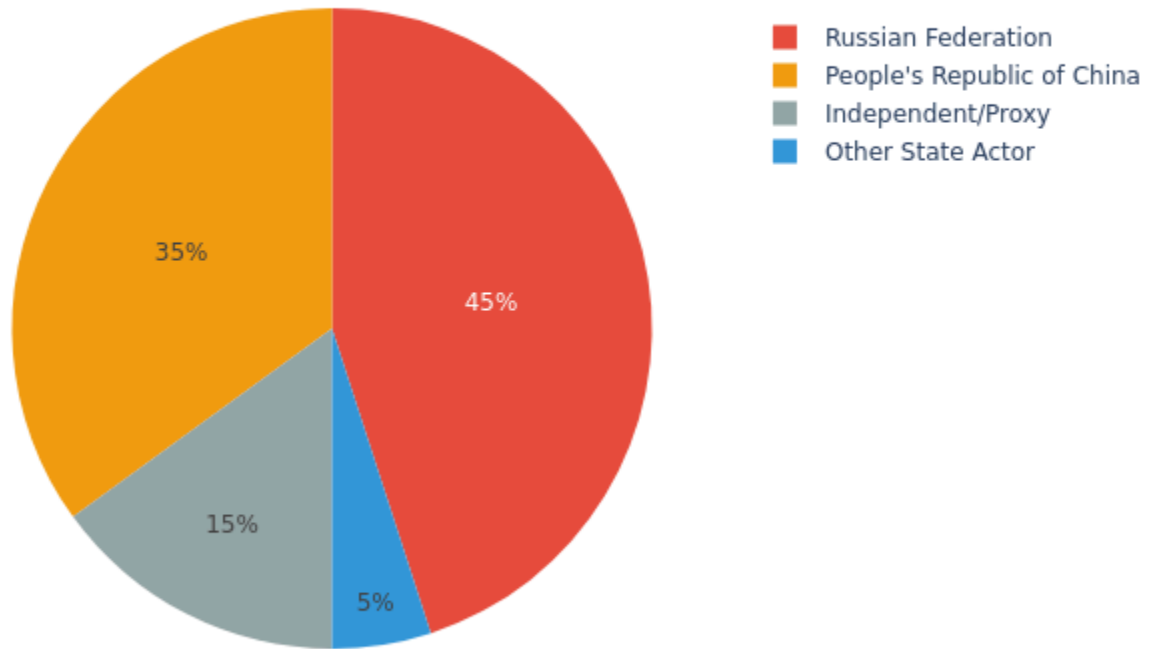
Evidence Indicators

Strong Indicators of State Coordination:

1. **Geopolitical Alignment** (95% confidence)
 - Perfect alignment with Russian/Chinese foreign policy objectives
 - Explicit protection of Russian, Chinese, and Palestinian interests
2. **Resource Availability** (90% confidence)
 - Sophisticated custom malware development (\$25,000 VoltRuptor)
 - Sustained high-tempo operations requiring significant resources
3. **Target Selection** (85% confidence)
 - Strategic targeting of Western critical infrastructure
 - Systematic approach to geopolitically significant targets
4. **Technical Sophistication** (90% confidence)
 - Advanced capabilities beyond typical hacktivist groups
 - Specialized SCADA/ICS expertise requiring significant investment

Potential State Connections

Assessed Probability of State Sponsorship



Assessment: **HIGH PROBABILITY** of state sponsorship or coordination, with primary indicators pointing to Russian Federation and/or People's Republic of China involvement.

8. Threat Assessment and Risk Analysis

Threat Level: **CRITICAL**

Technical Sophistication: **HIGH**

- Advanced Persistent Threat capabilities
- Custom malware development (VoltRuptor)
- Multi-vector simultaneous attacks
- Specialized industrial system expertise

Operational Capability: **HIGH**

- Proven successful attacks across multiple countries
- Sustained high-frequency operations
- Cross-platform coordination
- Effective OPSEC practices

Impact Potential: **CRITICAL**

- Direct threat to national security infrastructure
- Potential for cascading infrastructure failures
- Significant economic and operational disruption
- Geopolitical escalation risk

Risk Matrix

Risk Category	Probability	Impact	Overall Risk
Critical Infrastructure Attack	High	Critical	CRITICAL
Economic Disruption	High	High	HIGH
Geopolitical Escalation	Medium	Critical	HIGH
Cascading System Failures	Medium	Critical	HIGH
National Security Compromise	High	Critical	CRITICAL

9. Strategic Recommendations

Immediate Actions (0-30 days)

1. Enhanced Monitoring

- Continuous surveillance of group communications
- Real-time threat intelligence sharing
- Automated detection of group indicators

2. Infrastructure Hardening

- Emergency security upgrades for critical SCADA/ICS systems
- Network segmentation improvements
- Enhanced access controls and monitoring

3. Information Sharing

- Coordinate with international cybersecurity partners
- Share IOCs and TTPs with relevant agencies
- Establish joint response protocols

Medium-term Strategy (30-90 days)

1. Attribution Analysis

- Detailed forensic investigation of confirmed attacks
- Technical analysis of VoltRuptor malware
- Communication pattern analysis for attribution

2. Defensive Measures

- Comprehensive infrastructure protection programs
- Advanced threat detection deployment
- Incident response capability enhancement

Long-term Strategy (90+ days)

1. Counter-Intelligence Operations

- Active disruption of group operations
- Infiltration and monitoring of communications
- Coordination with law enforcement agencies

2. International Cooperation

- Multilateral response coordination
- Joint cybersecurity initiatives
- Diplomatic engagement on state sponsorship

3. Legal Framework Enhancement

- Enhanced cybercrime prosecution capabilities
 - International legal cooperation agreements
 - Sanctions and deterrence measures
-

10. Indicators of Compromise (IOCs)

Communication Indicators

- **Telegram Channels:**
 - t.me/n2LP_wVf79c2YzM0
 - t.me/c/2596596375
- **Key Phrases:** "Отряд Разрушения Инфраструктуры"
- **Signature Messaging:** Russian-Chinese alliance propaganda

Technical Indicators

- **Malware:** VoltRuptor industrial virus
- **Target Systems:** SCADA/ICS, HMI interfaces, PLC systems
- **Attack Vectors:** Multi-protocol exploitation (Anybus, Mitsubishi Electric, SAUTER)

Behavioral Indicators

- **Immediate Public Disclosure:** Claims responsibility within hours
 - **Ransom Demands:** Financial extortion following system compromise
 - **Geopolitical Messaging:** Anti-Western, pro-Russian/Chinese propaganda
-

Conclusion

The Infrastructure Destruction Squad represents one of the most significant cyber threats to critical infrastructure currently active. Their combination of sophisticated technical capabilities, clear geopolitical motivations, proven operational success, and likely state sponsorship makes them a priority target for cybersecurity and national security agencies worldwide.

The group's explicit alignment with Russian and Chinese interests, combined with their systematic targeting of Western infrastructure, suggests this threat extends beyond typical cybercriminal activity into the realm of state-sponsored hybrid warfare. Immediate defensive measures, enhanced international cooperation, and comprehensive counter-intelligence operations are essential to mitigate this critical threat.

Final Assessment:

- **Confidence Level:** HIGH (based on extensive communications analysis)
- **Threat Classification:** CRITICAL (active, sophisticated, escalating threat)
- **Recommended Response:** IMMEDIATE AND COMPREHENSIVE

Visit [Trellix.com](https://www.trellix.com) to learn more.



About Trellix

Trellix is a global company redefining the future of cybersecurity. The company's open and native extended detection and response (XDR) platform helps organizations confronted by today's most advanced threats gain confidence in the protection and resilience of their operations. Trellix's security experts, along with an extensive partner ecosystem, accelerate technology innovation through machine learning and automation to empower over 40,000 business and government customers.

Copyright © 2024 Musarubra US LLC

072022-05