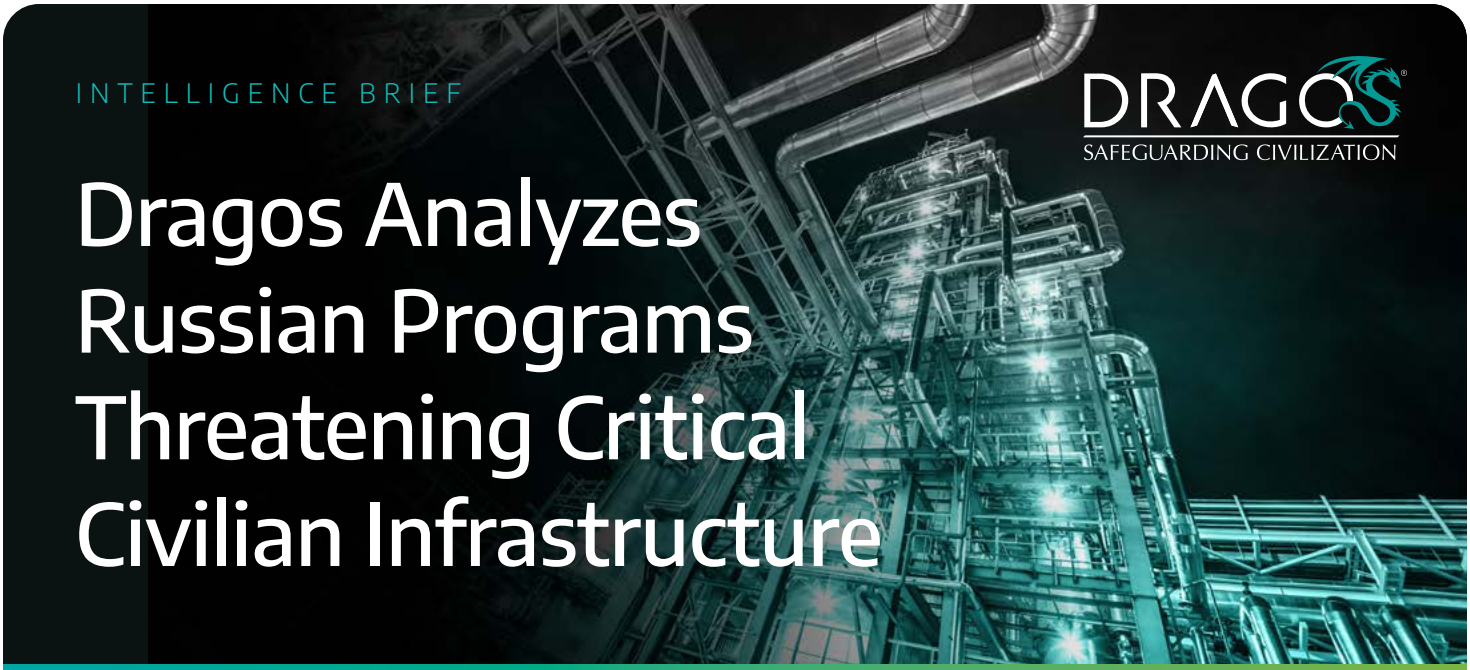


INTELLIGENCE BRIEF

Dragos Analyzes Russian Programs Threatening Critical Civilian Infrastructure

KEVIN WOOLF | SENIOR INTELLIGENCE ANALYST

BRYCE LIVINGSTON | SENIOR ADVISORY HUNTER

DRAGOS, INC

APRIL 2023

Overview

Dragos reviewed a series of alleged contracts between the Russian Company NTC Vulkan and the Russian Ministry of Defense that were highlighted in a recent press article from the Washington Post. This public intelligence brief outlines the threats to critical infrastructure described in those documents.[1] The Russian cyber program Amesit is a broad and wide-ranging program executed over several years with multiple sub-components and contractors. It is well documented that this cyber program includes intelligence organizations, private firms, and co-opted criminals who often work alongside government computer network operations (CNO) entities.[2] While we are missing the initial government Terms of Reference (TOR) that outlines what the government specified Amesit must be able to do, we can infer based on the Amesit-B testing and concept design documents what it is. Amesit-B, in Western terms, is an offensive computer network operations platform that includes signals intelligence (SIGINT), electronic warfare (EW), and malign influence capabilities.

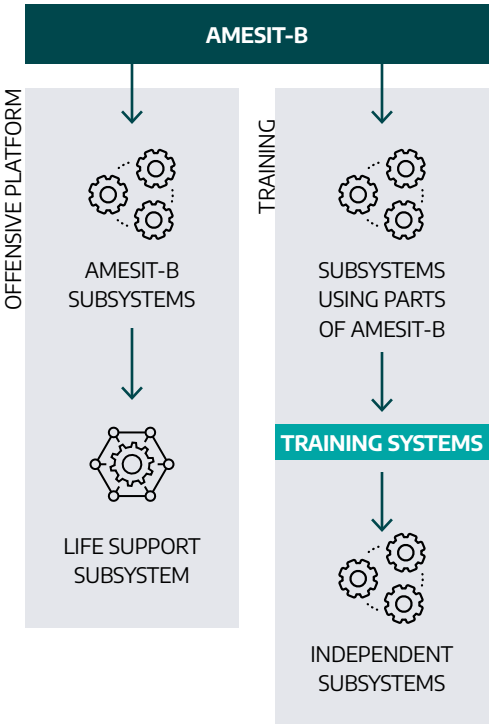
1 **Secret trove offers rare look into Russian cyberwar ambitions** — Washington Post

2 **Russian Cyber Units** – U.S. Congressional Research

Key Findings

- Dragos assesses with moderate confidence that the documents reviewed are legitimate and were leaked or stolen from a Russian contracting repository.
- It is unlikely that these tools and platforms are exclusively used for testing or training purposes.
- Modules contained in the Amesit-B platform could allow for a range of impacts in rail and petrochemical environments which could result in physical consequences, including damage to physical equipment or creating unsafe conditions where injury and loss of life are possible.The capabilities described are consistent with previous attacks attributed to various units of the Russian Military's GRU, with tactics, techniques, and procedures (TTP) overlapping with multiple identified threat groups.

Overview of Amesit-B



Amesit-B is a codeword identifying the development of a platform (software and hardware) with several sub-components. Amesit-B is a combined military EW and SIGINT platform used for conducting/coordinating SIGINT, EW operations, malign influence, and offensive and defensive cyber operations. Amesit-B, a sub-platform of the overall Amesit project, is a special software and hardware kit produced and tested by the Rostov Scientific Institute of Radiocommunications as the primary contractor and by NTC Vulkan as the sub-contractor. Amesit-B includes the following subsystems and capabilities:

- Formation of an autonomous segment of the data network
- Message decoding subsystem
- Internet and media monitoring subsystem
- Control of the information and technical facilities for telecommunications and life support systems. The Russian term 'life-support systems' refers to critical civilian infrastructure such as oil pipelines, rail and transport systems, water treatment facilities, etc.
- Data relaying subsystems using intermediate servers
- Preparation, placement, and promotion of special materials, referring to malign influence
- Testing of telecommunications equipment
- Storage subsystem
- Results processing subsystem

The concerning subcomponent is the "control of the information and technical facilities for telecommunications systems and life support systems" because it is designed to attack industrial control systems (ICS), specifically rail and petroleum industrial equipment.

Amesit-B Access Capabilities

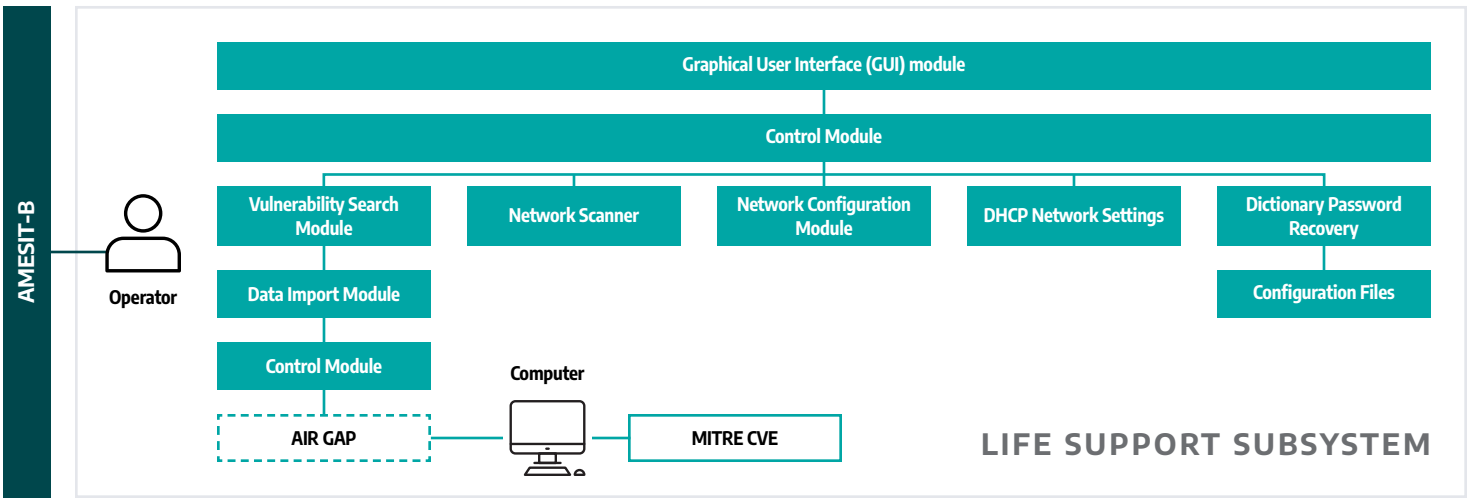
Dragos has a deep understanding of Russian Cyber, SIGINT, and EW programs, and some recent characterizations in the media likely do not take the context of the overall program into account, specifically regarding the necessity for potential attackers to achieve physical access to a target environment or equipment. Adversaries only need local area network (LAN) access to employ the offensive operational technology (OT) capabilities described in the testing documentation. Dragos assesses with moderate confidence that the system designers assumed LAN access would be guaranteed through physical control of local tier-one internet service provider (ISP) infrastructure. The exact manner to gain access to backend telecommunications equipment is unknown, whether through physical control in an occupation or covert means. The occupation example in the documents was Ukraine, which is now an offensive military occupation operation. However, such placement allows for man-in-the-middle (MiTM) attacks and exposes the management functions of the telecommunications equipment, allowing the equipment to be used in a variety of ways to proxy and manage local network traffic. It does not appear that physical access to a target OT environment is assumed or necessary.

Amesit-B is designed to enable a combatant commander to take physical and logical control of information flow in a geographic area in a likely assumed military occupation setting. Specifically, Amesit must be able to take control of the internet in the area through physical access to the local tier-one ISP network infrastructure —in addition to blocking/manipulating local global positioning system (GPS), cell service, and social media. Much of the Amesit-B technical documentation describes the core telecommunications equipment that can be 'accessed for management without authorization in the presence of physical access,' implying either a covert or occupation scenario.

Analyst Comment: It is important to note that capabilities are agnostic to delivery. That is, any malware planned for use against specified targets does not rely on this system for delivery. Though Ukraine is highlighted as a specific example in the documents, it does not preclude the GRU from using this tool in other geographic regions.

- **Concept Design:** The Amesit-B concept design documentation outlines at a high level how the Amesit-B program satisfies the technical requirements set out by the Russian Government in the Terms of Reference (TOR). Dragos did not have access to the original TOR, but the concept design states that the software for control of information and technical facilities associated with telecommunications and life support systems should provide for testing of the telecommunications equipment at the distribution and core levels for the possibility of penetration by an external intruder. Moreover, the software should provide for the possibility of installing 'third-party expansion modules' and conducting new types of load and functional testing not detectable by modern protection means aimed at blocking telecommunications equipment operation. At the same time, the concept design establishes the necessity to specify technical requirements for telecommunication equipment control and requirements for expansion modules.

- **Pre-Testing Methodology:** The pre-testing methodology documentation outlines the technical procedure for testing that each element of the concept design satisfies the TOR. The pre-testing methodology specifies that model environments must be created for Amesit-B with the ability to visualize the mechanisms of action and specify how to use the model to test the capability successfully. In that way, physical access to the model is assumed for the test procedure (although that is not explicitly indicated). But it does not specify that physical access to the target network or device itself is assumed for deploying capabilities. In fact, the portions of the documents detailing how to test the OT-specific offensive capabilities are subsumed under the overall requirement, noted above as "Concept Design." The inclusion of the OT-specific offensive testing and capabilities under this requirement and thorough analysis of the rest of the document leads Dragos to assess with moderate confidence that the designers of Amesit-B assume access for specific offensive capabilities is provided via control of the backend telecommunications infrastructure.



Amesit-B Life Support Special Software

This subcomponent of Amesit-B enables operators to scan networks and attempt to identify hardware, firmware, and software and has the central purpose of being used against industrial equipment. The system has a database that copies vulnerabilities from MITRE ATT&CK to automatically notify the operators of potential vulnerabilities within the scanned network. These vulnerabilities ultimately enable the operators to conduct computer network intrusions to collect information from networks and further accomplish **Damage to Property, Denial of Control, Loss of Control, Loss of Productivity and Revenue, Loss of Protection, Loss of Safety, Manipulation of Control, and Theft of Operational Information.** These MITRE ATT&CK techniques, in laymen's terms, could degrade, damage, or destroy physical equipment; or injure or kill people.

Assuming the contract was completed, two models were built and designed between 1:70 and 1:87 scale and included typical sensors and actuators for simulated cyber attacks with physical consequences.

Address Resolution Protocol (ARP) Spoofing Attack Scenarios

The two specifically tested capabilities included address resolution protocol (ARP) spoofing attacks which would result in significant impacts on rail and petrochemical equipment and operations. We have outlined the test success criteria of the two attack methods below:

- The first is an ARP-spoofing attack simulation on a model rail OT environment referred to as a 'test bench' which, if successful, results in physical changes in the industrial control processes accompanied by visual changes in the operation of the model (triggering of light alarms, the collision of objects, emission of smoke, etc.). Further, success criteria are defined as:
    - unauthorized track switchover
    - the collision of trains
    - accidents at the entrance to the depot and on the marshaling hill
    - loss of control over the speed of trains
    - failure of the combined heat and power (CHP) unit, and, consequently, de-energizing of all objects in the stand
    - failures in the operation of the barrier

- The second is an ARP-spoofing attack simulation on a model petrochemical OT environment, which, if successful, results in a physical change in technical industrial control processes accompanied by visual changes in the operation of the model. There was also a mention of Special Software. The specific goals of this simulation were to use "Special Software" to remotely:
    - close gate valves
    - shutdown the pump unit
    - overfill the tank
    - spill raw materials
    - cavitate the pump unit, accompanied by vibration of the pump unit
    - overheat of the pump unit, accompanied by smoke in the unit
    - smoke in the oil heating station in case of excessive operating temperatures.

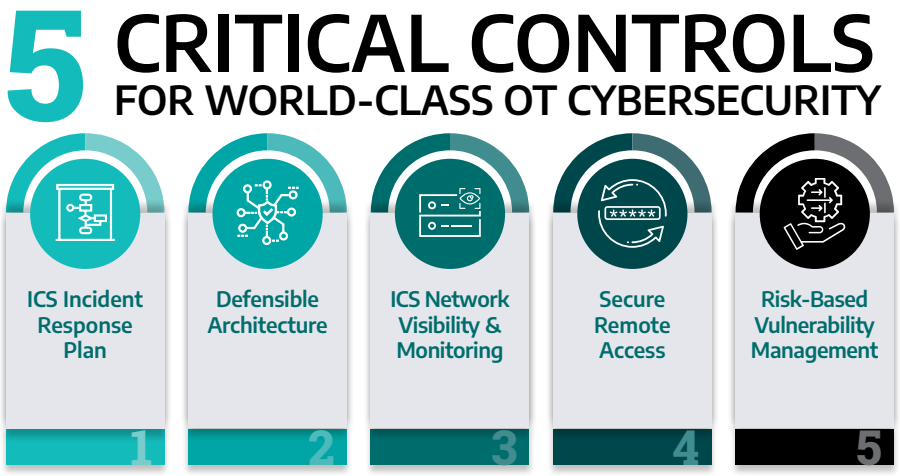
Conclusion

Russian intelligence services continue to invest in the development of more efficient cyber operations at the beginning of the attack lifecycle, as shown by contracted projects from NTC Vulkan. The projects also reveal interest in using cyber operations to amplify psychological effects and target critical infrastructure, including energy utilities, oil and gas, water utilities, and transportation systems. Defenders should be aware of these capabilities and priorities to protect critical infrastructure and services.

Recommendations

Considering this risk and related threats, Dragos recommends five critical controls for OT cybersecurity identified by the SANS Institute[3] that provide a framework to defend against adversary activity directed against OT networks, be it IP (Intellectual Property) theft, ransomware, or targeted cyber-physical effects. **Download our guide to SANS 5 Critical Controls to learn more.**

A first step in implementing these controls is achieving executive alignment on the role and importance of OT cybersecurity if not well understood. One potential way to achieve organizational alignment is to tie the effort to real-world scenarios. The information in the documents detailed above clearly outlines the capabilities developed for the adversary and their intended impacts. This detail can be instrumental in understanding how the capabilities might impact a given network, the potential operational and business implications, and the steps necessary to defend against and remediate the potential effects. Once an organization can achieve executive and board-level alignment on the importance of investing in OT cybersecurity, the foundation is in place to implement the five critical controls shown at right.



3 **The Five ICS Cybersecurity Critical Controls** — SANS

About Dragos, Inc.

Dragos, Inc. has a global mission to safeguard civilization from those trying to disrupt the industrial infrastructure we depend on every day. Dragos is privately held and headquartered in the Washington, DC area with regional presence around the world, including Canada, Australia, New Zealand, Europe, and the Middle East.

To learn more about our technology, services, and threat intelligence offerings, visit **dragos.com** or connect with us at **sales@dragos.com**.