SEKOIA.IO analysis of the #VulkanFiles leak

⋮ 3/30/2023

Key Takeaways

- Exfiltrated Russian-written documents provide insights into **cyber offensive tool projects** contracted by Vulkan private firm for the Russian Ministry of Defense.
- Scan-AS is a database used to **map adversary networks** in parallel or prior to cyber operations. Scan-AS is a subsystem of a wider management system used to conduct, manage and capitalize results of cyber operations.
- Amezit is an information system aimed at **managing the information flow on a limited geographical area**. It allows communications interception, analysis and modification, and can create wide information campaigns through social media, email, altered websites or phone networks.

Introduction

In January 2023, French newspaper Le Monde offered SEKOIA.IO to cooperate on investigating **exfiltrated Russian-written documents** related to the Moscow-based private company **Vulkan**. In parallel, Le Monde journalists were also cooperating with an international newspaper consortium led by Paper Trail Media on the subject. With Le Monde's agreement and as the consortium just published about "#VulkanFiles", SEKOIA.IO analysts provide a technical analysis of the two systems exposed, **Amezit** and **Scan-AS**, and offer use-case hypotheses.

The exfiltrated documents include user manuals, presentations, and technical documents dated from 2016 to 2019. They were allegedly exfiltrated from **Vulkan** firm, an IT company headquartered in the western suburbs of Moscow, near the Moscow Polytechnic University. Vulkan offers services such as pentesting, consulting, certifications, training or security operations center. Based on its public website, Vulkan works with private and public Russian entities, such as major banks (Sberbank), public organizations (RusHydro), telecom operators (Rostelecom) as well as foreign-based companies (Boeing, PSA).

Based on the documents' headers, this is a joint project between Vulkan and the **Rostov Federal Institute for Radio Technology**, a public administration under the tutelage of the FSB since at least 2010. Identified end customer of this project is the **Russian Ministry of Defense**.

Scan-AS

The first batch of documents SEKOIA.IO analysts consulted pertain to a project codenamed Scan-AS. Scan-AS is an **isolated database** used to **map adversary networks** in parallel or prior to cyber operations conducted by the Russian military intelligence services GRU.

This database can receive semi-formatted data from several sources that fall into **two main categories**. The data collected from **open sources** such as databases available online, and **closed sources** coming from active or passive operations such as Signal Intelligence (SIGINT) conducted by Russian intelligence service against targeted computers and telecommunication networks.

Open source inputs in Scan-AS rely on multiple **Internet scanning services** (including Shodan.io, Scans.io, and the Internet Census 2012), **vulnerability databases**, such as CVE and NVD lists, as well as **WHOIS bases** such as ARIN, RIPE or Verisign. These different sources of data **allow** the operators **to passively map** the **external partof an information system**: Autonomous systems, IP address ranges, domains and associated vulnerabilities for each discovered service.

Based on our comprehension of the documents, closed sources gather multiple results such as Cisco router configurations, which assists the operators to map routes inside the targeted infrastructure, exfiltrated email databases, as well as PCAP files and raw emails, possibly originating from SIGINT operations. **SEKOIA.IO analysts assess closed sources** used by ScanAS possibly **include data collected from offensive cyber operations as well as SIGINT activity.**

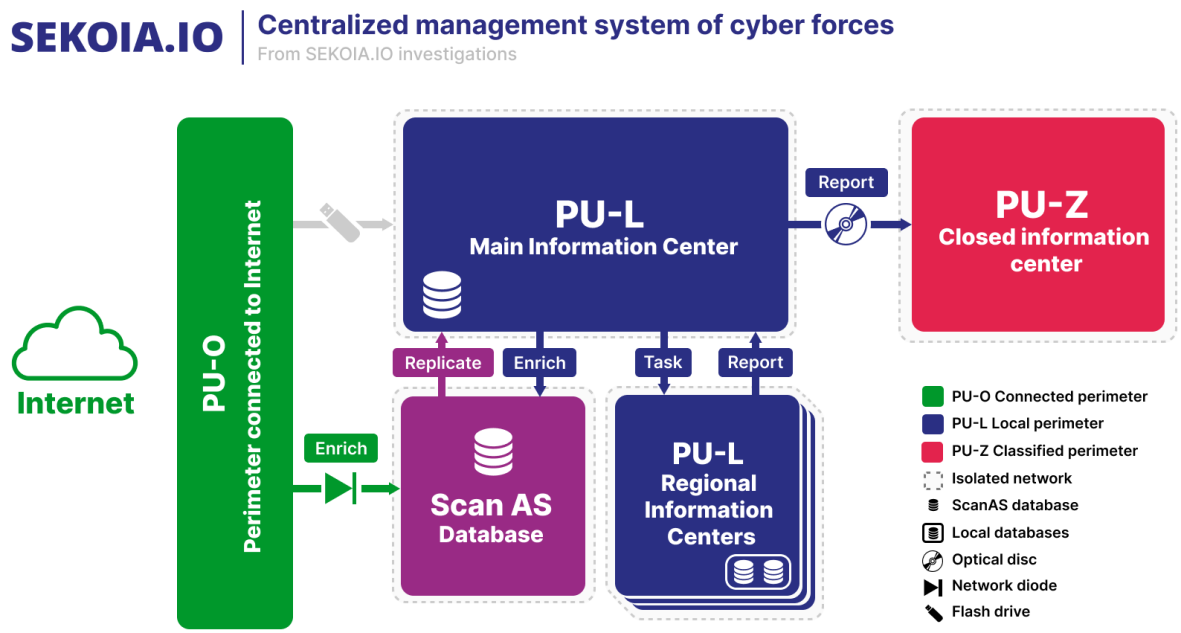
Scan-AS operators can map targeted information systems through a **graphical interface**, allowing **multiple operators** to work in parallel. It is possible to import and export any type of data useful for cartography and cyber operations (network schemes, exfiltrated data etc.) through the interface.

Centralized management system of cyber forces

The Scan-AS database is part of **a wider information system,** designated in the document as *"hardware and software system for centralized management of [cyber] special forces"*. This system is likely used to conduct, manage and capitalize results of cyber operations.

The centralized management system operates off the Internet through physically isolated networks. The full system is **designed withsubsystems** with different confidentiality levels.

The **first subsystem**, designated in the documents as "ПУ-Л / PU-L" – for local information system – can be seen as the **operation level management**, used to task operators and share operations data. The subsystem is isolated from the Internet. It shares the processed information to a Main Information Center (GIC) and several ground units in Regional Information Centers (RIC). According to the documents, the "ПУ-Л / PU-L" can not store classified information.



The **second subsystem** aimed at processing the operational reporting from the first one. Designated as "ПУ-З / PU-Z" – for closed information system -, it is a **classified network** entirely separated (**air gap**) from other subsystem. This subsystem is an **isolated replica** of "ПУ-Л / PU-L" **only dedicated to reporting**. It can contain classified information such as strategic orientation or full view of operations which are not available in the "PU-L" sub-system. The data transfer between "ПУ-Л / PU-L" to "ПУ-З / PU-Z" is only done by using optical discs.

Of note, having isolated networks does not presuppose that they are physically distant. Therefore, an operator with access to the PU-O network can, on the same desk, have access to the PU-L network with its associated applications and databases.

SEKOIA.IO takeaways on Scan-AS and Management system

Isolated networks and databases are commonly seen in use by Intelligence Services, to prevent their compromise from networks connected to the Internet.

SEKOIA.IO assess it is plausible "PU-L Regional Information Center" refers to intelligence units that are decentralized, for instance a SIGINT unit anywhere on the globe. Operators of the Main Information

Center could send a task that requires database requests on a decentralized database.

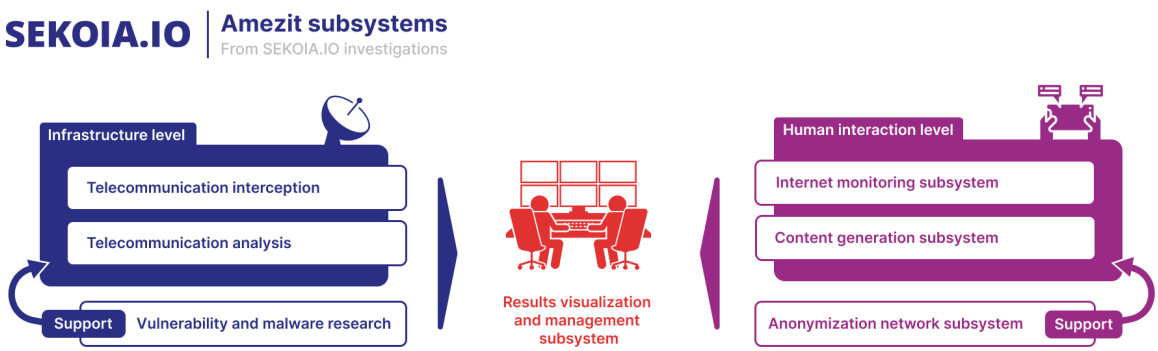
SEKOIA.IO TDR analysts point out that Scan-AS and its wider information system for cyber operations are coherent with the level of advancement and expertise expected for Russian intelligence service, including for cyber operations.

Amezit

Other documents consulted by SEKOIA.IO analysts are related to a second project named Amezit, an information system aimed at **managing the information flow on a limited geographical area**. The documents, dating from 2017, expose a preliminary design of a global system composed of multiple subsystems allowing the **collection**, **creation**, **modification** or **blocking of** the **information on a theater of military operations**.

Amezit's purpose is to manage information on two levels as represented in the figure below. First, the **infrastructure level,** by intercepting and analyzing network communications from routers and switches, allows the operators to **block** specific ISP subscriber's accesses or **redirect** users to filtered so-called "legitimate" resources.

Amezit also controls the information at the "human interaction" level. The system offers the possibility to **influence the targeted geographical** area with the **integrated creation, distribution** and **amplification of information** through multiple channels such as SMS, social networks (automated creation and management of fake profiles), blogs, phone network or internet forums.



Amezit information system's design document suggests a **centralized management of the subsystems operators** to monitor the current operations in a centralized system, renamed "Results visualization and management subsystem" in the schema above.

This subsystem works as a **command and control center** for situational awareness purposes fed by the subsystems ongoing operations thanks to a **geographic information system**. Data from each subsystem are transferred to a local data storage for visualization, as well as to monitor the Amezit subsystems infrastructure and software to detect Quality of Service (QoS) or security issues.

The management part aims at tasking a subsystem supervisor for a specific assignment. Once a team completes the task, a report is generated which can include materials related to the operation such as videos, pictures and documents.

Communication interception subsystem

The first subsystem presented in the design documents is a system **aimed** at **intercepting**, **blocking** and **altering communication** transiting through **telecommunication equipment** such as **switches** and **routers**.

The documents show this subsystem can be easily deployed with a simple laptop running **Astra Linux**. First, if the operator is present on the network managed by the equipment, the system attempts an automatic connection to the network. A scan is then launched to get the equipment's information (manufacturer and version) which is compared to **an exploit code catalog** to compromise the equipment.

Vulnerabilities scavenger hunt

The initial Amezit design describes an environment used for vulnerability research (such as fuzzing or reverse engineering) and malware development. It is worth noting that Vulkan tried to subscribe to a 3-years service offered by vulnerability brokers such as Secunia or Zerodium. Their demand was declined by the companies, exception made for the CANVAS tool by Immunity, a commercial security assessment tools vendor, through SoftLine, their authorized Russian software distributor.

It is worth noting that the design document explicitly references exploits and implants used by the Equation Group and published in open sources by the Shadow Brokers, indicating these exploits will be integrated into the solution. Additional research is planned to be undertaken to discover new vulnerabilities, including in telecommunication equipment.

If no exploit code is available, the system launches a **bruteforce attack** against the equipment's management protocol. Once the telecommunication equipment is compromised, the operator can **redirect the network flow** to the **communication analysis subsystem**, or **neutralize the device** with a simple configuration change.

If the equipment can not be compromised, the operators can deploy a complete **new infrastructure** in parallel. Such implementation is done either by **disconnecting the network equipment power supply** or by **jamming the frequencies** used for wireless ones.

SEKOIA.IO analysts did not access the **operators manual, detailing** the techniques leveraged by the operators to **redirect the network traffic** to the **communication analysis subsystem**. Therefore, it is not clear whether this is achieved through changing the equipment configuration to create new routes or tunnels, or using tailored implants.

Communication analysis subsystem

Data collected by the interception subsystem is analyzed by a specific subsystem that we call "**Communication analysis subsystem**". This system is composed of several nodes which can analyze or conduct on-the-fly modification of the processed data to block or redirect the subscribers to specific websites. The Amezit analysis system **does not seem to analyze all communications,** but only those of certain subscribers (or pool of subscribers) previously selected and associated with an infiltrated telecommunication equipment.

Once the data is received by the analysis system, a dissection of the protocols (FTP, HTTP, POP3, IMAP, SMTP, SNMP, IPSec etc.) is done to extract the **metadata** and associated **payload**. When the protocol isn't encrypted, or when the **protocol security is downgraded** by the interception system, the payloads are extracted, saved and analyzed. If the retrieved payloads (such as files) are password-protected, they are sent to an **FPGA-based distributed cracking system** to break their protection.

The communication analysis subsystem of Amezit has the capacity to **block or redirect** subscribers communications by tampering with specific protocols. This is done to **prevent the usage of anonymization technologies** such as **TOR**, **I2P** or **private VPNs** services, as well as redirecting targeted subscribers to specific websites called "legitimate ressources". These websites are created by a **cloning system** aimed at disseminating false information by injecting data in **mirrored websites**.

In addition to its ability to **intercept** and **tamper network** protocols, this system is equipped with a **graphical interface** allowing operators to **consult and analyze the collected data**. The design document displays capabilities of this interface, including :

- View intercepted communications in graphs or data tables;
- List intercepted files as well as the cracked passwords;
- Link several selectors together (MAC addresses, IP addresses, email addresses etc.);
- List subscribers using VPN protocols;
- List connections blocked by the system and associated subscribers;

By-design, the Amezit interception and communication analysis subsystems seem restricted to **very targeted operations** on telecommunication infrastructure of a **specific area**.

Looking at OSINT data and publications related to telecommunication tampering since the beginning of the Russo-Ukrainian conflict, **we were not able to link any event** in occupied territories (such as BGP hijacks or blank SIM card deployment) **to the use of Amezit's interception subsystem**.

Internet monitoring subsystem

Amezit allows the **analysis** of **publications related to specific geographical regions** on multiple Internet platforms such as social networks, news websites or Internet forums. The design document stipulates that ten social networks need to be monitored, including Facebook, Twitter or VKontakte. The specifications also stipulate that other networks used in Central Asia and the Middle East will need to be integrated.

From an operator point of view, this subsystem has a graphical interface that shows the collected information in the form of graphs, on a planisphere, and inside data tables. It allows the operator to browse and search all public posts of a specific user (or private, under certain conditions), to make thematic searches throughout the content of collected data and to trace the primary sources of an article. Each collected material is subjected to a **semantic analysis** to **determine** which **sentiments** emerge from it to present them to the operator.

Not only is Amezit's Internet monitoring subsystem dedicated to monitoring purposes on social networks, it is also designed to discover key users that can be used as relays for Russian-aligned narratives amplification.

Content generation subsystem

Other subsystems presented in the design documents of Amezit are dedicated to disseminate information on various communication networks such as emails, SMS/MMS, voice (phone), blogs, forums, news portals and social networks. For that purpose, Amezit embeds a system allowing operators to create mass campaigns of narrative distribution which mimics legit users' interactions on social media platforms.

This subsystem is composed of several parts. The first one is a **propaganda materials creation module**, by using common tools such as video, sound and photo editors. The created materials are then stored in a document management system, where each created media is classified, and where the materials' **metadata are cleaned** and replaced by fake ones to hinder traceability.

The second part of the information generation subsystem is dedicated to interaction with social media platforms and posting of generated materials. Based on its specifications , Amezit should offer the capability to register new users by cloning real profiles or creating new ones. Created users need to behave as real ones by reacting or posting posts and media.

Another Amezit feature is **massive publication campaigns broadcasting** on social networks, in public groups and joined closed groups. It provides operators with metrics used to track reactions to publications: number of likes, friends, replies, mentions or redirects.

To make this subsystem operational, several **security measures** implemented by social network companies to prevent bots should be **bypassed**. For instance, the SMS-based account verification occuring during the user registration can be bypassed by using SIM banks or onlines services. Another security measure discussed in the conceptual design is the captcha put in place by the social networks against robots. To circumvent this measure, the "Antigate" online service which employs human workers paid to solve captchas is suggested.

Private anonymization network subsystem

To disseminate and monitor information on the Internet, the design document of Amezit provides another subsystem aimed at maintaining an **anonymization network** used by the Information generation and Internet monitoring subsystems.

The designed anonymization network consists of a supervised and secure network of purchased servers hosted worldwide, allowing an operator to choose an exit country from an interface. Several designs are discussed in the document, such as:

- VPN chained via several layers of purchased servers;
- VPN chained via a combination of purchased servers -> TOR -> purchased servers;
- VPN sending data to the TOR network, which will use TOR as exit nodes;
- VPN chained with a combination of purchased servers-TOR-purchased botnet.

The last design (using purchased accesses from a botnet) is not suggested as it presents several design issues such as the unstable status and life time of the exit nodes, the possibility to be detected by security solutions and then, be examined by security researchers.

The authors of the document seem to recommend the first solution, by using OpenVPN, allowing a high speed and a total control of the anonymisation network, whose operational security is presented as the cornerstone. The authors suggest creating **anonymization chains** which link nodes **between countries with no international judicial cooperation** to prevent follow up investigations. Moreover each node needs to use secure boot and encrypted containers to store their operating system and tools, preventing it from being seized and analyzed. Standard hardening methods such as closing all ports, deleting unnecessary services, working under non privileged users and changing default services banners is also advised.

In terms of protection against SIGINT and traffic analysis, they suggest using a different key on each node to prevent eavesdropping of the whole network if a node is seized. They also recommend augmenting junk data transferred through these nodes, by, for example, setting up TOR relay nodes, public file sharing sites, using bittorrent to download random files automatically or by installing open VPN/HTTP proxies.

This network is monitored and managed through a console where an administrator can assign virtual routes to specific users and groups. Each node logs events, such as unauthorized route changes, and sends usage statistics and potential security incidents (reboot, etc.) to the administrator through the TOR onion service.

It is worth noting that the design document of this anonymisation system shows **state of the art methods** which can be employed to **prevent the possibility to track the source** of an information. However, as of today, we do not have evidence proving its existence in observed GRU operations.

SEKOIA.IO takeaways on Amezit

Amezit's information control features on limited geopolitical area echoe Russian maneuvers on telecom and broadcasting devices in formerly occupied Kherson region. Academic researchers observed that Russians, as they invaded Ukrainian territories, implemented actions to systematically take over and reconfigure radio and television antennas, to broadcast their narrative to the population. In May 2022, Kherson residents were distributed blank SIM cards by Russian personnel. In terms of Internet service providers (ISPs), Kherson network was rerouted in June 2022 to the Russian network through the Crimea-based operator Miranda-Media.

Although SEKOIA.IO did not find any technical evidence or open source resources linking Amezit, Scan-AS or other systems mentioned in the documents to the ongoing Russian military operation in Ukraine, it is possible Amezit system specifications are coherent with described activities in the context of the Russo-Ukrainian conflict.

SEKOIA.IO analysts assess it is possible that Amezit was designed as **a tool to replace the information bubble in occupied territories** to broadcast Russian narrative, either to legitimate their operations, or to discourage any type of resistance. With deceiving social media campaigns, fake information broadcasted on cellular networks, altered content on trusted internet sites, local resistance could be hindered when convinced by fake claims of adversarial success. **Amezit** can be seen as a **projection tool** of the Russian information surveillance and censorship system sometimes referred to as RuNet.

Conclusion

Exfiltrated Vulkan documents provided insights into two different information systems supposedly designed for Russian military intelligence services. If Scan-AS, a tool used to map and prepare operations on advisory networks, is relatively common and expected, Amezit particularly caught SEKOIA.IO analysts' attention.

Amezit global system gathers infrastructure control features – communications interception, analysis and modification – and information level control features – internet monitoring and automated content creation. In this sense, **Amezit is an illustration of the Russian information warfare doctrine**, a concept which looks for strategic gains through the combination of offensive cyber operations, electronic warfare, psychological operations, and information operations.