

Vulkan Unveiled: Tools of The Trade

PART 3 :: 7/4/2023



THE RUNDOWN

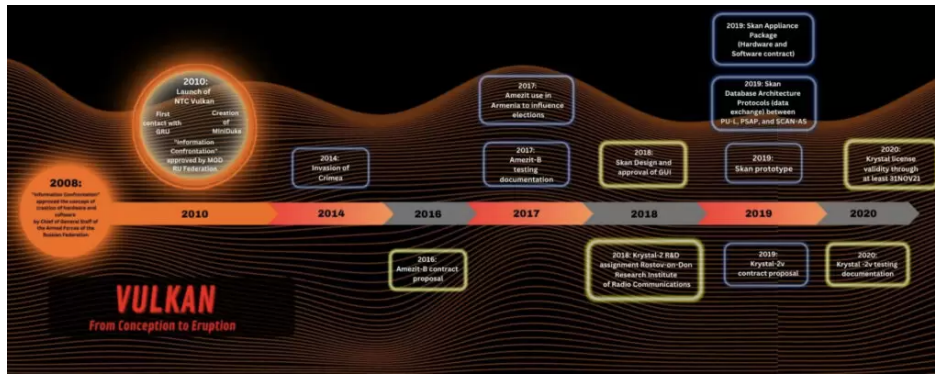
In *Strike Source's* previous pieces, we explored who NTC Vulkan is, their leadership, and the potential geopolitical implications of Vulkan's role in Russian cyberwarfare. In this third and final instalment of our Vulkan series, we explore the tools unveiled by the Vulkan files leak, focusing on their capabilities and potential implications.

The leaked documents revealed the existence of Amezit, which is a project for the development of a complex and dangerous cyberwarfare tool developed by Vulkan. Amezit is able to breach telecommunications equipment, manipulate internet traffic, generate counterfeit social media profiles, and disseminate disinformation. Its sophisticated subsystems can intercept, block, and modify traffic, reroute network flows, analyze protocols, and even prevent individuals from utilizing TOR or a VPN.

The leaks also shone light on Krystal2V, Vulkan's secretive and sophisticated training program for Russia's cyber warriors of tomorrow. Beyond a training program though, Krystal2V served as a platform to test the Amezit system on sophisticated operations, including testing its abilities to disable control systems for critical infrastructure.

Skan, an advanced software tool employed by Vulkan for ongoing vulnerability analysis of the internet, was another tool uncovered amongst the leaked documents. Skan utilizes open-source and closed-source data collection methods to consolidate information on system weaknesses. It enables operators to create extensive maps of external networks, pre-empt cyberattacks, and plot intricate attack paths, providing a significant advantage in cyber warfare strategy.

The tools unveiled in the Vulkan files leak not only emphasize the sophistication of these cyber capabilities but also underscore the potential risks they pose to global security, information networks, and critical infrastructure.



Spotted in The Wild – MiniDuke

The recent hotbed of attention should not let anyone think that Vulkan has only been active recently. In 2013, a cyberattack dubbed “MiniDuke” targeted and successfully compromised government entities in over 20 countries, including Ukraine, Romania, and the U.S. The attackers leveraged sophisticated social engineering combined with a highly customized backdoor to infiltrate and extract intelligence from targets.

The cyberattack was later attributed to APT 29, also known as “Cozy Bear” or “The Dukes.” APT 29 has been linked to the SVR, Russia’s foreign intelligence agency, and is credited with leading some of the most infamous cyber espionage campaigns from the last decade.

Shortly before the attack, in late 2012, the group sent out an email to test the malware’s ability to bypass Gmail virus filters. The sender’s email address was later tied to the MiniDuke attack, and the recipient’s address belonged to the NTC Vulkan domain.

While the presumably successful tests raised no immediate red flags, Google researchers were able to conclusively tie NTC Vulkan to APT 29’s MiniDuke attack when one of the hackers made a mistake over the course of the operation. Namely, the same IP address used to register the Google account which the malware was sent from was also used to rent a command-and-control server, a central server that manages and coordinates the activities of networked devices.

While it was too late to stop the hacking campaign at the time of the discovery, the slip-up resulted in a definitive link being established between NTC Vulkan and APT 29, a state-sponsored cyber threat actor.

As mentioned in our first and second articles, MITRE later identified the first use of MiniDuke as being in 2010. This validates that the relationship between Vulkan and the Russian intelligence apparatus dates back to the cradle of the company.

Amezit

Embedded in the trove of leaked documents are mentions of a project dubbed Amezit, a creation of Vulkan. Amezit is a multifaceted tool, exhibiting the ability to breach telecommunications equipment, scrutinize communications, and monitor targets’ internet activity. Its capabilities extend to manufacturing counterfeit social media profiles and establishing a grid of fabricated accounts that are pivotal to spreading disinformation.

Amezit stands out as a sweeping system. The primary subsystem intercepts, blocks, and modifies traffic traversing telecommunications devices like switches and routers. Once breached, this apparatus can be manipulated to reroute network flows or neutralized via a simple configuration change. The intercepted data is subsequently funneled into a specific analysis subsystem that deconstructs protocols and alters data instantaneously to block or redirect users to designated websites. Amezit can be used to prevent specific individuals from using the TOR or a VPN.

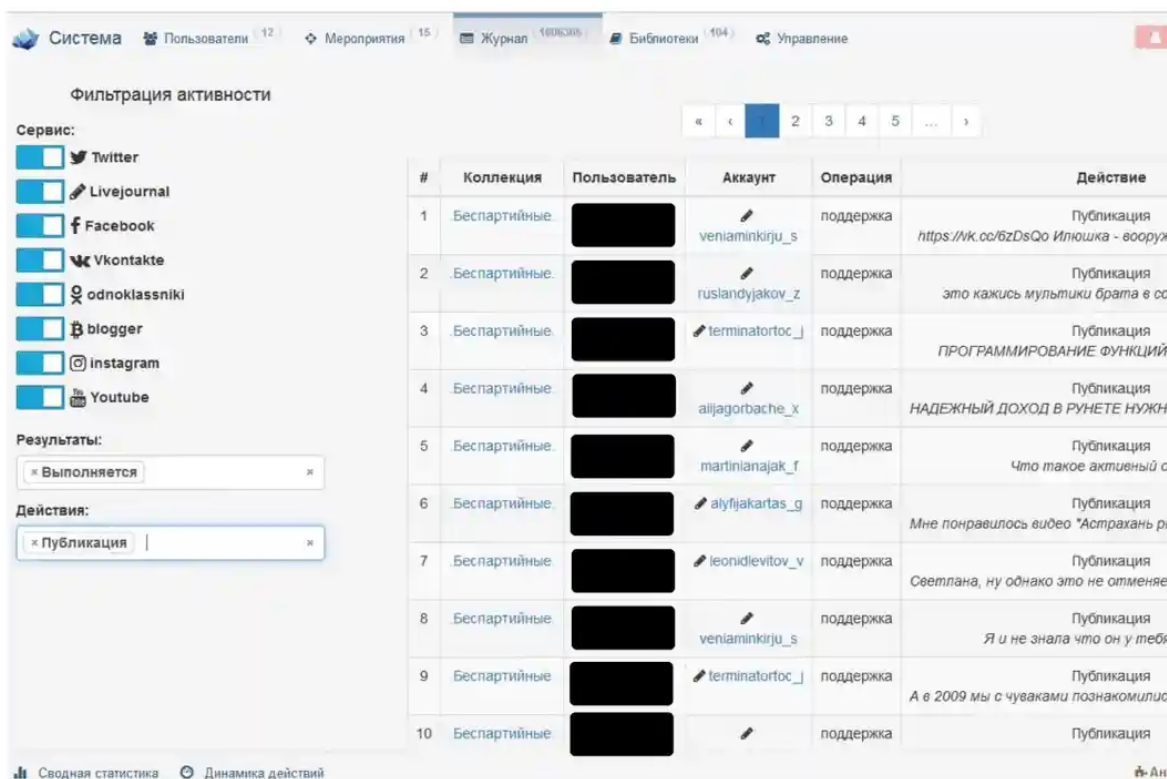
Additionally, the system is capable of singling out influential social media users and figures who could potentially spread narratives in line with Russian interests. This means that Amezit is not merely an analytic of offensive tool, but a cornerstone and loudspeaker in disinformation campaigns through its ability to generate, distribute, and amplify disinformation through various communication channels such as SMS, social networks, and internet forums. Amezit hosts a module for crafting propaganda, armed with tools for video, audio, and image manipulation.

Upon creation of propaganda materials, Amezit can initiate widespread publication campaigns across social media platforms, tracking public response metrics including likes, replies, and redirects.

The tool could be deployed anywhere with ease, akin to Metasploit, it is an all-in-one tool for the mass sowing of disinformation. Detecting the use of the Amezit in action would be challenging to say the least.

Other journalists failed to report on a crucial element, which is the link to Russian telecom providers, as we highlighted in our previous article. Having an in-depth understanding of these systems, Vulkan had the ability to customize the tool precisely to meet their clients’ (GRU, FSB) requirements. Additionally, there were speculations

circulating that the tool would require physical connection to telecom networks. However, the truth is that agencies such as the GRU would inherently also have access to these systems.



The screenshot shows the 'Журнал' (Journal) section of the Amezit tool. It features a navigation bar at the top with tabs for 'Система', 'Пользователи', 'Мероприятия', 'Журнал', 'Библиотека', and 'Управление'. Below the navigation bar is a 'Фильтрация активности' (Activity Filtering) section with a 'Сервис:' (Service) dropdown menu containing options for Twitter, Livejournal, Facebook, Vkontakte, odnoklassniki, blogger, Instagram, and Youtube. There are also 'Результаты:' (Results) and 'Действия:' (Actions) dropdown menus. The main content is a table with 10 rows of activity logs. Each row includes a number, a collection name, a user name, an account name, an operation type, and a description of the action.

#	Коллекция	Пользователь	Аккаунт	Операция	Действие
1	Беспартийные	[REDACTED]	veniaminkirju_s	поддержка	Публикация https://vk.cc/bzDsQo Илюшка - вооруж
2	Беспартийные	[REDACTED]	ruslandyjakov_z	поддержка	Публикация это какись мультики брата в со
3	Беспартийные	[REDACTED]	terminatorfoc_1	поддержка	Публикация ПРОГРАММИРОВАНИЕ ФУНКЦИЙ
4	Беспартийные	[REDACTED]	aiijagorbache_x	поддержка	Публикация НАДЕЖНЫЙ ДОХОД В РУНЕТЕ НУЖН
5	Беспартийные	[REDACTED]	martinianajak_1	поддержка	Публикация Что такое активный о
6	Беспартийные	[REDACTED]	alyfjakartas_g	поддержка	Публикация Мне понравилось видео "Астрахань рь
7	Беспартийные	[REDACTED]	leonidlevitov_v	поддержка	Публикация Светлана, ну однако это не отменяе
8	Беспартийные	[REDACTED]	veniaminkirju_s	поддержка	Публикация Я и не знала что он у тебя
9	Беспартийные	[REDACTED]	terminatorfoc_1	поддержка	Публикация А в 2009 мы с чуваками познакомилис
10	Беспартийные	[REDACTED]	[REDACTED]	поддержка	Публикация

Рисунок 22 – Раздел «Журнал»

Overview of the Amezit tool's social media component

Based on evidence found in the documents, the system was employed during the parliamentary elections in Armenia back in 2017. During that time, numerous accounts were utilized to disseminate a fabricated document alleging United States interference in the voting process. Additionally, trolls were deployed in a campaign targeting former US presidential candidate Hillary Clinton, as well as following the assassination of Colonel Maksym Shapoval, who served as the commander of the special reserve of Ukraine's Main Intelligence Directorate. This case saw bots responsible for generating identical posts containing a link to a conspiracy article on VKontakte, suggesting that the military officer was actually killed by his own colleagues.



Леонид Федотов

@1984leonidfedo1

стильный паца любящий девченок!!!!да которые любят крутить попками!!!!

Россия twitter.com/1984leonidfedo1 Joined October 2014

Troll account discovered to be operated using the Amezit tool

In order to ensure the operator and their intentions remain anonymous, Amezit contains a module which allows them to choose an exit country from a list of options. Several designs are discussed in the documents, 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.

It is a tool intricately designed to outwit social networks' bot-prevention security measures, emphasizing its sophistication and potential for unchecked propagation of disinformation.

Krystal-2V: Training The Next Generation

In 2018, Vulkan received a contract to develop an extensive training program dubbed Krystal-2V. This innovative program was designed to accommodate simultaneous operations by up to 30 trainees, serving as a platform for training new generations of cyber warriors. But Krystal-2V wasn't just a routine training program; it tested the Amezit system on a variety of sophisticated operations, including disabling control systems for critical infrastructure in the transportation sector, covering rail, air, and sea transport.

According to our source, who is an intelligence analyst with extensive knowledge of the documents, it has been discovered that among the files, there was a seating plan intended for prospective Krystal trainees during their sessions at Vulkan HQ. The purpose of these sessions was not only to demonstrate cyberwar weapons but also to provide comprehensive tutorials on the usage of these highly advanced tools.

"This is the platform and training model I'd use if I was going to war and invading a country", commented our source. From the documents, the program had been first thought of in 2018 at the Rostov-On-Don Research Institute of Radio Communications, with a contract being proposed and signed in 2019 to run through until November 2021.

Additionally, the functionality of Krystal-2V was dependent on modules. Considering the impending war, our source informed us that Vulkan conducted risk assessments on their supply chains, specifically those providing the necessary software to complete the program. Vulkan's objective was to determine which vendors would disregard sanctions and continue selling to them, as well as identify those who would not cooperate.

Communications in the documents also pointed to intersections between what is covered in the Krystal training program and Amezit. Our source stated that the creators were instructed to, "Talk to the Amezit group to not duplicate efforts."

The implications of this training program stretch far beyond simple capacity building – it reveals the potential for widespread disruption of civilian infrastructure, a notion that significantly escalates the perceived threat from these cyberwarfare operations.

Skan: Sandworm's Crown Jewel

Skan presents an equally troubling insight into cyber warfare strategies. It is an advanced software tool, which can conduct ongoing analysis of the internet for system vulnerabilities. This project aims to amass a catalogue of weaknesses to be exploited by the GRU for future cyberattacks.

To build its repository, Skan employs an open-source data collection tool that leverages various internet scanning services like Shodan.io, vulnerability databases, and WHOIS databases. By consolidating this information, operators can create extensive maps of external networks. Skan also utilizes a closed-source data collection tool that integrates data procured from offensive cyber operations and SIGINT activity. Joe Slowik, Threat Intelligence Manager at Huntress, sheds light on how Skan operates and suggests that Skan isn't an independent tool, but likely works in tandem with other software to maximize its usefulness.

A document from 2019 further reveals Skan's capabilities, indicating that it could present possible attack scenarios and even map out all network nodes involved in a cyberattack. This ability to pre-empt and plot intricate attack paths grants substantial leverage in devising and carrying out cyber operations. Skan seems to cultivate collaboration among the multiple hacking units operating under the umbrella of Russian intelligence, reinforcing its pivotal role in cyber warfare strategy.

THE TAKEAWAY

It is evident that the global security landscape is facing a formidable challenge in the form of state-sponsored cyber threat actors. The tools exposed in the Vulkan leak, such as Amezit, Krystal-2V, and Skan, demonstrate the sophisticated capabilities of these actors and their potential to disrupt information networks and critical infrastructure.

The need for a cohesive cybersecurity strategic plan is now more crucial than ever. Governments, organizations, and cybersecurity professionals must work together to develop robust defenses and proactive measures to counter these threats. This includes investing in advanced technologies, fostering international collaborations, and implementing stringent security protocols.

Only through a unified and comprehensive approach can we effectively defend against the evolving tactics of state-sponsored actors and safeguard our digital ecosystems. Failure to do so would leave us vulnerable to significant risks

and potential consequences for global security. It is imperative that we prioritize cybersecurity and take decisive action to protect our societies in this rapidly evolving digital age.