



Fronton: A Botnet for Creation, Command, and Control of Coordinated Inauthentic Behavior

Delivered May 2022

TABLE OF CONTENTS

EXECUTIVE SUMMARY	3
FRONTON	4
SANA	6
Behavior Models	8
Newsbreaks	10
Response Models	13
Groups	14
Other Files	15
0DAY TECHNOLOGIES	17
CURRENT STATUS OF SANA	19
APPENDIX A: VK ACCOUNTS USED BY SANA	20

EXECUTIVE SUMMARY

In March 2020, a hacktivist group called “Digital Revolution” claimed to have hacked a subcontractor to the FSB. They claimed the hack occurred in April 2019. They released documents and contracts about a botnet system of Internet of Things (IoT) devices built by a contractor, 0day Technologies. This botnet is known by the codename Fronton (ФРОНТОН). Media outlets went crazy. Headlines called it a tool that could be used to “turn off the Internet in a small country.”¹ Most analyses assumed that the goal of the system was distributed denial of service (DDoS). A day later, another tranche of documents, images, and a video were released, with significantly less fanfare.

Nisos research focused on that distribution of content. This release noted that DDoS “is only one of the many capabilities of the system.”² Nisos analyzed the data and determined that Fronton is a system developed for coordinated inauthentic behavior on a massive scale. This system includes a web-based dashboard known as SANA that enables a user to formulate and deploy trending social media events en masse. The system creates these events that it refers to as *Инфоповоды*, “newsbreaks,” utilizing the botnet as a geographically distributed transport. SANA provides for the creation of social media persona accounts, including email and phone number provisioning. In addition, the system provides facilities for creating these newsbreaks on a schedule or reactive basis. Two example lists of posting source dictionaries were included in the data. One, involving comments around a squirrel statue in Almaty, Kazakhstan may have affected the reporting on a BBC story. As of April 2022, 0day technologies has changed its domain from 0day[.]ru to 0day[.]llc. An instance of the SANA system appears to be up at [https://sana.0day\[.\]llc](https://sana.0day[.]llc). Nisos assesses that this is possibly a testing or demo instance, and is not currently used by the FSB.

Nisos researchers conducted open source research to discover 0day is known as 0Dt, full name Zeroday Technologies LLC (0Дт, ООО ЗИРОУДЭЙ ТЕХНОЛОДЖИС) based at Ulitsa Profsoyuznaya, D. 125, Etazh Tsokolnyi Pomesht. I, Kom. 14 Moscow; Moscow; Postal Code: 117647.³ Additional research indicated well-publicized Russian hacker Pavel SITNIKOV (known by his alias FlatL1ne) may be employed by 0Dt. SITNIKOV previously bragged about his connections with APT28, aka Fancy Bear and was arrested by Russian authorities in 2021.⁴ We assess that he likely has extensive knowledge of the functionality of the Fronton infrastructure and Sana front-end systems.

¹ [https://www.bbc\[.\]com/russian/news-51951933](https://www.bbc[.]com/russian/news-51951933)

² [http://web.archive\[.\]org/web/20200322062701/http://www.d1g1r3v.net/](http://web.archive[.]org/web/20200322062701/http://www.d1g1r3v.net/)

³ [https://www.emis\[.\]com/php/company-profile/RU/0Dt_000_0%D0%94%D1%82_%D0%9E%D0%9E%D0%9E_en_4765737.html](https://www.emis[.]com/php/company-profile/RU/0Dt_000_0%D0%94%D1%82_%D0%9E%D0%9E%D0%9E_en_4765737.html)

⁴ [https://therecord\[.\]media/an-interview-with-russian-hacker-pavel-sitnikov-there-is-no-hacking-scene-now-only-commerce/](https://therecord[.]media/an-interview-with-russian-hacker-pavel-sitnikov-there-is-no-hacking-scene-now-only-commerce/)

FRONTON

A March 2020 article in ZDNET highlighted that a hacktivist group called “Digital Revolution” claimed to have hacked a subcontractor to FSB Center 18 (Unit 64829) in April 2019. “Digital Revolution” claimed to have information, shared with some security researchers, that revealed Unit 64829 had issued a procurement order to the Russian contractor to implement a project called Fronton. Security researchers assessed Fronton was designed to create an IoT botnet for cyber attacks.⁵

The procurement order from Unit 64829 tasked Russian company InformInvestGroup CJSC - a longstanding contractor for the Russian Ministry of Internal Affairs - with creating an Internet of Things hacking tool.⁶ In turn, this company subcontracted this work to Moscow-based software company ODT (0day) LLC.⁷

Nisos acquired a tranche of documents from this hack from a Mega.nz link posted by “Digital Revolution.” We discovered that a portion of the Fronton tool called SANA [NFI, possibly an acronym for Соцсетный Аналитический Научный Аппарат, Social media Analytical Scientific Apparatus], appears to be a system for creating and managing multiple social media accounts for the purpose of posting disinformation on social media channels.

The Fronton system appears to have been developed as part of a research project known as Avenir (Аvenir) that was published in 2017 by the Kvant Scientific Research Institute. As early as 2010, the US Treasury Department identified this institute as being controlled by the FSB based upon a Russian government decree that defined the organization’s governance.⁸ The author of the report describes the disruptive power of social media and proposes methods for creating “social media waves” as a means of “spreading manipulative models in information spaces” or “a controlled method of information dissemination to a target audience.”⁹ It notes that “information technologies used in social networks create the potential for authoritarian socialization and manipulative influence on a person; moreover....they challenge the interests of public and state security.” It continues describing the various ways that social media responses can affect universal needs and how to influence an audience by utilizing three methods of persuasion (logos, pathos and ethos).¹⁰

⁵ [https://www.zdnet\[.\]com/article/hackers-breach-fsb-contractor-and-leak-details-about-iot-hacking-project/](https://www.zdnet[.]com/article/hackers-breach-fsb-contractor-and-leak-details-about-iot-hacking-project/)

⁶ [https://twitter\[.\]com/SwitHak/status/1241781096716656646](https://twitter[.]com/SwitHak/status/1241781096716656646)

⁷ [https://pbs.twimgimg\[.\]com/media/ETuw04qX0AEP3Nz.png](https://pbs.twimgimg[.]com/media/ETuw04qX0AEP3Nz.png)

⁸ [https://home.treasury\[.\]gov/news/press-releases/sm0410](https://home.treasury[.]gov/news/press-releases/sm0410)

⁹ [https://static1.squarespace\[.\]com/static/5bdc659f7c9327ff92ac4233/5c19af94562fa765670d3403/5c19afaaf950b7c1b74d4b80/1545187250403/1.3.png](https://static1.squarespace[.]com/static/5bdc659f7c9327ff92ac4233/5c19af94562fa765670d3403/5c19afaaf950b7c1b74d4b80/1545187250403/1.3.png)

¹⁰

[https://images.squarespace-cdn\[.\]swcom/content/5bdc659f7c9327ff92ac4233/1545187255827-WAJE41MY4G3RLXX8ODZM/1.4.png?content-type=image%2Fpng](https://images.squarespace-cdn[.]swcom/content/5bdc659f7c9327ff92ac4233/1545187255827-WAJE41MY4G3RLXX8ODZM/1.4.png?content-type=image%2Fpng)

ФГУП «Научно-исследовательский институт «Квант»

Экз. № _____

УТВЕРЖДАЮДиректор ФГУП
«НИИ «Квант»
д-р техн. наук

Г.С. Елизаров

2017

ОТЧЕТ О НАУЧНО-ИССЛЕДОВАТЕЛЬСКОЙ РАБОТЕ**ИССЛЕДОВАНИЕ ПРИМЕНИМОСТИ МОДЕЛЕЙ ГЛУБОКОГО ОБУЧЕНИЯ
ДЛЯ ЗАДАЧ МОНИТОРИНГА ОБЩЕСТВЕННОГО МНЕНИЯ В
СОЦИАЛЬНЫХ СЕТЯХ**

(заключительный)

Авенир

Главный инженер НИО-5,
ответственный исполнитель
М.А. Пендохов

2017

Нормоконтролёр

Н.И. Кузнецова

2017

Москва 2017

Picture 1: The cover page for the Avenir project¹¹

Fronton is the backend infrastructure of the social media disinformation platform and consists of several components. The primary purpose of the botnet is not to create Denial of Service attacks, but to lay groundwork for massively scalable coordinated inauthentic behavior. The fundamental component is the distributed transport system. This system consists of a layer of compromised IoT devices that communicate with front-end server infrastructure. These servers then pass their data over VPNs or the TOR network to back-end servers. While the system could not exist without this groundwork, it is not the focal point of the Fronton network. This base layer is then utilized by the SANA platform in order to coordinate inauthentic behavior and propagate disinformation at a global scale.

¹¹[https://static1.squarespace\[.\]com/static/5bdc659f7c9327ff92ac4233/5c19b1460ebbe870700591b0/5c19b14e4fa51a319da1ef82/1545187669608/2.1.png](https://static1.squarespace[.]com/static/5bdc659f7c9327ff92ac4233/5c19b1460ebbe870700591b0/5c19b14e4fa51a319da1ef82/1545187669608/2.1.png)

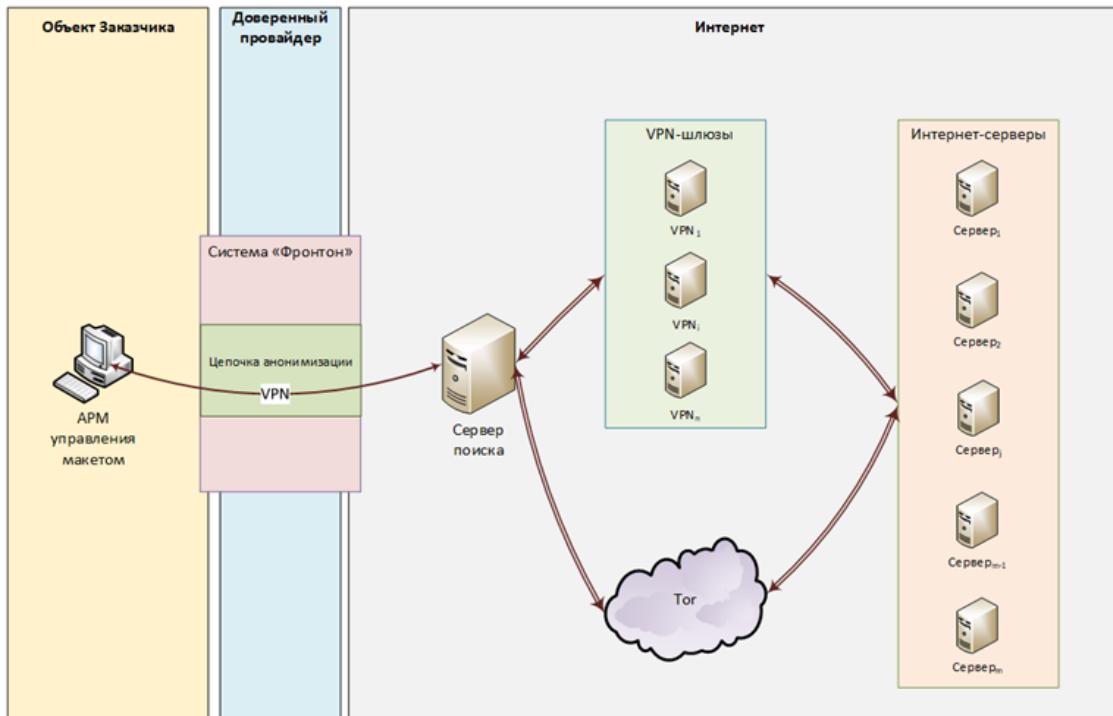


Рис. 1. Структурная схема макета

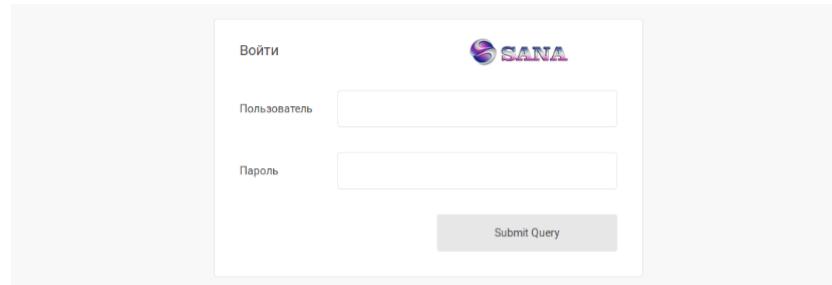
Picture 2: A Map of the Fronton Transport Network. The yellow is the “Customer Object” containing the “Network Control Workstation.” That traverses Fronton System VPN that goes to servers and into other VPNs or the TOR cloud to internet servers.¹²

SANA

Sana is the user interface to the social media disinformation platform. “Digital Revolution” released a video along with twenty other files, sixteen of which appear to be screenshots. The video, which they also released to Youtube, describes some of the steps taken when using the SANA user interface.¹³

¹²[https://images.squarespace-cdn\[.\]com/content/v1/5bdc659f7c9327ff92ac4233/1584446642686-KK1LSX5547FT3O1VECSL/ke17ZwdGBToddl8pDm48kEk5SweHS-JLcda0fJaTdKRZw-zPPgdn4jUwVcJE1ZvWQUxwkmyExgINqGp0lVTJZamWLI2zvYWH8K3-s_4yszcp2ryTl0HqTOaaUohrl8PITHi6P0XHNs93_Ym_Mu5HnCV-n8Xed7W8-fGEIGQxEm0/2.PNG](https://images.squarespace-cdn[.]com/content/v1/5bdc659f7c9327ff92ac4233/1584446642686-KK1LSX5547FT3O1VECSL/ke17ZwdGBToddl8pDm48kEk5SweHS-JLcda0fJaTdKRZw-zPPgdn4jUwVcJE1ZvWQUxwkmyExgINqGp0lVTJZamWLI2zvYWH8K3-s_4yszcp2ryTl0HqTOaaUohrl8PITHi6P0XHNs93_Ym_Mu5HnCV-n8Xed7W8-fGEIGQxEm0/2.PNG)

¹³ [https://www.youtube\[.\]com/watch?v=bATLEMoi_h0](https://www.youtube[.]com/watch?v=bATLEMoi_h0)



Picture 3: SANA Login Page

After the login page, the user is presented with the “Summary” page. The control menu is on the left side.



Picture 4: SANA Control Menu

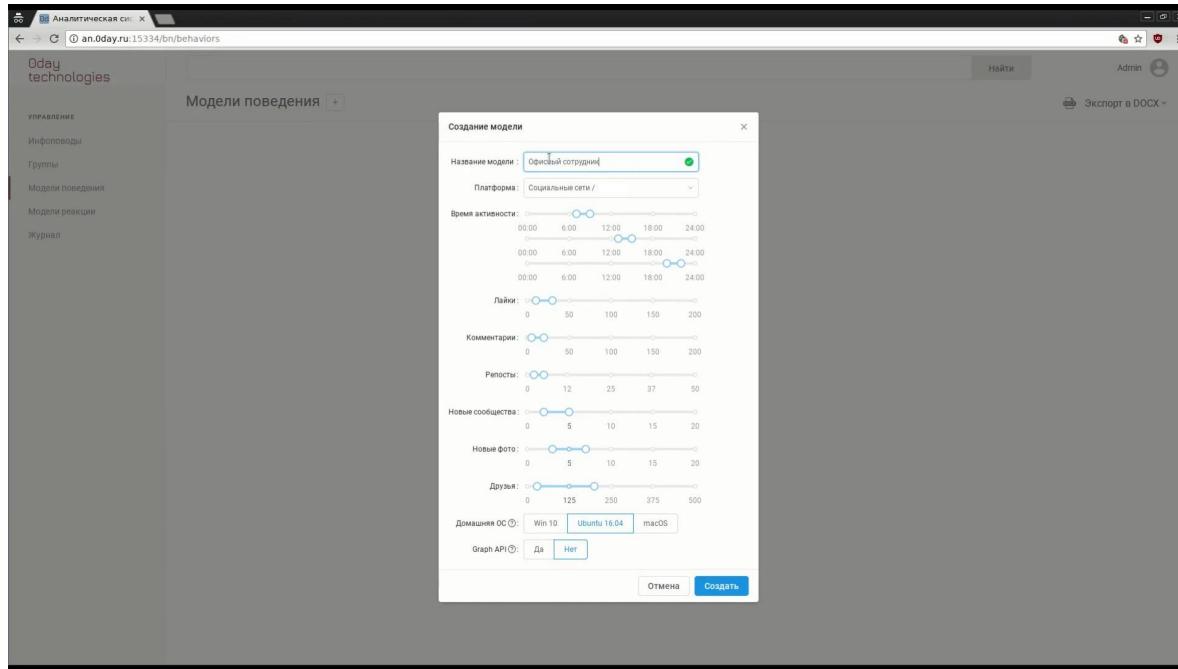
The video describes various aspects of the system:

- **Newsbreaks** tracks the occurrence of necessary messages at given sites and how to respond to them
- **Groups** implement flexible bulk management of bots
- **Behavior Models** sets up background bot activity which allows bots to be indistinguishable from normal users
- **Response Models** describes how to react to messages found
- **Dictionaries** stores and categorizes phrase-books, quotes, and comments for social media responses as positive, negative, and neutral influences based on topic. It also provides a location to store lists of names and surnames
- **Albums** allows maintenance of photograph sets for platform bot accounts.

The images released by “Digital Revolution” contain stills of a system that has been pre-populated with test botnet user Groups, Behavior Models, Response Models, and Newsbreaks.

Behavior Models

The video begins by showing the process of creating a behavior model.

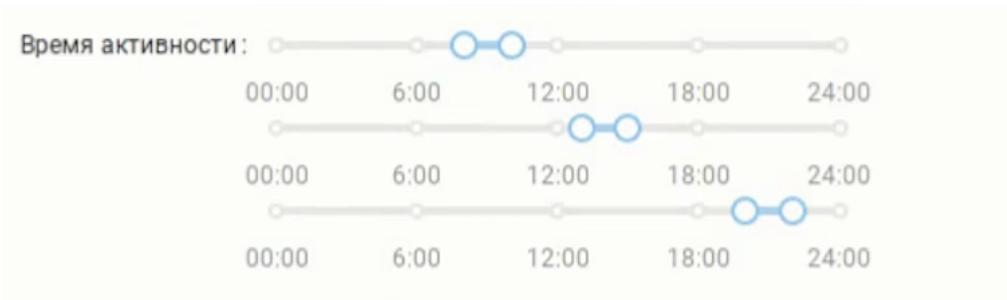


Picture 5: The Behavior Models have different settings based on platform

It indicates that the process differs depending on the supported platform. The supported platforms include:

- Social media (6 popular social media platforms)
- Blog Sites
- Media Sites
- Forums (various engines)
- Sites (various engines)

The Behavior Model creation process allows an operator to specify the times that bots associated with the model should be active.



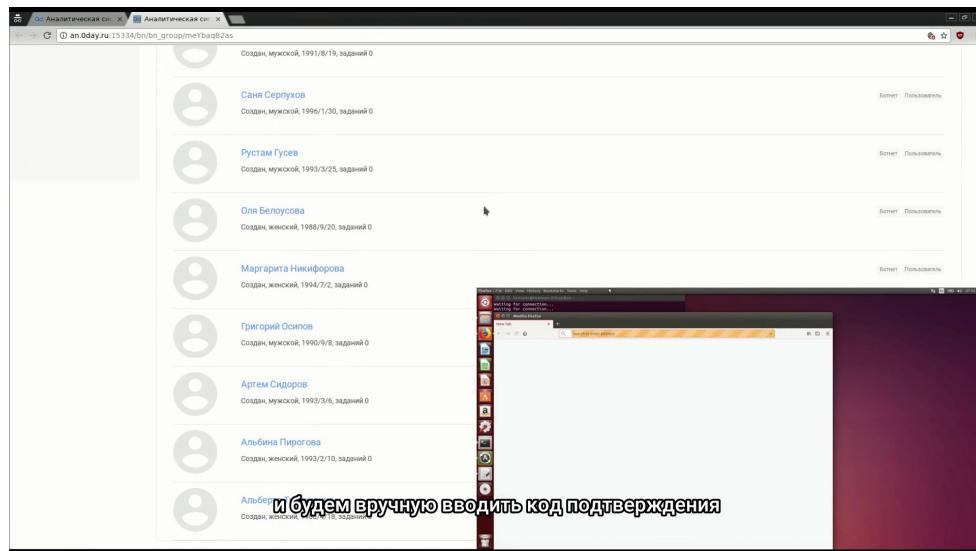
Picture 6: The Behavior model selector for the “Activity time” setting

It also allows an operator to configure how many likes, comments, and reactions a bot account should create, as well as how often it should create photos and interact with groups on a weekly basis. An operator can also specify a numeric range of the number of friends a bot should maintain.

In addition, the system specifies the OS that should be associated with the bot. The OS options indicated in the video include:

- Windows 10
- Ubuntu 16.04
- macOS

In the video, the operator creates a Behavior Group that runs on the Ubuntu operating system. Actions taken on a bot in this activity group indicate that a VirtualBox Virtual Machine is created for the user under which the automated actions occur. It is not clear if this capability also exists for the Windows and macOS options.



Picture 7: A list of real bot profiles. One has been chosen to be created and the OS is running in the foreground because the option to observe activity has been selected. The caption says “And we will enter the confirmation code manually”.

Newsbreaks

The screenshot displays two tables of newsbreaks data:

Источник	Инфоповод	Ссылка	Время	Текст	Количество*
engnews.kz	Астана	engnews.kz/boring-v-podderku-govornika-ostelli-yutodi-v-astane-353709/	2018-09-16T23:49:00	12 В поддерку Геннида Г...	1,00
engnews.kz	Астана	engnews.kz/kazakhstan_nevestkazakhstan/prityla-delegatuya-bentnalogo-352880/	2018-09-07T00:02:23	8 В Министерстве обороны Р...	1,00
zakon.kz	Астана	www.zakon.kz/39922_kommunashka_posh-domoy-k.html	2018-10-02T06:54:56	За текущий год инвентариза...	1,00
zakon.kz	Астана	www.zakon.kz/932750_turki-mozhet-porabotyati.html	2018-08-15T08:57:54	Не лучшие времена пережив...	1,00
zakon.kz	Астана	www.zakon.kz/31196_v-kirgizstanskoj-mangistaujskoj.html	2018-08-07T15:09:07	Все прокуроры состояли в П...	1,00
engnews.kz	Астана	engnews.kz/kazakhstan_nevestkazakhstan/poprost-horochina-naevet-poryadok-pravom-354199/	2018-09-24T11:59:39	3 Аким Астаны попросил ...	1,00
engnews.kz	Астана	engnews.kz/nauka-i-sreda/produga-za-773-fenge-v-otmenenii-354540/	2018-10-05T06:24:57	О допинге продукт в обише...	1,00
irk.kz	Астана	www.irk.kz/150170-kazhyne-zalidzenno-po-zapiske-na-nikolaev-berge-yuzhnyi-astana.html	2018-09-01T11:42:14	На исполнение китай ф...	1,00
engnews.kz	Астана	engnews.kz/zhigansk-act-welcomes-a-newly-created-352818/	2018-09-04T00:15:24	15 Курс начинаты составлен...	1,00
engnews.kz	Астана	engnews.kz/zhigansk-act-welcomes-a-newly-created-352818/	2018-09-04T00:15:24	15 Курс начинаты составлен...	1,00
irk.kz	Астана	www.irk.kz/759337_nazarmen-podstrel-nigmatova-k-din-aytoba.html	2018-09-17T00:23:37	13 и 14 октября 2018 года...	1,00
zakon.kz	Астана	www.zakon.kz/399111_v-kazaynene-vlenna-ekzamenu-10.html	2018-09-09T00:48:54	Указом Службы акимата...	1,00
zakon.kz	Астана	www.zakon.kz/932256_v-zameneno-objekt-medzina.html	2018-09-21T14:01:38	Касым-Жомарт Токаев...	1,00
engnews.kz	Астана	engnews.kz/zhigansk-act-welcomes-a-newly-created-352818/	2018-10-01T14:24:23	Время издачено пешебюро ...	1,00

Summary (Filtered) 1891.00 1 - 15 of 1001 Items

F B N Comment	Количество*
Summary	18 818.00

18 818.00 1 - 1 of 1 Items

Picture 8: SANA Summary Page

Newsbreaks appear to be the core of the system. The summary page lists the previously deployed newsbreaks, including the shared link source, shared link, release time, social media post text, and the quantity of posts. All of the posts in the images are dated in the 2018 timeframe. The observed summary page appears to show that there are 1891 posts total.

The screenshot shows a list of infopovody (infoprompts) from the SANA system:

Инфоповоды	Найти
testvk1	Быть: Инфоповод
Сибери Новосибирске, Мониторинг без реакции, событий: 0	
vk_3_users	Быть: Инфоповод
* Мониторинг без реакции, событий: 0	
vk_group	Быть: Инфоповод
* Мониторинг без реакции, событий: 0	
vk_user	Быть: Инфоповод
* Мониторинг без реакции, событий: 0	
vk_user2	Быть: Инфоповод
* Мониторинг без реакции, событий: 0	
Абенов доллар положительно	Быть: Инфоповод
Нацбанк курс долларов. Круглосуточно, событий: 0	
Астана	Быть: Инфоповод
Астана Astana. Весь день, событий: 0	

Picture 9: Newsbreaks Page

According to Russian email marketing firm, Email Soldiers, a **newsbreak** is an event that creates information “noise” around a brand or company and attracts media attention. They are the best way to create buzz about a topic of interest, because companies can come up with newsbreaks themselves at any time with little to no expense.¹⁴

Добавление инфоповода

Name	Название: Cyberpunk 2077 
Source Platform	Источник: Социальные сети / 
Source Group	stopgameteam
+ Добавить	
Keywords to react to	Шаблон: cyberpunk
	2077 
+ Добавить	
Beginning at (time)	Начиная с : 2018-06-20 05:06:07 
Reaction group/model	Реакция : Группа одобряющих 
	Выберите действие 
	Одобрение 
	Осуждение

Отмена
Создать

Picture 10: Newbreak creation dialogue

A named newsbreak can be configured on the system using the newsbreak creation dialogue. In this menu, an operator can choose the platform, and any subgroup on the platform to search for keywords.

14

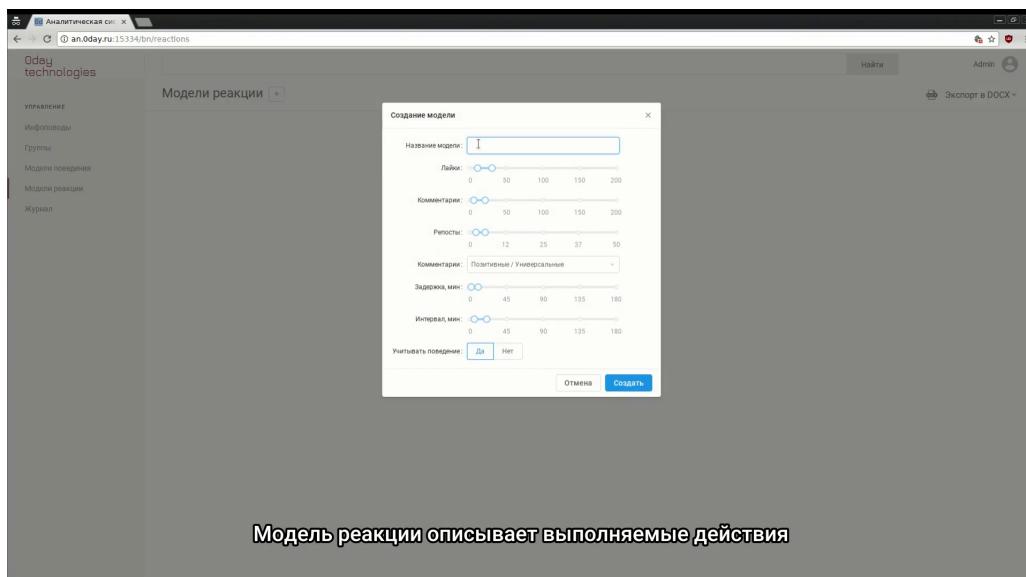
[https://emailsoldiers\[.\]ru/glossary/newseworthy#:~:text=%D0%98%D0%BD%D1%84%D0%BE%D0%BF%D0%BE%D0%B2%D0%BE%D0%B4%20%E2%80%94%20%D1%8D%D1%82%D0%BE%20%D0%BD%D0%B5%20%D0%BF%D1%80%D0%BE%20%D0%B7%D0%B0%D0%BA%D1%83%D0%BF%D0%BA%D1%83,%D0%BA%D0%BE%D1%82%D0%BE%D1%80%D1%8B%D0%B5%20%D0%BF%D1%80%D0%BE%D0%BD%D0%B8%D0%BA%D0%B0%D1%8E%D1%82%20%D0%B2%D0%A1%D0%9C%D0%98%20%D0%B1%D0%BD%D1%81%D0%BF%D0%BB%D0%B0%D1%82%D0%BD%D0%BE](https://emailsoldiers[.]ru/glossary/newseworthy#:~:text=%D0%98%D0%BD%D1%84%D0%BE%D0%BF%D0%BE%D0%B2%D0%BE%D0%B4%20%E2%80%94%20%D1%8D%D1%82%D0%BE%20%D0%BD%D0%B5%20%D0%BF%D1%80%D0%BE%20%D0%B7%D0%B0%D0%BA%D1%83%D0%BF%D0%BA%D1%83,%D0%BA%D0%BE%D1%82%D0%BE%D1%80%D1%8B%D0%B5%20%D0%BF%D1%80%D0%BE%D0%BD%D0%B8%D0%BA%D0%B0%D1%8E%D1%82%20%D0%B2%D0%A1%D0%9C%D0%98%20%D0%B1%D0%BD%D1%81%D0%BF%D0%BB%D0%B0%D1%82%D0%BD%D0%BE).

The system then reacts after a given date/time and selects a group of botnet users with which to react positively, negatively or indifferently using one of the predefined reaction models.

Once a newsbreak is defined, the Newsbreaks page lists existing newsbreaks. Many of those observed identify the platform targeted by the newsbreaks.

Response Models

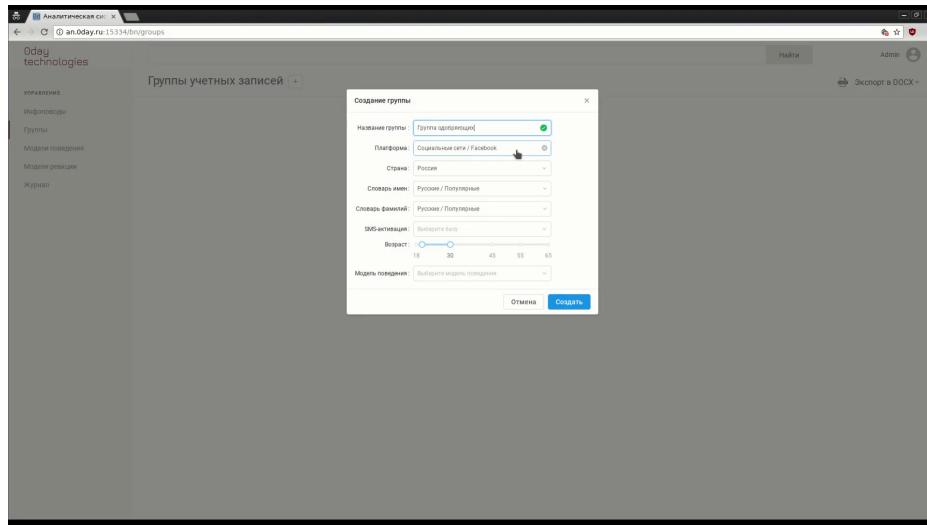
The Response Model specifies the actions to be performed after the instantiation or execution of a Newsbreak. This allows a group or groups of bots to exist for the purpose of reacting to news in a positive, negative, or neutral fashion, but not necessarily creating or sharing news.



Picture 11: The Response Models also have configurable settings.

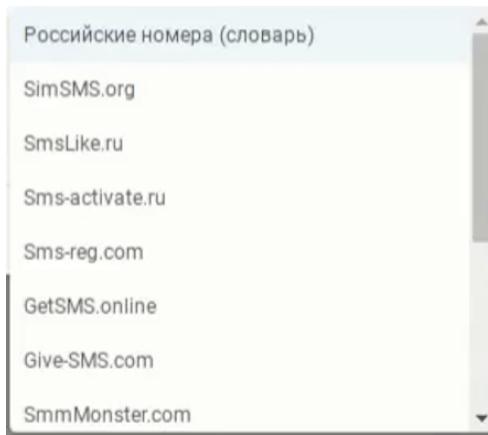
The Response Model allows an operator to specify weekly frequency of likes, comments, and reposts. It also allows for the selection of comments from the dictionary lists in order to direct the response patterns of the virtual social group. The configurator also allows the operator to specify a minimum frequency of actions, and a minimum interval between actions. It also appears that there is a machine learning (ML) system involved that can be turned on or off based on behavior observed on social media.

Groups



Picture 12: The Group creation dialogue

Groups are auto-generated sets of accounts created by the system that are organized by platform and country. The operator can choose from a list of names and a dictionary of surnames. The operator can then select the SMS API platform to use in order to create a phone number to automatically respond to two-factor authentication requests and other platform text requests. Nisos observed 7 services used by the platform, but only two thirds of the list of services was displayed on the video. The system can then be triggered to auto-generate any number of accounts in a group at the click of a button.



Picture 13: SMS services supported via API by SANA

Other Files

In the SANA files available to Nisos was a text file titled “NUR_OTAN_Positive.” It contained numerous one to two sentence snippets of text expressing support for the Nur Otan political party in Kazakhstan. Nuro Otan [meaning “Radiant Fatherland”] has been the ruling party in Kazakhstan since 1999 and was led by Nursultan Nazarbayev until January 2022. Nazarbayev was president of Kazakhstan from 1990 to 2019 and was Chairman of the Security Council of Kazakhstan until January 2022.¹⁵¹⁶

Examples of these snippets translated into English are:

- Now in the state many reforms are being carried out, and the Nur Otan party takes an active part in this. This makes me happy
- The country’s main party actively participates in the political life of Kazakhstan. We are with you!
- The facts speak for themselves. Decent and stable.
- Nur Otan changes lives and destinies! Thank you for being Nur Otan.
- Well done! Really reasonable.
- The future of our nation is in the hands of Nur Otan.
- We want more of these parties.
- Forward and only forward. Make our country more and more beautiful.
- The party may not be able to do everything in a row, but the result is definitely better than everyone else’s.

Another text file, titled “squirrel negative,” contained a list of negative phrases criticizing the installation in July 2018 of a large wooden squirrel sculpture in Kazakhstan that was partly financed with public funds. The phrases sometimes aim their derision at “Baibek,” a reference to Bauyrjan Baibek, the mayor of Almaty. It appears that criticism of the sculpture made it into a BBC report on the issue.¹⁷ It is unclear whether any of the Russian disinformation influenced that report.¹⁸

Examples of these phrases translated into English are:

- How much can you spend on pseudo-art
- It would be better to give this money to orphanages
- Is the squirrel a new symbol of Kazakhstan ?!
- Why do we need this one-time installation?
- Guys, you have nowhere to spend money ?!
- I’m Shocked! How so ?! Baibek does what he wants.
- Think of something more original.
- This is not the case! I’m going into a coma. Wake up when everything is fine. That is, never.

¹⁵https://en.wikipedia.org/wiki/Nur_Otan

¹⁶https://en.wikipedia.org/wiki/Nursultan_Nazarbayev

¹⁷ <https://www.bbc.com/news/world-asia-44792722>

¹⁸ https://en.wikipedia.org/wiki/Bauyrjan_Baibek

- People, don't scold Baybek. All the same, art promotes (sarcasm)
- The government has gone wild. Give money back to the people.
- What kind of art is this? Where do you see art?
- Squirrel. Are you serious???
- Why so much money for one squirrel ?!
- I am certainly not an art critic, but this is definitely not an art object.
- It does not even need to be taken to a landfill, you can immediately set it on fire. Less garbage and less work.
- This squirrel will fall apart before winter. And why a squirrel! ?! It's not clear at all.
- Oh yes Baibek, oh yes well done.

Another file titled aerospike_vk.txt contains the output of a NoSQL query of approximately 644 VK accounts on an aerospike server. Nisos assesses that this portion of the SANA database is used for monitoring social media posts as well as staging coordinated inauthentic behavior. Data included in the lists reflects data observed in other screenshots from the system.

The VK accounts identified in the the aerospike_vk.txt file appear to be real social media accounts. Many of these accounts appear to share a common interest in white-water rafting, kayaking, and similar water sports. Nisos assesses that these accounts may belong to social media interest groups monitored and influenced by the inauthentic account group clusters.

АККАУНТЫ	ИНФОПОВОДЫ	ЗАДАНИЯ ПЛАТФОРМЫ	ВНЕШНИЕ ЗАДАНИЯ	ЖУРНАЛ
	Адиль Баймуратов Заблокирован, мужской, 1991/10/4, тел. +778405897, новых заданий 0			Ботнет Пользователь
	Адиль Сарсөнов Сервисный аккаунт, мужской, 1994/8/28, тел. +77052489403, новых заданий 0			Ботнет Пользователь
	Айдана Бабаева Зарегистрирован, женский, 1997/4/5, тел. +77762133512, новых заданий 1			Ботнет Пользователь
	Айнур Алмасова Сервисный аккаунт, женский, 1996/2/21, тел. +77051958637, новых заданий 0			Ботнет Пользователь
	Аксултан Сапарбеков Создан, мужской, 1991/1/6, тел. не задан, новых заданий 2			Ботнет Пользователь
	Алим Габдуллин Статус неизвестен (reg_failed), мужской, 1991/8/1, тел. +77071346569, новых заданий 2			Ботнет Пользователь
	Алмаз Абдрашев			Ботнет Пользователь

Picture 14: An bot account group of VK accounts. The group data indicates the platform, country, and model in use for the group. Individual account data listed includes current photo, account status, gender, date of birth, phone number, country, and number of tasks assigned. On the right, these users have indicators set that they are "Botnet User"

0DAY TECHNOLOGIES

0Dt, full name Zeroday Technologies LLC (0Дт, ООО ЗИРОУДЭЙ ТЕХНОЛОДЖИС, Tax ID Number: 7728795098)¹⁹ is a technology company that “specializes in the development of automation and information protection tools.”²⁰ The company was founded in 2011 by Ruslan Radjabovich GILYAZOV, who is on the Information Security faculty at Moscow State University and has published and spoken on topics related to information security, malware, and blockchain security.²¹ In addition to the SANA technology, 0Dt has spent significant effort developing technologies for Russian lawful intercept applications, technologies known as SORM, which they tout on their website as some of their premier capabilities. In a letter written to the Russian state Telecom firm, Rostelecom, GILYAZOV complained about not getting any traction from the firm, who try to develop everything internally. He mentions contracts his company has with the FSB Center 18, the customer of the Fronton/SANA system, and Center 12, the developers and certifiers of SORM-related equipment²².

Nisos investigated other employees of 0Dt and discovered a LinkedIn profile for Pavel SITNIKOV, currently working as a Systems Analyst at 0Dt, LLC. SITNIKOV is a prominent figure of the hacking underground who, under the alias FlatL1ne, brags about his connections to Russian hacking group APT28 aka Fancy Bear. He manages the Telegram group freedomf0x²³, where he shares data leaks, educational materials, and software used for security and penetration testing. In June 2020, he shared a link on Twitter to a sizable archive of leaked data that allegedly consisted of information on hundreds of police departments and fusion centers—his Twitter account is currently suspended.²⁴ SITNIKOV may have been involved in the December 2020 leaking of Musovites who had undergone COVID-19 treatment.²⁵ He is a member of multiple underground communities where he has a history of selling and sharing multiple malware source codes on the dark web, including banking and spam trojans.²⁶ SITNIKOV was arrested in 2021 by Russian authorities on charges of distributing malware via his Telegram channel.^{27 28}

¹⁹ The Russian phonetic spelling of Zeroday Technologies

²⁰ [https://0day\[.\]llc](https://0day[.]llc)

²¹

[https://scholar.google\[.\]com/scholar?hl=en&as_sdt=0%2C47&q=%D0%93%D0%98%D0%9B%D0%AF%D0%97%D0%9E%D0%92%D0%A0%D0%A3%D0%A1%D0%9B%D0%90%D0%9D+%D0%A0%D0%90%D0%94%D0%96%D0%90%D0%91%D0%9E%D0%92%D0%98%D0%A7&btnG=](https://scholar.google[.]com/scholar?hl=en&as_sdt=0%2C47&q=%D0%93%D0%98%D0%9B%D0%AF%D0%97%D0%9E%D0%92%D0%A0%D0%A3%D0%A1%D0%9B%D0%90%D0%9D+%D0%A0%D0%90%D0%94%D0%96%D0%90%D0%91%D0%9E%D0%92%D0%98%D0%A7&btnG=)

²² [https://swinopes.livejournal\[.\]com/655200.html](https://swinopes.livejournal[.]com/655200.html)

²³ [https://t\[.\]me/s/freedomf0x](https://t[.]me/s/freedomf0x)

²⁴ <https://therecord.media/an-interview-with-russian-hacker-pavel-sitnikov-there-is-no-hacking-scene-now-only-commerce/>

²⁵ <https://en.newizv.ru/news/politics/10-12-2020/people-who-are-ill-in-public-vast-databases-of-moscow-covid-patients-leaked-online>

²⁶ [https://therecord\[.\]media/an-interview-with-russian-hacker-pavel-sitnikov-there-is-no-hacking-scene-now-only-commerce/](https://therecord[.]media/an-interview-with-russian-hacker-pavel-sitnikov-there-is-no-hacking-scene-now-only-commerce/)

²⁷ [https://securityaffairs\[.\]co/wordpress/118464/cyber-crime/pavel-sitnikov-arrested.html](https://securityaffairs[.]co/wordpress/118464/cyber-crime/pavel-sitnikov-arrested.html)

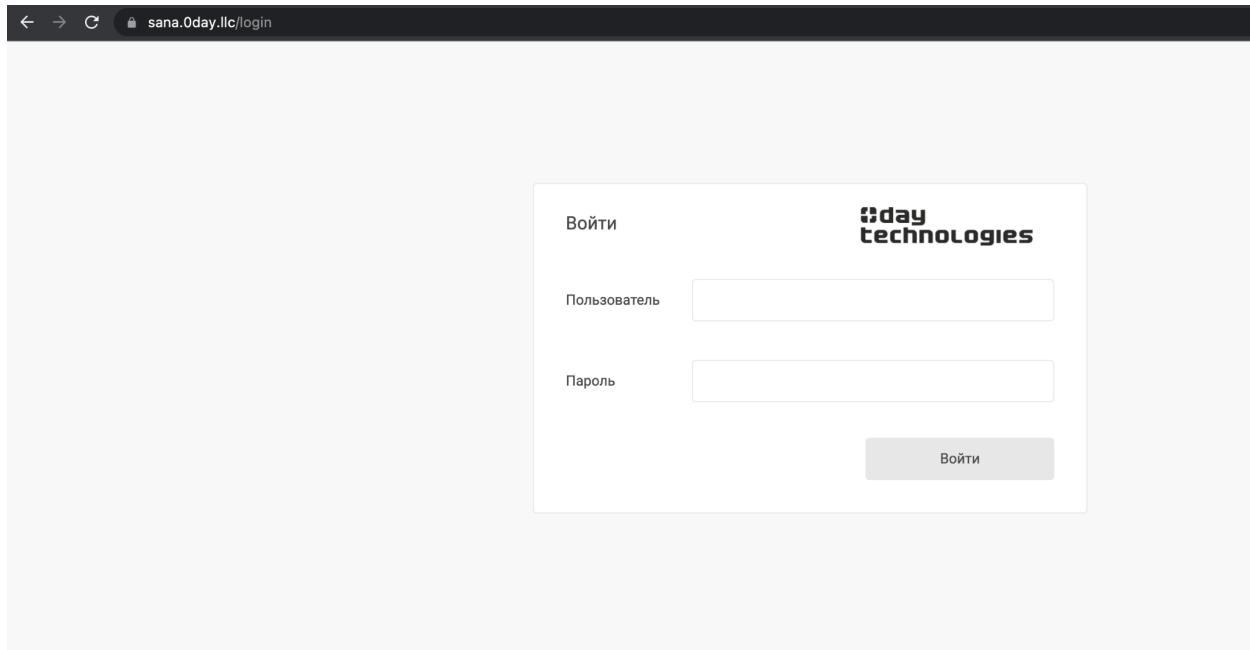
²⁸ <https://twitter.com/campuscodi/status/1399487674315153413?lang=en>

Picture 15: LinkedIn Profile of Pavel Sitnikov, alias FlatLine²⁹

CURRENT STATUS OF SANA

As of April 2022, 0day technologies has moved their domain to 0day[.]llc. An instance of a SANA login page appears to exist at sana.0day[.]llc. The title of the page is **аналитическая система**, which means Analytical System.

²⁹[linkedin\[.\]com/in/pavel-sitnikov31337](https://linkedin[.]com/in/pavel-sitnikov31337)

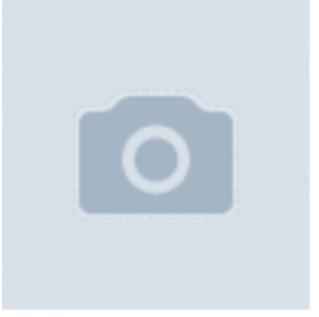


Picture 16: Current page at sana.0day[.]llc. The title of the page is **аналитическая система, Analytical System**

APPENDIX A: VK ACCOUNTS USED BY SANA

All identified accounts are residents of Kazakhstan.

Photo	Name	Handle	Sex	VK ID
	Азамат Алдаберген	id498242801	MALE	498242801
	Ербол Жаным	id498261632	MALE	498261632
	Женя Тё	id498426155	MALE	498426155

	Нариман Оспанов	id498402847	MALE	498402847
	Русик Ондаш	id498273535	MALE	498273535
	Руслан Сайдов	id498424584	MALE	498424584
	Света Светлова	dttwwmmadjg.a djjgptm	FEMALE	498297646

	Теймур Музаков	id498332685	MALE	498332685
	DELETED	id498255042	FEMALE	498255042
	DELETED	id498487612	MALE	498487612