Operation Texonto: Information operation targeting Ukrainian speakers in the context of the war

ESET Research, Ukraine Crisis – Digital Security Resource Center

A mix of PSYOPs, espionage and … fake Canadian pharmacies!

Matthieu Faou

21 Feb 2024 • , 14 min. read

ESET products and research have been protecting Ukrainian IT infrastructure for years. Since the start of the war in February 2022, we have prevented and investigated a significant number of attacks launched by Russia-aligned groups. We have also published some of the most interesting findings on WeLiveSecurity:

Even though our main focus remains on analyzing threats involving malware, we have found ourselves investigating an information operation or psychological operation (PSYOP) trying to raise doubts in the minds of Ukrainians and Ukrainian speakers abroad.

Operation Texonto

Operation Texonto is a disinformation/PSYOP campaign using spam mails as the main distribution method. Surprisingly, it doesn't seem that the perpetrators used common channels such as Telegram or fake websites to convey their messages. We have detected two different waves, the first one in November 2023 and the second one at the end of December 2023. The contents of the emails were about heating interruptions, drug shortages, and food shortages, which are typical themes of Russian propaganda.

In addition to the disinformation campaign, we have detected a spearphishing campaign that targeted a Ukrainian defense company in October 2023 and an EU agency in November 2023. The goal of both was to steal credentials for Microsoft Office 365 accounts. Thanks to similarities in the network infrastructure used in these PSYOPs and phishing operations, we are linking them with high confidence.

Interestingly, a few more pivots also revealed domain names that are part of Operation Texonto and related to internal Russian topics such as Alexei Navalny, the well-known Russian opposition leader who was in jail and died on February 16th, 2024. This means that Operation Texonto probably includes spearphishing or information operations targeting Russian dissidents and supporters of the late opposition leader. Those domains include:

- navalny-votes[.]net
- navalny-votesmart[.]net
- navalny-voting[.]net

Perhaps even stranger is that an email server, operated by the attackers and used to send PSYOP emails, was reused two weeks later to send typical Canadian pharmacy spam. This category of illegal business has been very popular within the Russian cybercrime community for a long time, as this blogpost from 2011 explains.

Figure 1 summarizes the main events of Operation Texonto.

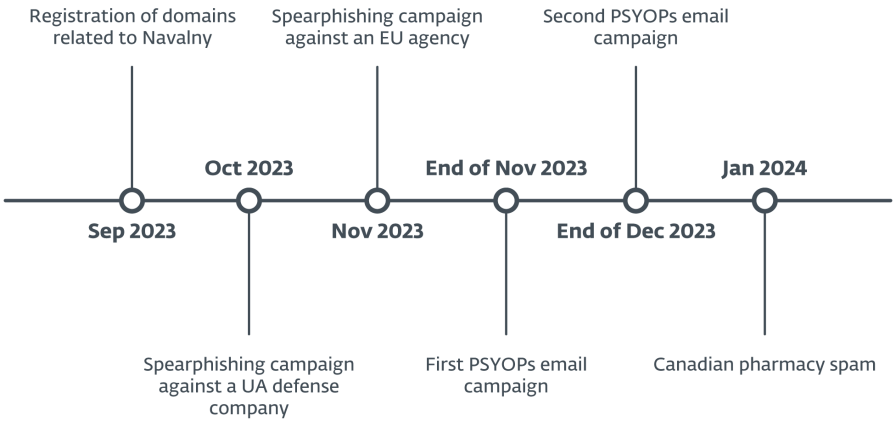


Figure 1. Timeline of Operation Texonto

The strange brew of espionage, information operations, and fake pharma can only remind us of Callisto, a well-known Russia-aligned cyberespionage group who was the subject of an indictment by the US DOJ in December, 2023. Callisto targets government officials, people in think tanks, and military-related organizations via spearphishing websites designed to mimic common cloud providers. The group has also run disinformation operations such as a document leak just ahead of the 2019 UK general election. Finally, pivoting on its old network infrastructure leads to fake pharma domains such as musclepharm[.]top or ukrpharma[.]ovh.

While there are several high-level points of similarity between Operation Texonto and Callisto operations, we haven't found any technical overlap and we currently do not attribute Operation Texonto to a specific threat actor. However, given the TTPs, targeting, and the spread of messages, we attribute the operation with high confidence to a group that is Russian aligned.

Phishing campaign: October–November 2023

Employees working at a major Ukrainian defense company received a phishing email in October 2023, purportedly coming from their IT department. The emails were sent from it.[redacted_company_name]@gmail.com, an email address most likely created specifically for this campaign, and the email subject was Запрошено утверждение:Планова інвентаризація (machine translation from Ukrainian: Approval requested: Planned inventory).

The content of the email is the following:

> У період з 02 жовтня по 13 жовтня співробітники відділу інформаційних технологій проводять планову інвентаризацію та видалення поштових скриньок, що не використовуються. Якщо Ви плануєте використовувати свою поштову адресу ([redacted_address]@[redacted_company_name].com) у майбутньому, будь ласка, перейдіть на веб-версію поштової скриньки за цим посиланням та увійдіть до системи, використовуючи свої облікові дані.
>
> Жодних додаткових дій не потрібно, Ваша поштова скринька отримає статус "підтверджений" і не буде видалена під час планової інвентаризації ресурсів. Якщо ця поштова адреса не використовується Вами (або її використання не планується в майбутньому), то в цьому випадку Вам не потрібно виконувати жодних дій - поштову скриньку буде видалено автоматично 13 жовтня 2023 року.
>
> З повагою,
>
> Відділ інформаційних технологій.

A machine translation of the email is:

> *In the period from October 2 to October 13, employees of the information technology department will conduct a planned inventory and removal of unused mailboxes. If you plan to use your email address ([redacted_address]@[redacted_company_name].com) in the future, please go to the web version of the mailbox at this link and log in using your credentials.*
>
> *No additional actions are required, your mailbox will receive the status "confirmed" and will not be removed during a scheduled resource inventory. If this email address is not used by you (or its use is not*

planned in the future), then in this case you do not need to take any action - the mailbox will be deleted automatically on October 13, 2023.

Best regards,

Department of information technologies.

The goal of the email is to entice targets into clicking on за цим посиланням (machine translation: at this link), which leads to https://login.microsoftidonline[.]com/common/oauth2/authorize?client_id=[redacted];redirect_uri=https%3a%2f%2foutlook.office365.com%2fowa%2f&resource=[redacted]&response_mode=form_post&response_type=code+id_token&scope=openid&msafed=1&msaredir=1&request-id=[redacted]&protectedtoken=true&claims=%7b%22id_token%22%3a%7b%22xms_cc%22%3a%7b%22values%22%3a%5b%22CP[redacted]&nonce=[redacted]&state=[redacted] (partially redacted). This URL points to the malicious domain login.microsoft**id**online[.]com. Note that this domain is very close to the official one, login.microsoftonline.com.

We haven't been able to retrieve the phishing page, but it was most likely a fake Microsoft login page intended to steal the targets' credentials.

For another domain belonging to Operation Texonto, choicelive149200[.]com, there were two VirusTotal submissions (one and two) for the URL https://choicelive149200[.]com/owa/auth/logon.aspx?replaceCurrent=1&url=https://hbd.eupolcopps.eu/owa/. Unfortunately, the site was no longer reachable at the time of analysis, but it was likely a credential-phishing page for the Outlook on the web/OWA webmail of eupolcopps.eu, the EU Coordinating Office for Palestinian Police Support. Note that we have not seen the email sample, just the URL submitted to VirusTotal.

First PSYOP wave: November 2023

On November 20th, we detected the first wave of disinformation emails with a PDF attachment sent to at least a few hundred recipients in Ukraine. People working at the Ukrainian government, energy companies, and even individuals, received the emails. We do not know how the list of email addresses was built.

Contrary to the previously described phishing campaign, the goal of these emails was to sow doubt in the mind of Ukrainians; for instance, one email says that "There may be heating interruptions this winter". It doesn't seem there was any malicious link or malware in this specific wave, only disinformation.

Figure 2 shows an email example. Its subject is Рекомендації моз україни на тлі дефіциту ліків (machine translation from Ukrainian: Recommendations of the Ministry of Health of Ukraine at the time of a shortage of medicines) and the email was sent from mozua@ua-minagro[.]com. Note that this address can be seen in the envelope-from and return-path fields.

ua-minagro[.]com is a domain operated by the attackers and was used exclusively for sending disinformation emails in this campaign. The domain is masquerading as the Ministry of Agrarian Policy and Food of Ukraine whose legitimate domain is minagro.gov.ua.

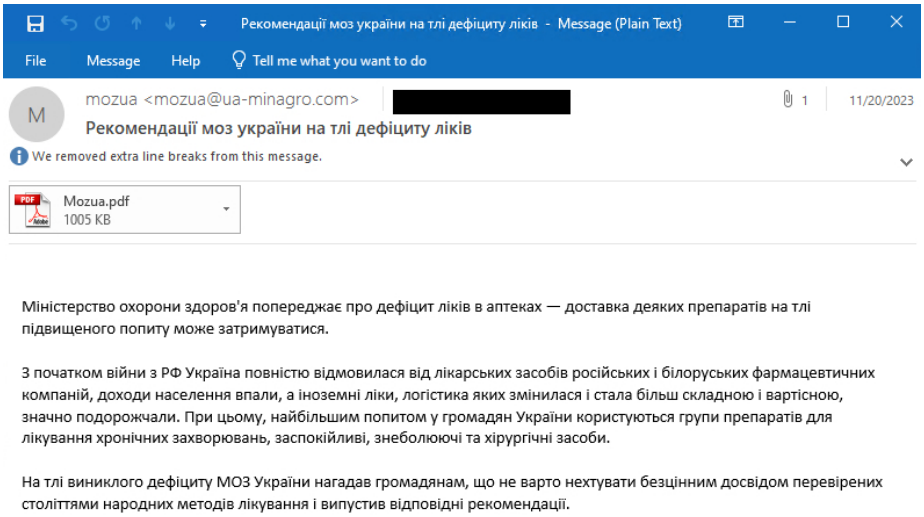


Figure 2. Disinformation email

Attached to the email is a PDF document, as shown in Figure 3. While it is not malicious per se, it also contains disinformation messages.

МІНІСТЕРСТВО ОХОРОНИ ЗДОРОВ'Я УКРАЇНИ

РЕКОМЕНДАЦІЇ МОЗ УКРАЇНИ НА ТЛІ ДЕФІЦИТУ ЛІКІВ

Міністерство охорони здоров'я попереджає про дефіцит ліків в аптеках — доставка деяких препаратів на тлі підвищеного попиту може затримуватися.

З початком війни з РФ Україна повністю відмовилася від лікарських засобів російських і білоруських фармацевтичних компаній, доходи населення впали, а іноземні ліки, логістика яких змінилася і стала більш складною і вартісною, значно подорожчали. При цьому, найбільшим попитом у громадян України користуються групи препаратів для лікування хронічних захворювань, заспокійливі, знеболюючі та хірургічні засоби.

На тлі виниклого дефіциту МОЗ України нагадав громадянам, що не варто нехтувати безцінним досвідом перевірених століттями народних методів лікування і випустив відповідні рекомендації.

МІНІСТЕРСТВО ОХОРОНИ ЗДОРОВ'Я УКРАЇНИ

ПАМ'ЯТКА З НАРОДНОЇ МЕДИЦИНИ

При підвищеній тривожності, безсонні

Звіробій допоможе відновити захисні сили організму-ця рослина ефективно бореться з вірусами і бактеріями. Звіробій здатний підвищувати тиск, лібідо. Настій звіробою ефективний при післяпологових депресіях. Але рослина протипоказана людям з підвищеним тиском і особливою чутливістю шкіри до сонячних променів.

Конопля має заспокійливий ефект, який ідеально підходить для зняття болю і стресу. Коноплю можна вживати в якості чаю, для чого необхідно залити 0,5 грама бруньок конопель склянкою гарячої води, додати ½ чайної ложки вершкового масла, меду і чайний пакетик (будь-якого сорту чаю). При сильних стресах коноплю можна вживати наступним чином. Вам знадобиться 1,5-2 кг дикої конопель, столова ложка соди без гірки, банку згущеного молока, 2 літри молока ~3% жирності і близько півлітра води (додається в процесі, щоб не тікало молоко). Всі інгредієнти необхідно змішати в 5-літровій каструлі і варити близько 30-40 хвилин. Не забувайте помішувати і при необхідності додавати води, дуже важливо, щоб молоко не пригоріло. Після варіння коноплю необхідно віджати, отриману рідину процідити і вживати всередину в кількості не більше 200 мл.за один прийом.

Figure 3. PDF attachment

The document is misusing the logo of the Ministry of Health of Ukraine and explains that due to the war, there is a drug shortage in Ukraine. It also says that the Ukrainian government is refusing to import drugs from Russia and Belarus. On the second page, they explain how to replace some drugs with plants.

What's interesting to note is that the email was sent from a domain masquerading as the Ministry of Agrarian Policy and Food of Ukraine, while the content is about drug shortages and the PDF is misusing the logo of the Ministry of Health of Ukraine. It is possibly a mistake from the attackers or, at least, shows they did not care about all details.

In addition to ua-minagro[.]com, five additional domains were used to send emails in this wave:

- uaminagro[.]com
- minuaregion[.]org
- minuaregionbecareful[.]com
- uamtu[.]com
- minagroua[.]org

minuaregion[.]org and minuaregionbecareful[.]com are masquerading as the Ministry of Reintegration of the Temporarily Occupied Territories of Ukraine whose legitimate website is https://minre.gov.ua/en/.

uamtu[.]com is masquerading as the Ministry of Development of Communities, Territories and Infrastructure of Ukraine, whose legitimate website is https://mtu.gov.ua.

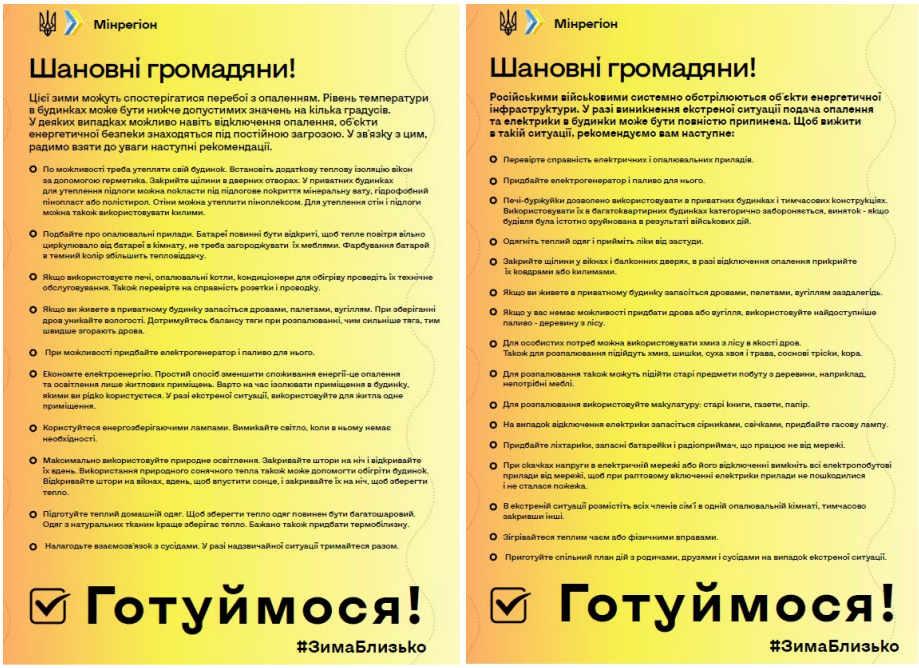
We have identified three more different email message templates, each with a different mail body and PDF attachment. A summary is provided in Table 1.

Table 1. Disinformation emails

Email body	Machine translation of the email body
Російськими військовими системно обстрілюються об'єкти енергетичної інфраструктури. У разі виникнення екстреної ситуації подача опалення та електрики в будинки може бути повністю припинена. Щоб вижити в такій ситуації, рекомендуємо вам наступне:	The Russian military is systematically shelling the energy facilities infrastructure. Heating supply in case of an emergency and electricity to homes may be completely cut off. To survive in such a situation, we recommend the following:
Цієї зими можуть спостерігатися перебої з опаленням. Рівень температури в будинках може бути нижче допустимих значень на кілька градусів. У деяких випадках можливо навіть відключення опалення, об'єкти енергетичної безпеки знаходяться під постійною загрозою. У зв'язку з цим, радимо взяти до уваги наступні рекомендації.	There may be heating interruptions this winter. Temperature level in houses can be several degrees below the permissible values. In some cases, it is even possible to turn off the heating, facilities energy security are under constant threat. In this regard, we advise you to take into account the following recommendations.

Email body	Machine translation of the email body
Міністерство охорони здоров'я попереджає про дефіцит ліків в аптеках — доставка деяких препаратів на тлі підвищеного попиту може затримуватися. З початком війни з РФ Україна повністю відмовилася від лікарських засобів російських і білоруських фармацевтичних компаній, доходи населення впали, а іноземні ліки, логістика яких змінилася і стала більш складною і вартісною, значно подорожчали. При цьому, найбільшим попитом у громадян України користуються групи препаратів для лікування хронічних захворювань, заспокійливі, знеболюючі та хірургічні засоби. На тлі виниклого дефіциту МОЗ України нагадав громадянам, що не варто нехтувати безцінним досвідом перевірених століттями народних методів лікування і випустив відповідні рекомендації.	The Ministry of Health warns of a shortage of medicines in pharmacies — delivery of some drugs against the background of increased demand may be delayed. With the beginning of the war with the Russian Federation, Ukraine completely refused Russian and Belarusian pharmaceutical drugs companies, incomes of the population fell, and foreign medicines, the logistics of which changed and became more complex and expensive, significantly became more expensive. At the same time, the greatest demand is from citizens. Ukraine uses groups of drugs for the treatment of chronic diseases, sedatives, pain relievers and surgical means. Against the background of the shortage, the Ministry of Health of Ukraine reminded citizens that you should not neglect the invaluable experience of the tested centuries of folk methods of treatment and released the appropriate ones recommended.
Агресія Росії призвела до значних втрат в аграрному секторі України. Землі забруднені мінами, пошкоджені снарядами, окопами і рухом військової техніки. У великій кількості пошкоджено та знищено сільськогосподарську техніку, знищено зерносховища. До стабілізації обстановки Міністерство аграрної політики та продовольства рекомендує вам урізноманітнити раціон стравами з доступних дикорослих трав. Вживання свіжих, соковитих листя трав у вигляді салатів є найбільш простим, корисним і доступним. Пам'ятайте, що збирати рослини слід далеко від міст і селищ, а також від жвавих трас. Пропонуємо вам кілька корисних і простих у приготуванні рецептів.	Russia's aggression led to significant losses in the agricultural sector of Ukraine. The lands are polluted by mines, damaged by shells, trenches, and the movement of military equipment. A large amount of agricultural machinery was damaged and destroyed, and granaries were destroyed. Until the situation stabilizes, the Ministry of Agrarian Policy and Food recommends diversifying your diet with dishes made from available wild herbs. Eating fresh, juicy leaves of herbs in the form of salads is the most simple, useful, and affordable. Remember that you should collect plants far from cities and towns, as well as from busy roads. We offer you several useful and easy-to-prepare recipes.

The related PDF attachments are allegedly from the Ukrainian Ministry of Regions (see Figure 4) and the Ministry of Agriculture (see Figure 5).



Мінрегіон

Шановні громадяни!

Цієї зими можуть спостерігатися перебої з опаленням. Рівень температури в будинках може бути нижче допустимих значень на кілька градусів. У деяких випадках можливо навіть відключення опалення, об'єкти енергетичної безпеки знаходяться під постійною загрозою. У зв'язку з цим, радимо взяти до уваги наступні рекомендації.

- По можливості треба утеплити свій будинок. Встановіть додаткову теплозу ізолюцію вікон за допомогою герметика. Закрийте щілини в дверних отворах. У приватних будинках для утеплення підлоги можна покласти під підлогове покриття мінеральну вату, гідрофобний пінопласт або полістирол. Стіни можна утеплити піноплексом. Для утеплення стін і підлоги можна також використовувати килими.
- Подбайте про опалювальні прилади. Батареї повинні бути відкриті, щоб тепле повітря вільно циркулювало від батареї в кімнату, не треба загороджувати їх меблями. Фарбування батарей в темний колір збільшить тепловіддачу.
- Якщо використовуєте печі, опалювальні котли, кондиціонери для обігріву проведіть їх технічне обслуговування. Також перевірте на справність розетки і проводку.
- Якщо ви живете в приватному будинку запасіться дровами, палетами, вугіллям. При зберіганні дров уникайте вологості. Дотримуйтесь балансу тяги при розпалюванні, чим сильніше тяга, тим швидше згорають дрова.
- При можливості придбайте електрогенератор і паливо для нього.
- Економте електроенергію. Простий спосіб зменшити споживання енергії-це опалення та освітлення лише житлових приміщень. Варто на час ізолювати приміщення в будинку, якими ви рідко користуєтеся. У разі екстреної ситуації, використовуйте для життя одне приміщення.
- Користуйтеся енергозберігаючими лампами. Вимикайте світло, коли в ньому немає необхідності.
- Максимально використовуйте природне освітлення. Закривайте штори на ніч і відкривайте їх вдень. Використання природного сонячного тепла також може допомогти обігріти будинок. Відкривайте штори на вікнах, вдень, щоб впустити сонце, і закривайте їх на ніч, щоб зберегти тепло.
- Підготуйте теплий домашній одяг. Щоб зберегти тепло одяг повинен бути багатошаровий. Одяг з натуральних тканин краще зберігає тепло. Бажано також придбати термобілизну.
- Налагодьте взаємозв'язок з сусідами. У разі надзвичайної ситуації тримайтеся разом.

Готуймося!

#ЗимаБлизько

Мінрегіон

Шановні громадяни!

Російськими військовими системно обстрілюються об'єкти енергетичної інфраструктури. У разі виникнення екстреної ситуації подача опалення та електрики в будинки може бути повністю припинена. Щоб вижити в такій ситуації, рекомендуємо вам наступне:

- Перевірте справність електричних і опалювальних приладів.
- Придбайте електрогенератор і паливо для нього.
- Печі-буржуйки дозволено використовувати в приватних будинках і тимчасових конструкціях. Використовувати їх в багатоквартирних будинках категорично заборонається, винятк - якщо будівля була істотно зруйнована в результаті військових дій.
- Одягніть теплий одяг і прийміть ліки від застуди.
- Закрийте щілини у вікнах і балконних дверях, в разі відключення опалення прикрийте їх ковдрами або килимами.
- Якщо ви живете в приватному будинку запасіться дровами, палетами, вугіллям заздалегідь.
- Якщо у вас немає можливості придбати дрова або вугілля, використовуйте найдоступніше паливо - деревину з лісу.
- Для особистих потреб можна використовувати хмиз з лісу в якості дров. Також для розпалювання підійдуть хмиз, шишки, суха хвоя і трава, соснові тріски, кора.
- Для розпалювання також можуть підійти старі предмети побуту з деревини, наприклад, непотрібні меблі.
- Для розпалювання використовуйте макулатуру: старі книги, газети, папір.
- На випадок відключення електрики запасіться сірниками, свічками, придбайте гасову лампу.
- Придбайте ліхтарики, запасні батарейки і радіоприймач, що працює не від мережі.
- При скачках напруги в електричній мережі або його відключенні вимкніть всі електропобутові прилади від мережі, щоб при раптовому включенні електрики прилади не пошкодилися і не сталася пожежа.
- В екстреній ситуації розмістіть всіх членів сім'ї в одній опалювальній кімнаті, тимчасово закривши інші.
- Зігрівайтеся теплим чаєм або фізичними вправами.
- Приготуйте спільний план дій з родичами, друзями і сусідами на випадок екстреної ситуації.

Готуймося!

#ЗимаБлизько

Figure 4. PDFs allegedly from the Ministry of Regions

Figure 5. PDF allegedly from the Ministry of Agriculture

In the last document, allegedly from the Ministry of Agriculture, they suggest to eat “pigeon risotto” and they even provide a photo of a living pigeon and a cooked pigeon.… This shows those documents were purposely created in order to rile the readers.

Overall, the messages align with common Russian propaganda themes. They are trying to make Ukrainian people believe they won’t have drugs, food, and heating because of the Russia-Ukraine war.

Second PSYOP wave: December 2023

About a month after the first wave, we detected a second PSYOP email campaign targeting not only Ukrainians, but also people in other European countries. The targets are somewhat random, ranging from the Ukrainian government to an Italian shoe manufacturer. Because all the emails are written in Ukrainian, it is likely that the foreign targets are Ukrainian speakers. According to ESET telemetry, a few hundred people received emails in this second wave.

We found two different email templates in this wave. The first one was sent on December 25th and is shown in Figure 6. As for the first wave, the email messages were sent from an email server operated by the attackers, infoattention[.]com in this case.

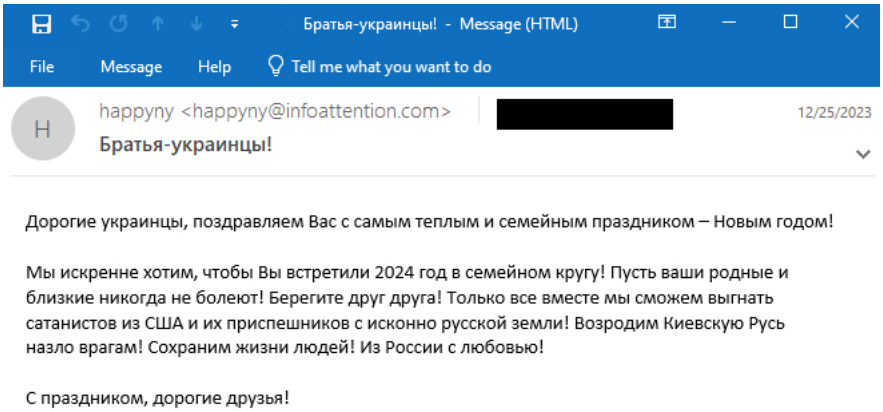


Figure 6. First email template of the second wave

A machine translation of the email body is the following:

> *Dear Ukrainians, we congratulate you on the warmest and most family holiday - the New Year!*
>
> *We sincerely want you to celebrate 2024 with your family! May your family and friends never get sick! Take care of each other! Only together we will be able to drive out the Satanists from the USA and their minions from the original Russian soil! Let's revive Kievan Rus in spite of our enemies! Let's save people's lives! From Russia with love!*
>
> *Happy holiday, dear friends!*

The second email template, shown in Figure 7, was sent on December 26th, 2023 from a different email server: stronginfo1[.]com. During this wave, two additional email addresses were used:

- happyny@infonotifi[.]com
- happyny@infonotification[.]com

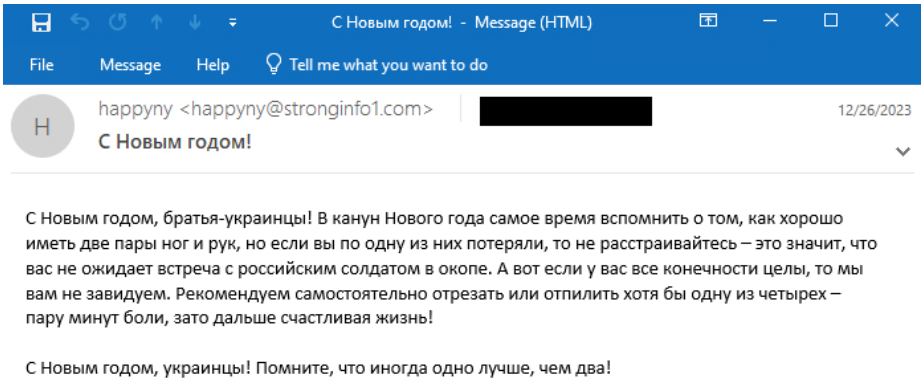


Figure 7. Second email template of the second wave

A machine translation of the email body is the following:

> *Happy New Year, Ukrainian brothers! On New Year's Eve, it's time to remember how good it is to have two pairs of legs and arms, but if you have lost one of them, then don't be upset - this means that you won't meet a Russian soldier in a trench. And here if all your limbs are intact, then we do not envy you. We recommend cutting or sawing off at least one of the four yourself - a couple of minutes of pain, but then a happy life!*
>
> *Happy New Year, Ukrainians! Remember that sometimes one is better than two!*

While the first PSYOP email campaign in November 2023 was rather well-prepared, with specially created PDF documents that were somewhat convincing, this second campaign is rather more basic and darker in its messaging. The second email template is particularly disturbing, with the attackers suggesting people amputate a leg or arm to avoid military deployment. Overall, it has all the characteristics of PSYOPs during war time.

Canadian pharmacy spam: January 2024

In a quite surprising twist of events, one of the domains used to send PSYOP emails in December 2023, infonotification[.]com, started being used to send Canadian pharmacy spam on January 7th, 2024.

An example is provided in Figure 8 and the link redirects to the fake Canadian pharmacy website onlinepharmacycenter[.]com. The spam campaign was moderately large (in the hundreds of messages at least) and people in many countries received such emails.

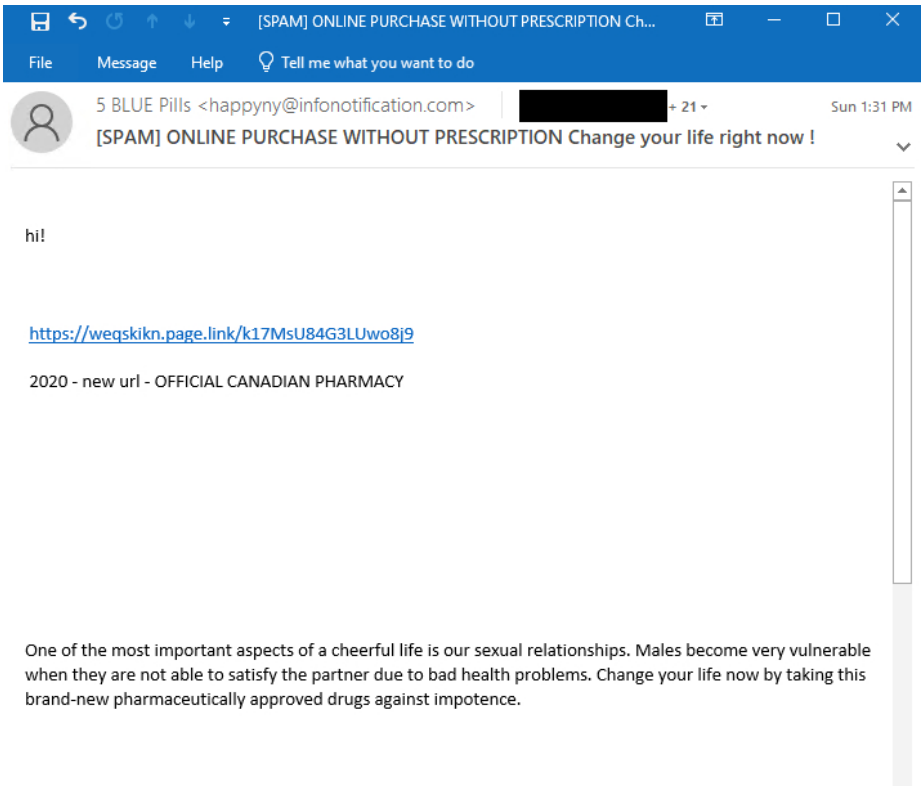


Figure 8. Canadian pharmacy spam

The emails were sent from happyny@infonotification[.]com and this was verified in the email headers:

```
Return-Path: <happyny@infonotification[.]com>
Delivered-To: [redacted]
[redacted]
Received: from infonotification[.]com ([185.12.14[.]13])
        by [redacted] with esmtps (TLS1.3:TLS_AES_256_GCM_SHA384:256)
        [redacted]
        Sun, 07 Jan 2024 12:39:10 +0000
```

Fake Canadian pharmacy spam is a business historically operated by Russian cybercriminals. It was extensively covered in the past by bloggers such as Brian Krebs, especially in his Spam Nation book.

Links between these spam campaigns

While we don't know why the operators of the PSYOP campaigns decided to reuse one of their servers to send fake pharmacy spam, it is likely that they realized that their infrastructure was detected. Hence, they may have decided to try to monetize the already burnt infrastructure, either for their own profit or to fund future espionage operations or PSYOPs. Figure 9 summarizes the links between the different domains and campaigns.

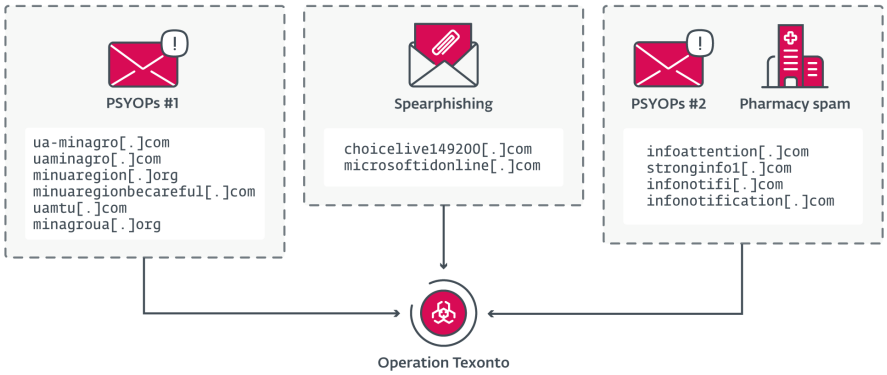


Figure 9. Operation Texonto summary

Conclusion

Since the start of the war in Ukraine, Russia-aligned groups such as Sandworm have been busy disrupting Ukrainian IT infrastructure using wipers. In recent months, we have observed an uptick in cyberespionage operations, especially by the infamous Gamaredon group.

Operation Texonto shows yet another use of technologies to try to influence the war. We found a few typical fake Microsoft login pages but most importantly, there were two waves of PSYOPs via emails probably to try to influence and demoralize Ukrainian citizens with disinformation messages about war-related topics.

A comprehensive list of Indicators of Compromise (IoCs) and samples can be found in our GitHub repository.

> For any inquiries about our research published on WeLiveSecurity, please contact us at threatintel@eset.com.
> ESET Research offers private APT intelligence reports and data feeds. For any inquiries about this service, visit the ESET Threat Intelligence page.

IoCs

Files

SHA-1	Filename	ESET detection name	Description
3C201B2E40357996B3832C72EA305606F07477E3	Minagroua111.pdf	PDF/Fraud.CDY	PDF used in an information operation against Ukraine.
15BF71A771256846D44E8CB3012EE6BC6F9E1532	Mozua.pdf	PDF/Fraud.CDU	PDF used in an information operation against Ukraine.
960341B2C296C425821E4B42435A0618B89D4037	Minregion.pdf	PDF/Fraud.CDT	PDF used in an information operation against Ukraine.
BB14153040608A4F559F48C20B98C1056C794A60	Minregion.pdf	PDF/Fraud.CDX	PDF used in an information operation against Ukraine.

Network

IP	Domain	Hosting provider	First seen	Details
N/A	navalny-votes[.]net	N/A	2023-09-09	Domain related to Alexei Navalny.
N/A	navalny-votesmart[.]net	N/A	2023-09-09	Domain related to Alexei Navalny.
N/A	navalny-voting[.]net	N/A	2023-09-09	Domain related to Alexei Navalny.
45.9.148[.]165	infoattention[.]com	Nice IT Services Group Inc.	2023-12-25	Server used to send emails in Operation Texonto.
45.9.148[.]207	minuaregionbecareful[.]com	Nice IT Services Group Inc.	2023-11-23	Server used to send emails in Operation Texonto.
45.9.150[.]58	stronginfo1[.]com	Nice IT Services Group Inc.	2023-12-25	Server used to send emails in Operation Texonto.
45.129.199[.]200	minuaregion[.]org	Hostinger	2023-11-21	Server used to send emails in Operation Texonto.
45.129.199[.]222	uamtu[.]com	Hostinger	2023-11-20	Server used to send emails in Operation Texonto.
46.249.58[.]177	infonotifi[.]com	serverius-mnt	2023-12-28	Server used to send emails in Operation Texonto.
89.116.52[.]79	uaminagro[.]com ua-minagro[.]com	IPXO LIMITED	2023-11-17	Server used to send emails in Operation Texonto.
154.49.137[.]16	choicelive149200[.]com	Hostinger	2023-10-26	Phishing server.
185.12.14[.]13	infonotification[.]com	Serverius	2023-12-28	Server used to send emails in Operation Texonto.
193.43.134[.]113	login.microsoftidonline[.]com	Hostinger	2023-10-03	Office 365 phishing server.
195.54.160[.]59	minagroua[.]org	BlueVPS	2023-11-21	Server used to send emails in Operation Texonto.

Email addresses

- minregion@uaminagro[.]com
- minregion@minuaregion[.]org
- minregion@minuaregionbecareful[.]com
- minregion@uamtu[.]com
- mozua@ua-minagro[.]com
- mozua@minagroua[.]org
- minagroua@vps-3075.lethost[.]network
- happyny@infoattention[.]com
- happyny@stronginfo1[.]com
- happyny@infonotifi[.]com
- happyny@infonotification[.]com

MITRE ATT&CK techniques

This table was built using version 14 of the MITRE ATT&CK framework.

Tactic	ID	Name	Description
Resource Development	T1583.001	Acquire Infrastructure: Domains	Operators bought domain names at Namecheap.
	T1583.004	Acquire Infrastructure: Server	Operators rented servers at Nice IT, Hostinger, Serverius, and BlueVPS.
Initial Access	T1566	Phishing	Operators sent emails with disinformation content.
	T1566.002	Phishing: Spearphishing Link	Operators sent emails with a link to a fake Microsoft login page.
Defense Evasion	T1036	Masquerading	Operators used domain names similar to official Ukrainian government domain names.