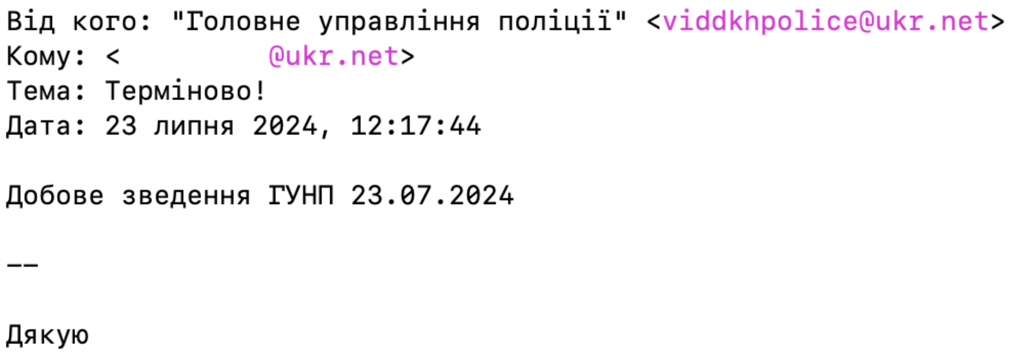
# Russia-nexus actor targets Ukraine

: 7/24/2024

Recently an email was forwarded to Virustotal, appearing to show a ukr.net sender spoofing “Headquarters Police Department” (Головне управління поліції), targeting a government organization related to the Ukrainian economy.

Detection takeaways:

1. the zip attachment was only 341 bytes, and the underlying attachment was even smaller at 134 bytes
2. these very small sizes may bypass filters analysts or tools use to weed out junk files



```
Від кого: "Головне управління поліції" <viddkhpolice@ukr.net>
Кому: <          @ukr.net>
Тема: Терміново!
Дата: 23 липня 2024, 12:17:44

Добове зведення ГУНП 23.07.2024

--

Дякую
```

Figure 1: email spoofing a Ukrainian police org

| Attachment | sha256 | trans |
|---|---|---|
| терміново_23_07_2024.zip | c16926a74f8d30b4086057241edc46e88bb0cf675ff5b5ced93ea654ea2b4e26 | (urgently _23_0 |
| терміново_info_23_07_2024.html | 9e49db0eb920e130c0393a87c96434b9f0257025584cf546f623c1cb0b074333 | (urgently_info_2 |

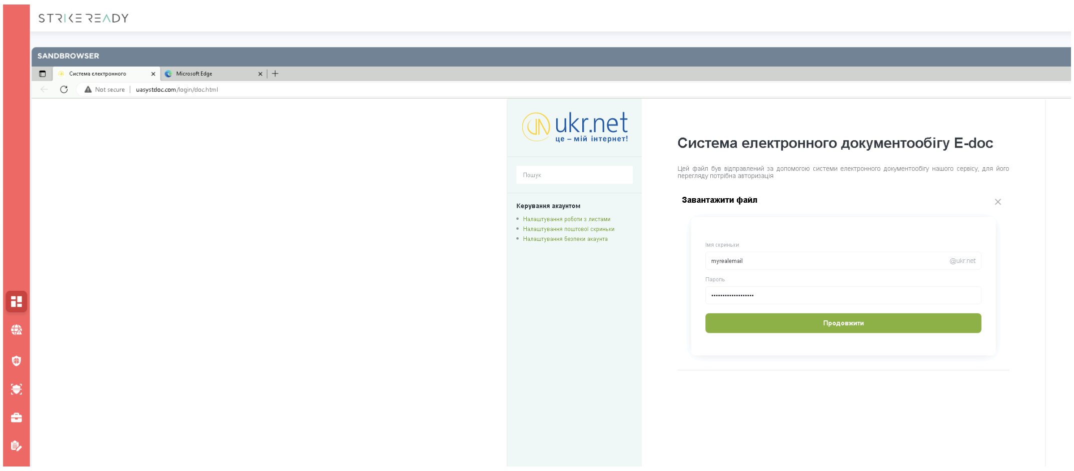
Figure 2: attachments to email

The initial HTML was very small, 134 bytes, and was simply a redirect to an external site.

```html
<!DOCTYPE html>
<html>
 <meta http-equiv="refresh"content="0;url=http://uasystdoc.com/login/doc.html">
<body>
</body>
</html>
```

Figure 3: simple redirect, perhaps to prevent anti-spam detection

The page content is the below, and one can notice that it’s a phishing page for ukr.net, a Ukrainian webmail service. This service is a frequent target for Russia-nexus threat actors.



Система електронного документообігу E-doc

Цей файл був відправлений за допомогою системи електронного документообігу нашого сервісу, для його перегляду потрібна авторизація

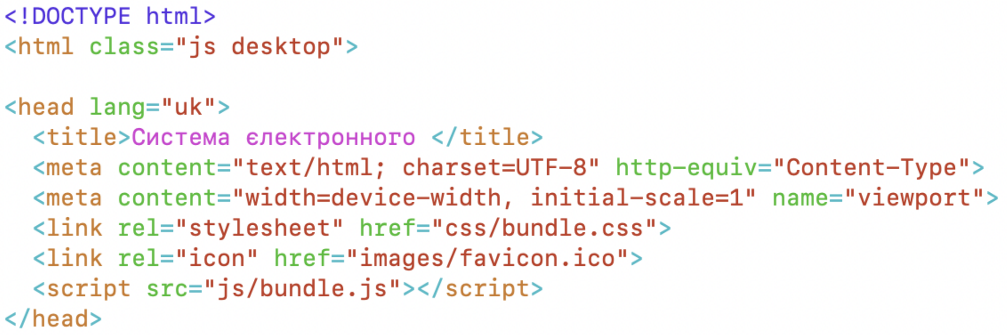
Завантажити файл

Імя скриньки: myrealemail @ukr.net

Пароль: ••••••••••••••••••••

Figure 4: UKR credential phishing

The doc.html page contains a numerous amount of sig-able artifacts to find similar phishing pages. Signatures need not be written on malicious content to be effective. In the below example, the `<head lang="uk">` is unusual. `lang=` is typically inside a `<html>` tag instead of `<head>`, but when you can combine this with other indicators, two weak signals can become a strong signature.



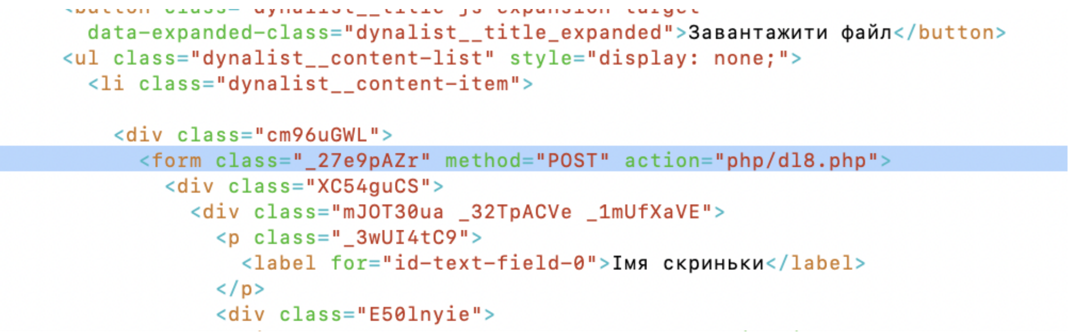
```
<!DOCTYPE html>
<html class="js desktop">

<head lang="uk">
  <title>Система електронного </title>
  <meta content="text/html; charset=UTF-8" http-equiv="Content-Type">
  <meta content="width=device-width, initial-scale=1" name="viewport">
  <link rel="stylesheet" href="css/bundle.css">
  <link rel="icon" href="images/favicon.ico">
  <script src="js/bundle.js"></script>
</head>
```

Figure 5: snippet of doc.html

| landing pages | sha256 |
|---|---|
| doc.html | efd54e566767de3e35597dae60d317b388460ffc2b3231bd4897b254863835cc |
| index.html | 5d93ee6f0f4e88d06f384a84ec4401100ec6b1d01062af23acebd3f314379be0 |
| file1.html | 5b694114129846328da15d79e2bc6a4b19f887e86ae8f0abc6d9572a8b88e431 |

Figure 6: associated landing pages

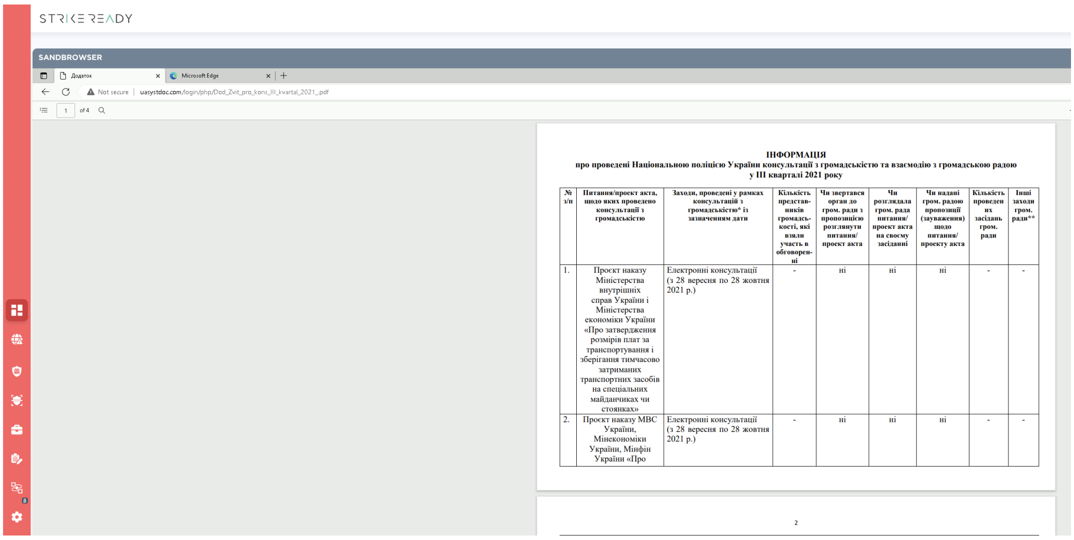
Examining the landing pages, we can notice the credentials will be POST'd to a PHP script and then redirected.



```
    <button class="dynalist__title js-expansion target"
      data-expanded-class="dynalist__title_expanded">Завантажити файл</button>
    <ul class="dynalist__content-list" style="display: none;">
      <li class="dynalist__content-item">

        <div class="cm96uGWL">
          <form class="_27e9pAZr" method="POST" action="php/dl8.php">
            <div class="XC54guCS">
              <div class="mJOT30ua _32TpACVe _1mUfXaVE">
                <p class="_3wUI4tC9">
                  <label for="id-text-field-0">Імя скриньки</label>
                </p>
                <div class="E50lnyie">
```

Figure 7: Analysts raise an eyebrow at "dl8"

After the credentials are sent, the PHP script redirects us to a decoy that might be interesting to a Ukrainian target. When analysts see "dl8.php", they typically wonder what may live at "dl1.php", "dl2.php", etc.



uasystdoc.com/login/php/Dod_Zvit_pro_kons_III_kvartal_2021_.pdf

**ІНФОРМАЦІЯ**
**про проведені Національною поліцією України консультації з громадськістю та взаємодію з громадською радою**
**у ІІІ кварталі 2021 року**

| № з/п | Питання/проект акта, щодо яких проведено консультації з громадськістю | Заходи, проведені у рамках консультацій з громадськістю* із зазначенням дати | Кількість представників громадськості, які взяли участь в обговоренні | Чи звертався орган до гром. ради з пропозицією розглянути питання/ проект акта | Чи розглядала гром. рада питання/ проект акта на своєму засіданні | Чи надані гром. радою пропозиції (зауваження) щодо питання/ проекту акта | Кількість проведених засідань гром. ради | Інші заходи гром. ради** |
|---|---|---|---|---|---|---|---|---|
| 1. | Проєкт наказу Міністерства внутрішніх справ України і Міністерства економіки України «Про затвердження розмірів плат за транспортування і зберігання тимчасово затриманих транспортних засобів на спеціальних майданчиках чи стоянках» | Електронні консультації (з 28 вересня по 28 жовтня 2021 р.) | - | ні | ні | ні | - | - |
| 2. | Проєкт наказу МВС України, Мінекономіки України, Мінфін України «Про | Електронні консультації (з 28 вересня по 28 жовтня 2021 р.) | - | ні | ні | ні | - | - |

Figure 8: decoy content after credentials are entered

After looping through dl[0-9].php, we can harvest a number of other interesting decoy files as well as IOCs.

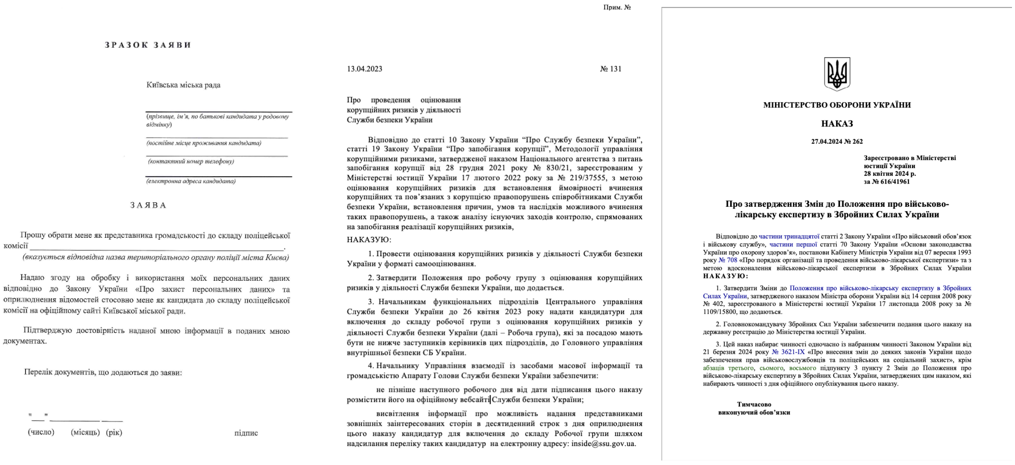
| | |
|---|---|
| dl.php | 82.221.139[.]200/login/php/1308_8711629.html |
| dl2.php | 82.221.139[.]200/login/php/zrazok.pdf |

dl3.php 82.221.139[.]200/login/php/organizations_kharkiv_2021_12_03-1.xlsx
dl4.php 82.221.139[.]200/login/php/47.pdf
dl5.php 82.221.139[.]200/login/php/tsu-sbu-vid-13042023-131-site.doc
dl6.php ukainua[.]com/login/php/d534990-20240427.pdf
dl7.php ukainua[.]com/login/php/Dod_Zvit_pro_kons_III_kvartal_2021_.pdf
dl8.php uasystdoc[.]com/login/php/Dod_Zvit_pro_kons_III_kvartal_2021_.pdf

Figure 9: credential gathering and decoy redirecting scripts

A sampling of the decoy content is show below.

**zrazok.pdf** **47.pdf** **d534990-20240427.pdf**



ЗРАЗОК ЗАЯВИ

Київська міська рада

(прізвище, ім'я, по батькові кандидата у родовому відмінку)

(постійне місце проживання кандидата)

(контактний номер телефону)

(електронна адреса кандидата)

ЗАЯВА

Прошу обрати мене як представника громадськості до складу поліцейської комісії ________________________________.
(вказується відповідна назва територіального органу поліції міста Києва)

Надаю згоду на обробку і використання моїх персональних даних відповідно до Закону України «Про захист персональних даних» та оприлюднення відомостей стосовно мене як кандидата до складу поліцейської комісії на офіційному сайті Київської міської ради.

Підтверджую достовірність наданої мною інформації в поданих мною документах.

Перелік документів, що додаються до заяви:

"___" ___________ _____
(число) (місяць) (рік) підпис

Прим. №

13.04.2023 № 131

Про проведення оцінювання корупційних ризиків у діяльності Служби безпеки України

Відповідно до статті 10 Закону України "Про Службу безпеки України", статті 19 Закону України "Про запобігання корупції", Методології управління корупційними ризиками, затвердженої наказом Національного агентства з питань запобігання корупції від 28 грудня 2021 року № 830/21, зареєстрованим у Міністерстві юстиції України 17 лютого 2022 року за № 219/37555, з метою оцінювання корупційних ризиків для встановлення ймовірності вчинення корупційних та пов'язаних з корупцією правопорушень співробітниками Служби безпеки України, встановлення причин, умов та наслідків можливого вчинення таких правопорушень, а також аналізу існуючих заходів контролю, спрямованих на запобігання реалізації корупційних ризиків,

НАКАЗУЮ:

1. Провести оцінювання корупційних ризиків у діяльності Служби безпеки України у форматі самооцінювання.

2. Затвердити Положення про робочу групу з оцінювання корупційних ризиків у діяльності Служби безпеки України, що додається.

3. Начальникам функціональних підрозділів Центрального управління Служби безпеки України до 26 квітня 2023 року надати кандидатури для включення до складу робочої групи з оцінювання корупційних ризиків у діяльності Служби безпеки України (далі – Робоча група), які за посадою мають бути не нижче заступників керівників цих підрозділів, до Головного управління внутрішньої безпеки СБ України.

4. Начальнику Управління взаємодії із засобами масової інформації та громадськістю Апарату Голови Служби безпеки України забезпечити:

не пізніше наступного робочого дня від дати підписання цього наказу розмістити його на офіційному вебсайті Служби безпеки України;

висвітлення інформації про можливість надання представниками зовнішніх заінтересованих сторін в десятиденний строк з дня оприлюднення цього наказу кандидатур для включення до складу Робочої групи шляхом надсилання переліку таких кандидатур на електронну адресу: inside@ssu.gov.ua.

МІНІСТЕРСТВО ОБОРОНИ УКРАЇНИ

НАКАЗ

27.04.2024 № 262

Зареєстровано в Міністерстві
юстиції України
28 квітня 2024 р.
за № 616/41961

Про затвердження Змін до Положення про військово-лікарську експертизу в Збройних Силах України

Відповідно до частини тринадцятої статті 2 Закону України «Про військовий обов'язок і військову службу», частини першої статті 70 Закону України «Основи законодавства України про охорону здоров'я», постанови Кабінету Міністрів України від 07 вересня 1993 року № 708 «Про порядок організації та проведення військово-лікарської експертизи» та з метою вдосконалення військово-лікарської експертизи в Збройних Силах України **НАКАЗУЮ:**

1. Затвердити Зміни до Положення про військово-лікарську експертизу в Збройних Силах України, затвердженого наказом Міністра оборони України від 14 серпня 2008 року № 402, зареєстрованого в Міністерстві юстиції України 17 листопада 2008 року за № 1109/15800, що додаються.

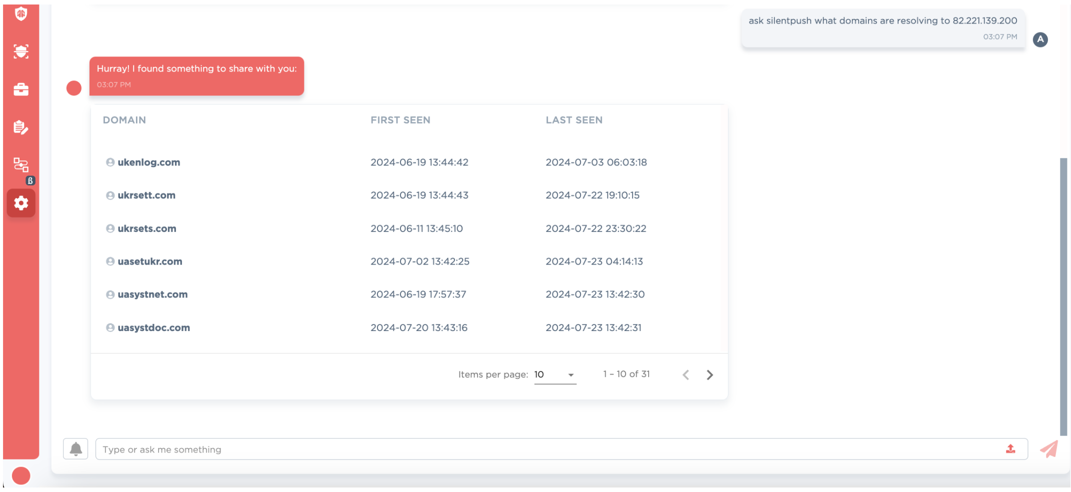
2. Головнокомандувачу Збройних Сил України забезпечити подання цього наказу на державну реєстрацію до Міністерства юстиції України.

3. Цей наказ набирає чинності одночасно із набранням чинності Законом України від 21 березня 2024 року № 3621-IX «Про внесення змін до деяких законів України щодо забезпечення прав військовослужбовців та поліцейських на соціальний захист», крім абзаців третього, сьомого, восьмого підпункту 3 пункту 2 Змін до Положення про військово-лікарську експертизу в Збройних Силах України, затверджених цим наказом, які набирають чинності з дня офіційного опублікування цього наказу.

**Тимчасово**
**виконуючий обов'язки**

Figure 10: three of the decoy files from the table above, showing Ukrainian themes

A quick pivot to passivedns through our community account at silentpush shows many likely related domains, shared in our github.



ask silentpush what domains are resolving to 82.221.139.200
03:07 PM

Hurray! I found something to share with you:
03:07 PM

| DOMAIN | FIRST SEEN | LAST SEEN |
|---|---|---|
| ukenlog.com | 2024-06-19 13:44:42 | 2024-07-03 06:03:18 |
| ukrsett.com | 2024-06-19 13:44:43 | 2024-07-22 19:10:15 |
| ukrsets.com | 2024-06-11 13:45:10 | 2024-07-22 23:30:22 |
| uasetukr.com | 2024-07-02 13:42:25 | 2024-07-23 04:14:13 |
| uasystnet.com | 2024-06-19 17:57:37 | 2024-07-23 13:42:30 |
| uasystdoc.com | 2024-07-20 13:43:16 | 2024-07-23 13:42:31 |

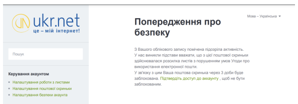
Items per page: 10 1 – 10 of 31

Type or ask me something

Figure 11: passive dns for 82.221.139[.]200

Lastly, pivots on the layout of the phishing page, combined with negating legitimate infrastructure, will lead to similar phishing campaign.

**Phish** **IOCs**



Керування акаунтом
- Налаштування роботи з листами
- Налаштування поштової скриньки
- Налаштування безпеки акаунта

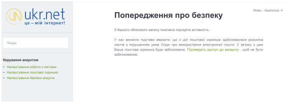
Попередження про безпеку

З Вашого облікового запису помічена підозріла активність.
У нас виникли підстави вважати, що з цієї поштової скриньки здійснювалася розсилка листів з порушенням умов Угоди про використання електронної пошти.
У зв'язку з цим Ваша поштова скринька через 3 доби буде заблокована. Підтвердіть доступ до аккаунту , щоб не бути заблокованим.

changepassword-ukr[.]net/desktop/security/login/

38963b61113b7b88e3fce30539e63b4745f8d91f8e2577b6597a09648b105733

Figure 12: UKR.NET.pdf



Керування акаунтом
- Налаштування роботи з листами
- Налаштування поштової скриньки
- Налаштування безпеки акаунта

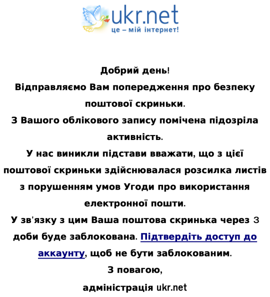
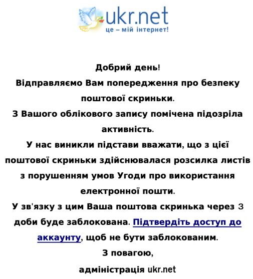
Попередження про безпеку

З Вашого облікового запису помічена підозріла активність.

У нас виникли підстави вважати, що з цієї поштової скриньки здійснювалася розсилка листів з порушенням умов Угоди про використання електронної пошти. У зв'язку з цим Ваша поштова скринька буде заблокована. Підтвердіть доступ до аккаунту , щоб не бути заблокованим.

accounts.ukr-reset[.]email/login/

2f1f4b077b6fc40d8f0c995e80657448478a08acdf0e33ee2b73602bda62270c

| Phish | IOCs |
|---|---|
| <br>ukr.net<br>це – мій інтернет!<br>Добрий день!<br>Відправляємо Вам попередження про безпеку поштової скриньки.<br>З Вашого облікового запису помічена підозріла активність.<br>У нас виникли підстави вважати, що з цієї поштової скриньки здійснювалася розсилка листів з порушенням умов Угоди про використання електронної пошти.<br>У зв'язку з цим Ваша поштова скринька через 3 доби буде заблокована. Підтвердіть доступ до аккаунту, щоб не бути заблокованим.<br>З повагою,<br>адміністрація ukr.net<br>Figure 13: Попередження.pdf | accounts.ukr-mails[.]net/login<br>853f21ba9a8a362a9bafc98204eb70b8c23ba845359e694984711ec1485d0c2f |
| <br>ukr.net<br>це – мій інтернет!<br>Добрий день!<br>Відправляємо Вам попередження про безпеку поштової скриньки.<br>З Вашого облікового запису помічена підозріла активність.<br>У нас виникли підстави вважати, що з цієї поштової скриньки здійснювалася розсилка листів з порушенням умов Угоди про використання електронної пошти.<br>У зв'язку з цим Ваша поштова скринька через 3 доби буде заблокована. Підтвердіть доступ до аккаунту, щоб не бути заблокованим.<br>З повагою,<br>адміністрація ukr.net | accounts.kv-ukr[.]net/login/<br>e159886a173f021b345ad152ad84beed3ac39b6a7455805c255f38d7b4c9434c |

| Vendor | Threat Actor name |
|---|---|
| Google Cloud Security (neé Mandiant) | UNC3707 |
| You? | Get in touch for blog pre-releases! |

Figure 14: Other validated vendor names for this actor

Our github provides a download to the raw samples mentioned in the blog, as well as the indicators.

## Acknowledgements

The authors would like to thank the reviewers, as well as peer vendors, for their comments and corrections. Please get in touch at research@strikeready.com if you have corrections, or would like to collaborate on research.