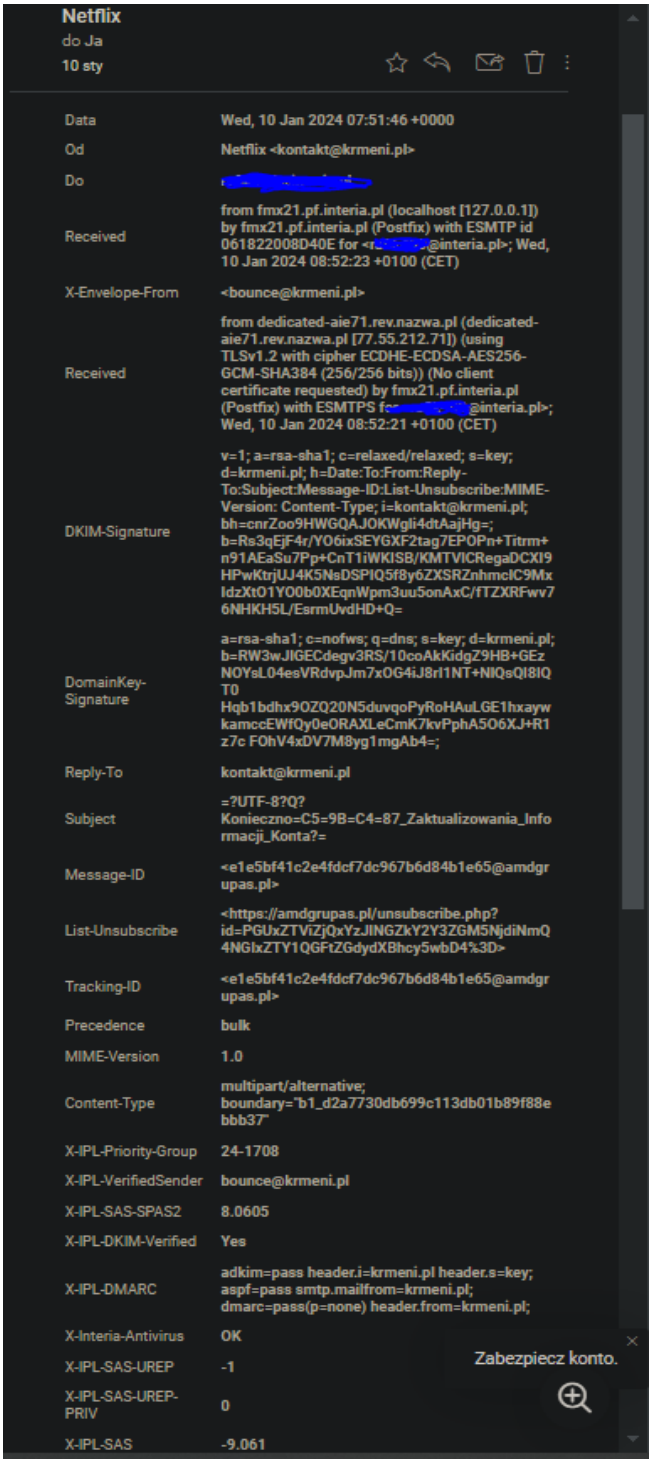
**Scenariusz „ analiza Phishingowego emaila”**

Email który otrzymaliśmy

# Wstęp

W ramach niniejszej analizy zbadamy e-mail, który na pierwszy rzut oka wygląda, jakby został wysłany przez Netflix. Przyjrzymy się dokładnie jego szczegółom, aby ustalić, czy jest to prawdziwa wiadomość, czy próba wyłudzenia danych (phishing). Wiadomość została sprawdzona na poczcie @interia.pl, a nie na Gmailu, który skutecznie usuwa wiadomości w folderze spam po 30 dniach. Analiza tego e-maila pozwoli określić, jakie kroki należy podjąć, aby zidentyfikować phishingowe wiadomości i zabezpieczyć się przed nimi.

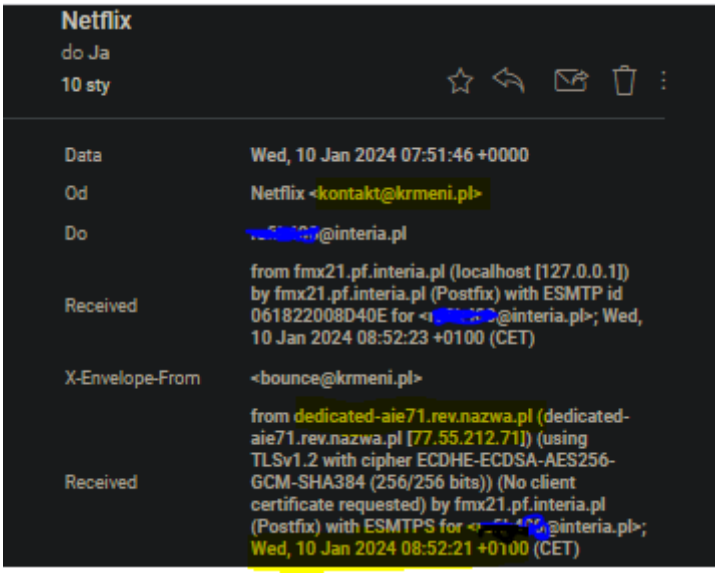
W pierwszej kolejności pobieramy „Szczegóły wiadomości”



# Analiza techniczna

„Nagłówki wiadomośći”

W pierwszej kolejności pobraliśmy szczegóły wiadomości, aby przeanalizować nagłówek **"Od"**. E-mail został wysłany z adresu **kontakt@krmeni[.]pl**, który próbuje podszyć się pod Netflix. W celu potwierdzenia tych informacji, można poszukać oficjalnych adresów Netflixa na ich stronie.




Po potwierdzeniu informacji wiemy już że to phishing, teraz naszym celem jest zbadanie do kogo należy domena oraz co jestem celem  podszywającego, np. ustalenie jakie dane chce wyłudzić czy zachęca do pobrania i uruchomienia pliku lub wejścia na podaną stronę.

Sprawdzając informacje o serwerach SMTP w nagłówkach „Received” odczytujemy informacje o serwerze wysyłającym „dedicated-aie71.rev.nazwa.pl” oraz o jego adresie IP: 77.55.212.71.

Oraz brak certyfikatu klienta co oznacza że serwer nie wymagał certyfikatu klienta, co informuje nas  że komunikacja była zabezpieczona(TLSv1.2), ale serwer nie weryfikował tożsamości klienta za pomocą certyfikatu.

Mając dane serwera domeny sprawdzamy za pomocą whois albo void ip do kogo należy domena oraz kiedy została utworzona

```
inetnum:        77.55.192.0 - 77.55.239.255
netname:        NAZWAPL-VPS
descr:          VPS and dedicated servers
country:        PL
admin-c:        NA15967-RIPE
tech-c:         NA15967-RIPE
status:         ASSIGNED PA
mnt-by:         NETART-PL-MNT
created:        2019-01-07T11:11:04Z
last-modified:  2023-03-31T10:44:12Z
source:         RIPE

role:           NETART GROUP Administrator
address:        nazwa.pl
address:        ul. Pana Tadeusza 2, 30-727 Krakow
address:        Poland
phone:          +48 801 332233
phone:          +48 12 2978810
fax-no:         +48 12 2978808
abuse-mailbox:  abuse@netart.com
admin-c:        MS45596-RIPE
admin-c:        MM48507-RIPE
tech-c:         MS45596-RIPE
tech-c:         MM48507-RIPE
nic-hdl:        NA15967-RIPE
mnt-by:         NETART-PL-MNT
created:        2005-06-15T21:03:58Z
last-modified:  2023-10-26T08:39:16Z
source:         RIPE # Filtered

% Information related to '77.55.208.0/20AS15967'

route:          77.55.208.0/20
origin:         AS15967
mnt-by:         NETART-PL-MNT
created:        2018-06-06T07:18:46Z
last-modified:  2019-04-17T11:21:18Z
source:         RIPE

% This query was served by the RIPE Database Query Service version 1.114 (DEXTER)
```

Analiza: **Kluczowe informacje:**

**Zakres adresów IP**: **77.55.192.0 - 77.55.239.255**

**Nazwa sieci**: NAZWAPL-VPS **Kraj**: Polska (PL)

**Opis**: VPS i serwery dedykowane **Dostawca**: NetArt

**Kontakt w sprawie nadużyć**: **abuse@netart.com**

**Data utworzenia**: 7 stycznia 2019

**Ostatnia modyfikacja**: 31 marca 2023

**Numer systemu autonomicznego**: AS15967

**Adres administracyjny:**

**Administrator**: NETART GROUP Administrator

**Adres**: nazwa.pl, ul. Pana Tadeusza 2, 30-727 Kraków, Polska

**Telefony**: +48 801 332233, +48 12 2978810

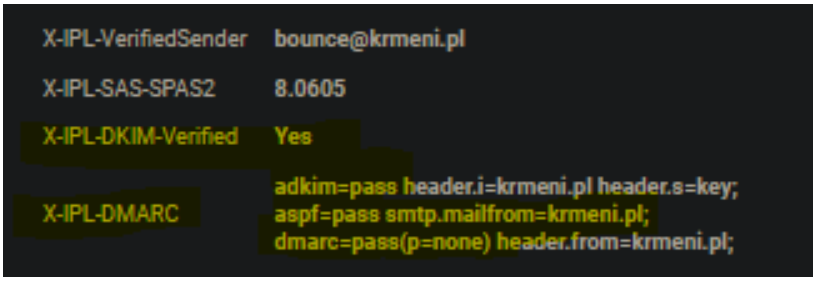
Następnie sprawdzamy nagłówki SPF/DKIM/DMARC

**Wynik SPF**: **aspf=pass** oznacza, że serwer SMTP, który wysłał wiadomość, jest autoryzowany do używania domeny krmeni.pl zgodnie z polityką SPF.

**Wynik DKIM**: **X-IPL-DKIM-Verified: Yes** wskazuje, że podpis DKIM został poprawnie zweryfikowany, co potwierdza autoryzację wiadomości przez domenę krmeni.pl.

**Wynik SMTP**: **smtp.mailfrom=krmeni.pl** potwierdza, że domena używana w polu MAIL FROM przeszła weryfikację SPF.

**Wynik DMARC**: **adkim=pass** oznacza, że podpis DKIM dla domeny krmeni.pl jest zgodny z domeną w polu From wiadomości e-mail, co potwierdza, że wiadomość jest autoryzowana przez nadawcę i spełnia wymagania polityki DMARC.




Podsumowanie analizy nagłówków SPF/DKIM/DMARC

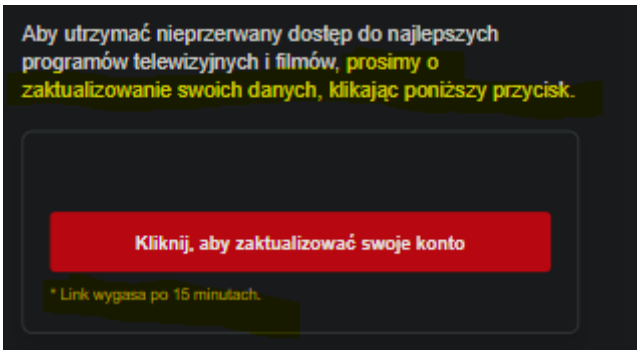
Analizując e-maila z domeny krmeni.pl, zauważam, że wyniki SPF, DKIM i DMARC są pozytywne. **SPF (aspf=pass)** wskazuje, że serwer SMTP wysyłający wiadomość jest autoryzowany przez domenę krmeni.pl. To sugeruje, że serwer jest uprawniony do wysyłania e-maili z tej domeny, ale nie gwarantuje, że sama domena jest legalna. Atakujący mogą skonfigurować serwery SMTP, które przechodzą weryfikację SPF, ale są używane do phishingu.

**Podpis DKIM (X-IPL-DKIM-Verified: Yes**) został poprawnie zweryfikowany, co oznacza, że wiadomość została podpisana przez domenę krmeni.pl i nie została zmieniona. Mimo to, przestępcy mogą prawidłowo skonfigurować podpis DKIM, aby wyglądało na autoryzowane, nawet jeśli domena jest używana do działań phishingowych.

**Wynik DMARC (adkim=pass)** oznacza, że podpis DKIM zgadza się z domeną w polu From, co spełnia wymagania polityki DMARC. To potwierdza, że wiadomość jest zgodna z polityką domeny. Jednak pozytywne wyniki DMARC, SPF i DKIM nie wykluczają, że domena krmeni.pl może być używana do phishingu.

Podsumowując, chociaż techniczne weryfikacje są pozytywne, wiemy że jest to domena phishingowa (adres podszywa się pod Netflixa udowodniliśmy sprawdzając poprawną domene którą używa Netflix) załóżmy że przeoczyliśmy jedną literówke w emailu albo ze adress jest zgodny z naszą bazą zaufanych senderów ale są podejrzenia że może zawierać elementy phishingowe.

Co dalej? Teraz skupiamy się na analizie treści emaila w poszukiwaniu znamion złośliwości czyli np. elementów socjologii  które kążą nam zrobić coś natychmiast bez zastanowienia albo formularzy próbujących wyłudzić nasze danę czy URLów prowadzących do zęwnętrznych stron.




Znajdujemy element socjologii który mówi nam że musimy coś zrobić już bo działamy pod presją czasu i zaraz on się skończy „Link wygasa po 15 minutach”

Oraz znajdujemy  obrazek który po kliknięciu przenosi nas na inny adres URL.

Sprawdzamy co to za adres URL używając jednego z narzędzi: virus total/sandbox/ip.void/ url scanio/anyrun/browseonline

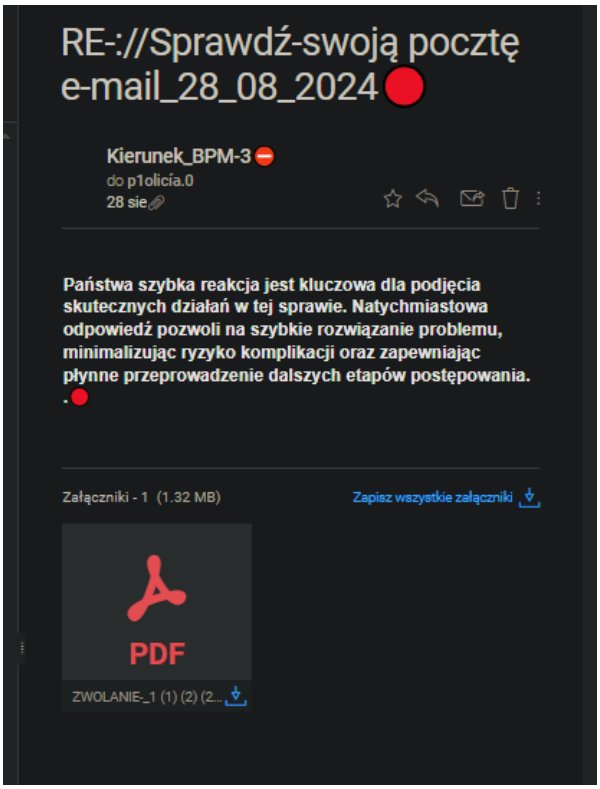
Link który wyodrębniliśmy to
https://motofuria[.]bernadetalena[.]pl/patrykkewin/tumójemailnteria[.]pl

Sprawdzając url różnymi narzędziami dowiadujemy się żę domena już nie działa ( email analizowany jest ze stycznia 2024 roku)

Dla przykładu wynik który pierwotnie powinniśmy otrzymać z Virustotala.

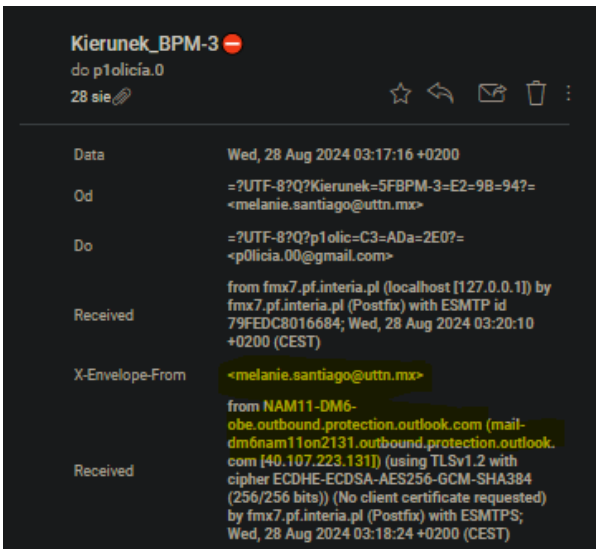
# Analiza Techniczna

Scneariusz: Analiza phishingowego emaila z załącznikiem.




Na pierwszy rzut oka widzimy już błędy gramatyczne oraz stylistyczne sugerujące że może to być phishing. Tytuł „RE-://Sprawdź-swoją-pocztę e-mail_28_08_2024” nie brzmi legitnie, tak samo „Natychmiastowa odpowiedź pozwoli na szybkie rozwiązanie problemu, minimalizując ryzyko komplikacji oraz zapewniając płynne przeprowadzenie dalszych etapów” zdanie nie brzmi za dobrze oraz zawiera element socjotechniki który mówi że coś musimy zrobić już(w tym przypadku pobrać  i uruchomić plik), co sugeruje nam  że mamy  najprawdopodobniej do czynienia z phishingiem.

Następnie przechodzimy do analizy nagłówka, wchodzimy w szczegóły wiadomości.



Ustalamy nadawce w tym przypadku będzie to **„melanie.santiago@uttn.mx”**

oraz zwracamy uwagę ze adres email nadawcy jest zakodowany w UTF-8

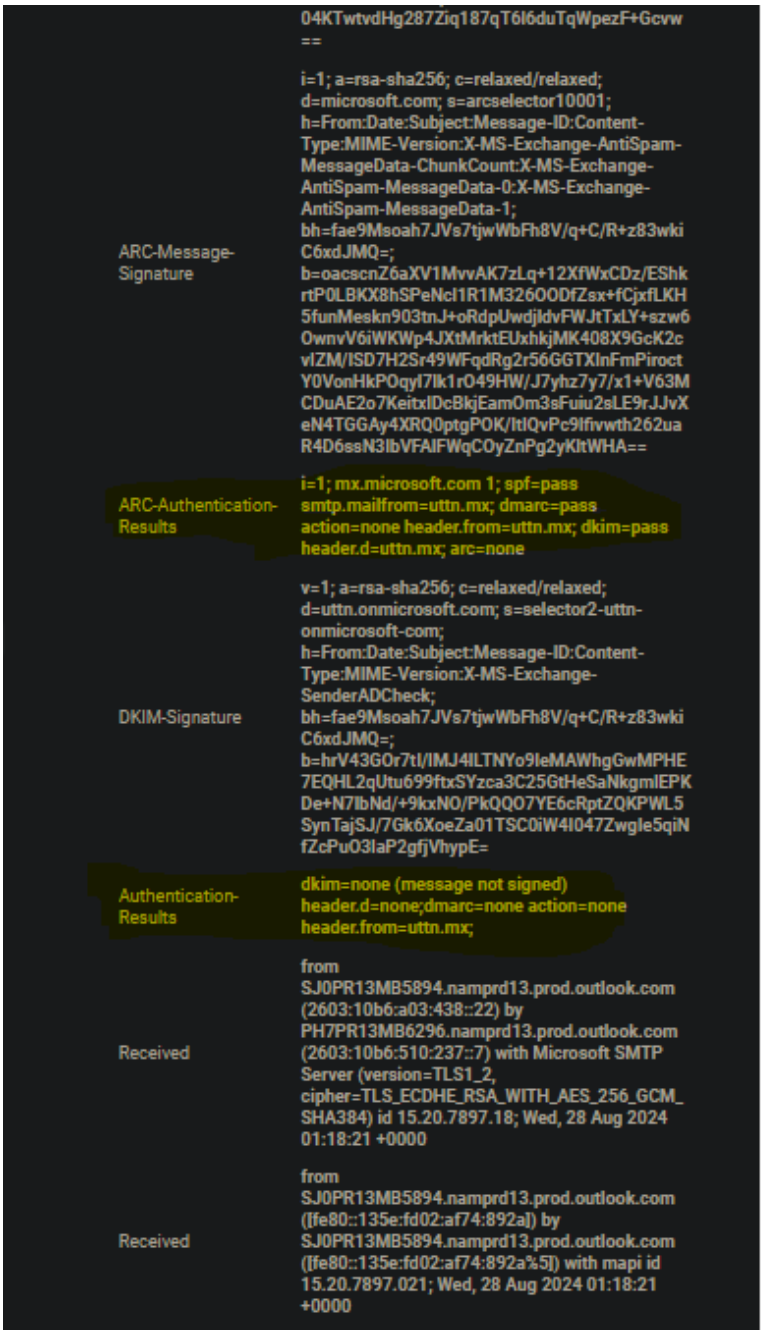
oraz odbiorce w tym przypadku **”p0licia.00@gmail.com”**

Sam adress sugeruje nam próbe phishingu ponieważ próbuje podszyć się pod policje.

Jednak zauważamy że w miejscu **„Do”** nie ma naszej domeny ani naszego emaila (@interia.pl)

Jest to spowodowane najprawdopodobniej tym  że wiadomość mogła być wysyłana do wielu odbiorców, a nasz adres znalazł się na liście.

Przechodzimy do dalszej analizy.



| | |
|---|---|
| | 04KTwtvdHg287Ziq187qT6l6duTqWpezF+Gcvw== |
| ARC-Message-Signature | i=1; a=rsa-sha256; c=relaxed/relaxed; d=microsoft.com; s=arcselector10001; h=From:Date:Subject:Message-ID:Content-Type:MIME-Version:X-MS-Exchange-AntiSpam-MessageData-ChunkCount:X-MS-Exchange-AntiSpam-MessageData-0:X-MS-Exchange-AntiSpam-MessageData-1; bh=fae9Msoah7JVs7tjwWbFh8V/q+C/R+z83wkiC6xdJMQ=; b=oacscnZ6aXV1MvvAK7zLq+12XfWxCDz/EShkrtP0LBKX8hSPeNcl1R1M326OODfZsx+fCjxfLKH5funMeskn903tnJ+oRdpUwdjldvFWJtTxLY+szw6OwnvV6iWKWp4JXtMrktEUxhkjMK408X9GcK2cvlZM/ISD7H2Sr49WFqdRg2r56GGTXInFmPiroctY0VonHkPOqyl7lk1rO49HW/J7yhz7y7/x1+V63MCDuAE2o7KeitxlDcBkjEamOm3sFuiu2sLE9rJJvXeN4TGGAy4XRQ0ptgPOK/ItlQvPc9lfivwth262uaR4D6ssN3lbVFAIFWqCOyZnPg2yKltWHA== |
| ARC-Authentication-Results | i=1; mx.microsoft.com 1; spf=pass smtp.mailfrom=uttn.mx; dmarc=pass action=none header.from=uttn.mx; dkim=pass header.d=uttn.mx; arc=none |
| DKIM-Signature | v=1; a=rsa-sha256; c=relaxed/relaxed; d=uttn.onmicrosoft.com; s=selector2-uttn-onmicrosoft-com; h=From:Date:Subject:Message-ID:Content-Type:MIME-Version:X-MS-Exchange-SenderADCheck; bh=fae9Msoah7JVs7tjwWbFh8V/q+C/R+z83wkiC6xdJMQ=; b=hrV43GOr7tl/IMJ4ILTNYo9leMAWhgGwMPHE7EQHL2qUtu699ftxSYzca3C25GtHeSaNkgmlEPKDe+N7lbNd/+9kxNO/PkQQO7YE6cRptZQKPWL5SynTajSJ/7Gk6XoeZa01TSC0iW4I047Zwgle5qiNfZcPuO3IaP2gfjVhypE= |
| Authentication-Results | dkim=none (message not signed) header.d=none;dmarc=none action=none header.from=uttn.mx; |
| Received | from SJ0PR13MB5894.namprd13.prod.outlook.com (2603:10b6:a03:438::22) by PH7PR13MB6296.namprd13.prod.outlook.com (2603:10b6:510:237::7) with Microsoft SMTP Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.7897.18; Wed, 28 Aug 2024 01:18:21 +0000 |
| Received | from SJ0PR13MB5894.namprd13.prod.outlook.com ([fe80::135e:fd02:af74:892a]) by SJ0PR13MB5894.namprd13.prod.outlook.com ([fe80::135e:fd02:af74:892a%5]) with mapi id 15.20.7897.021; Wed, 28 Aug 2024 01:18:21 +0000 |

Widzimy ze wiadomość najpierw posiada  autoryzacje SPF, SMTP, DKIM a pożniej nie, czym to jest spowodowane, co to oznacza i dalczego wyniki są różne?

**Różne instancje weryfikacji**:

**ARC** jest mechanizmem, który pozwala na autoryzację wiadomości, gdy przechodzi przez różne serwery. W przypadku ARC, wyniki weryfikacji mogą być różne w zależności od tego, na którym etapie wiadomość była analizowana.

**Weryfikacja DKIM w ARC** mogła być przeprowadzona na poziomie serwera, który miał dostęp do odpowiednich kluczy publicznych i mógł zweryfikować podpis. W związku z tym, ARC może wskazywać, że podpis był ważny dla **uttn.mx**, nawet jeśli wiadomość nie zawierała podpisu DKIM w momencie, gdy dotarła do Twojego serwera.

**Brak podpisu w końcowej wiadomości**:

Gdy wiadomość dotarła do Twojego serwera, mogła nie mieć podpisu DKIM, co spowodowało, że weryfikacja DKIM zakończyła się niepowodzeniem. To może się zdarzyć, jeśli wiadomość została zmodyfikowana w drodze (np. przez serwer pośredniczący) lub jeśli nie została podpisana w ogóle.

**Różnice te mogą wynikać z:**

Zmian w wiadomości podczas jej przesyłania przez różne serwery.

Różnych instancji weryfikacji, które mogą dawać różne wyniki w zależności od tego, na jakim etapie wiadomość była analizowana.

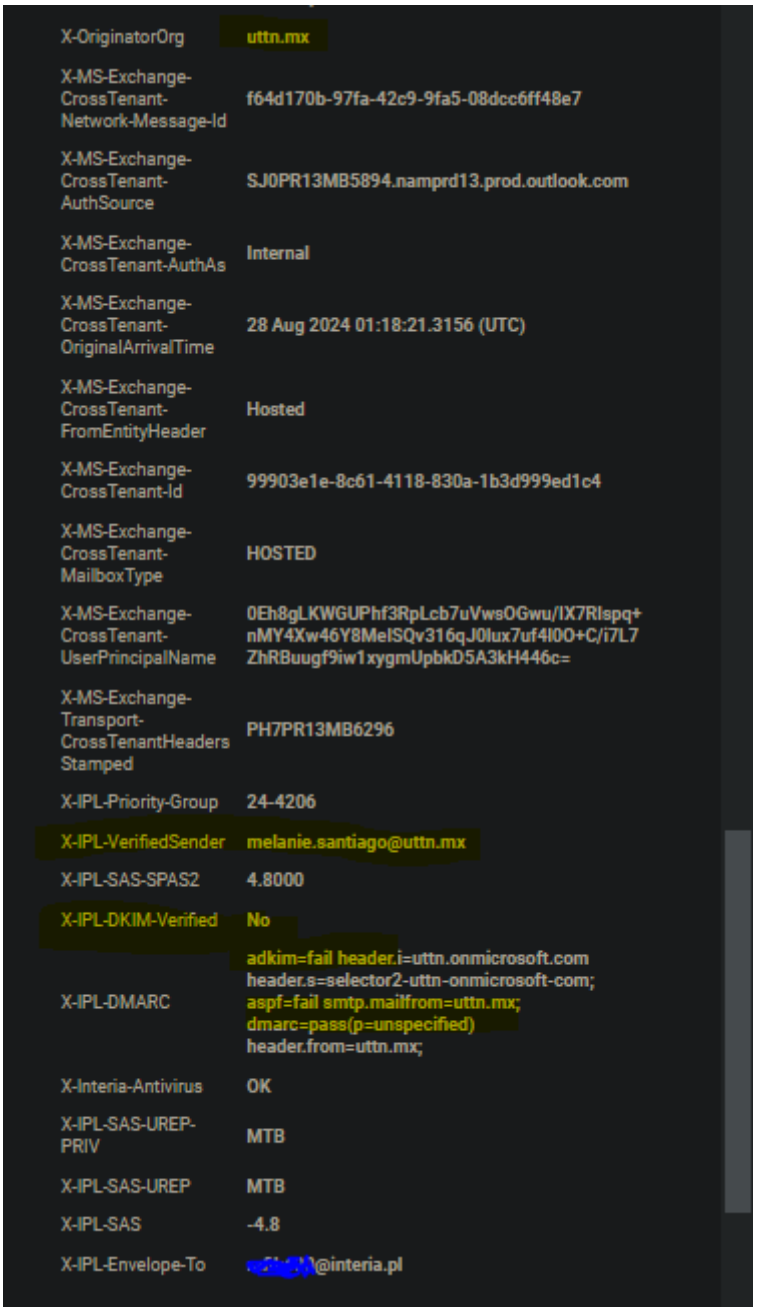
| | |
|---|---|
| Received | from SJ0PR13MB5894.namprd13.prod.outlook.com (2603:10b6:a03:438::22) by PH7PR13MB6296.namprd13.prod.outlook.com (2603:10b6:510:237::7) with Microsoft SMTP Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.7897.18; Wed, 28 Aug 2024 01:18:21 +0000 |
| Received | from SJ0PR13MB5894.namprd13.prod.outlook.com ([fe80::135e:fd02:af74:892a]) by SJ0PR13MB5894.namprd13.prod.outlook.com ([fe80::135e:fd02:af74:892a%5]) with mapi id 15.20.7897.021; Wed, 28 Aug 2024 01:18:21 +0000 |
| Reply-To | policjiinterwencja@gmail.com |
| Subject | =?UTF-8?Q?RE-:// Sprawd=C5=BA-swoj=C4=85_poczt=C4=99_e-mail=5F28=5F08=5F2024=F0=9F=94=B4?= |
| Message-ID | <NyIWBi4ed3IPus7J7TrEgbE2DuJR27mTphM0OhM@LAPTOP-54QPVHAK> |
| X-Mailer | PHPMailer 6.8.0 (https://github.com/PHPMailer/PHPMailer) |
| Content-Type | multipart/mixed; boundary="b1=_NyIWBi4ed3IPus7J7TrEgbE2DuJR27mTphM0OhM" |
| X-ClientProxiedBy | BN9PR03CA0805.namprd03.prod.outlook.com (2603:10b6:408:13f::30) To SJ0PR13MB5894.namprd13.prod.outlook.com (2603:10b6:a03:438::22) |
| MIME-Version | 1.0 |
| X-MS-PublicTrafficType | Email |
| X-MS-TrafficTypeDiagnostic | SJ0PR13MB5894:EE_\|PH7PR13MB6296:EE_ |
| X-MS-Office365-Filtering-Correlation-Id | f64d170b-97fa-42c9-9fa5-08dcc6ff48e7 |
| X-MS-Exchange-SenderADCheck | 1 |
| X-MS-Exchange-AntiSpam-Relay | 0 |

Analizując email dalej możemy zwrócić uwagę na nagłówek **„Received”** oraz **„X-ClientProxiedBy”** co informuje nas że wiadomość przeszła przez kilka serwerów z różnymi adresami IPv6 oraz że że mogła być przetwarzana przez dodatkowy serwer w łańcuchu dostarczania.

**Message-ID** jest unikalnym identyfikatorem wiadomości, który jest generowany przez klienta pocztowego lub serwer i daje nam informację że wiadomość została wygenerowana na lokalnym komputerze z nazwą **„LAPTOP-54QPVHAK”** co może wskazywać że wiadomość była wysyłana z aplikacji na komputerze osobistym.

**X-Mailer** - Ten nagłówek wskazuje, że wiadomość została wysłana za pomocą biblioteki PHPMailer.

**Reply-To: “**policjiinterwencja@gmail.com” informuje nas że ten adres jest używany jako adres do odpowiedzi co budzi duże wątpliwości, ponieważ nie jest zgodny z domeną nadawcy (uttn.mx) i sugeruje nam phishing.

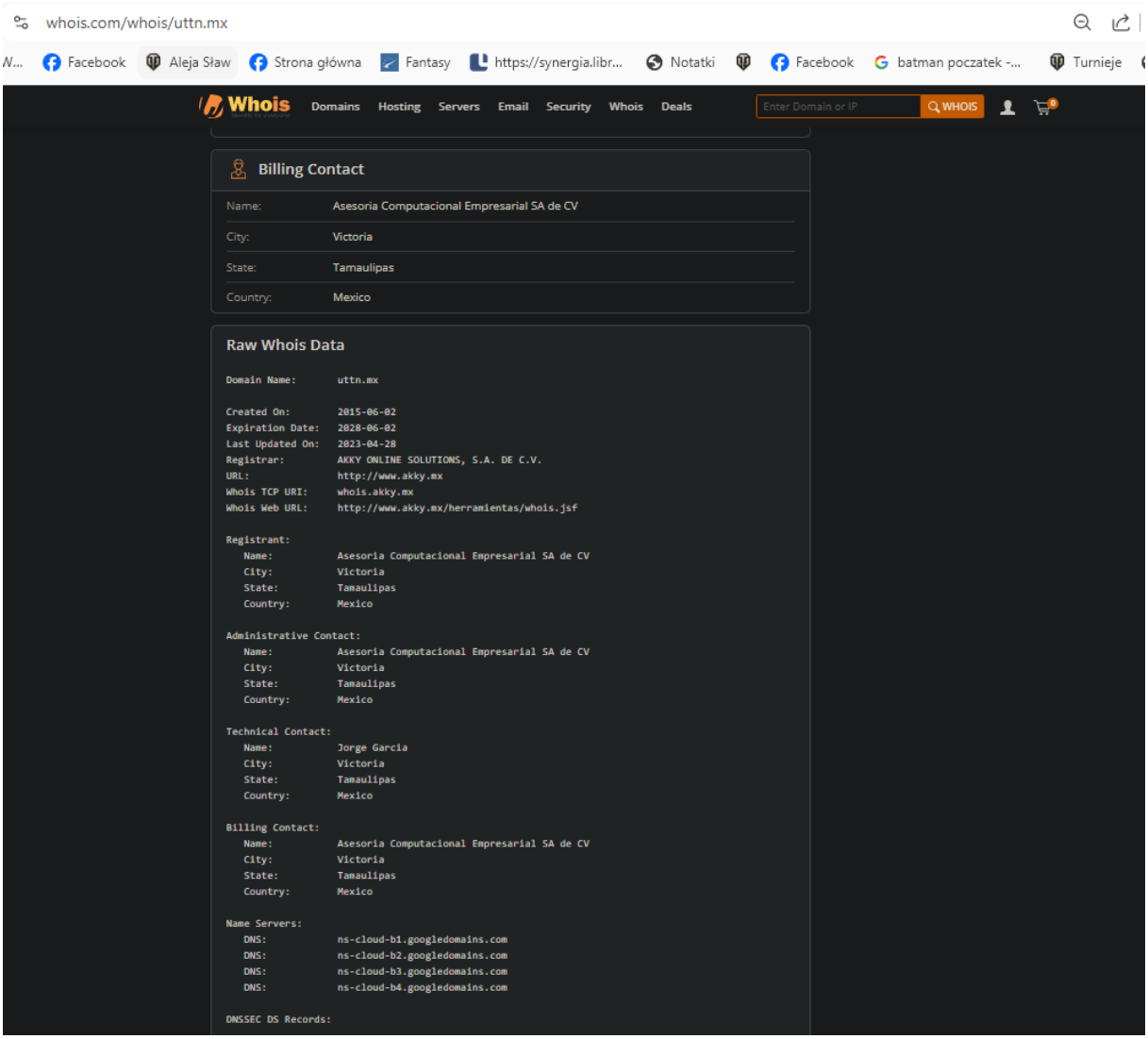


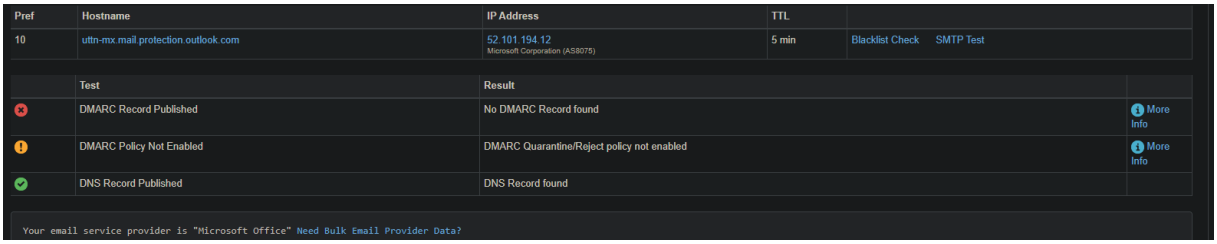
| | |
|---|---|
| X-OriginatorOrg | uttn.mx |
| X-MS-Exchange-CrossTenant-Network-Message-Id | f64d170b-97fa-42c9-9fa5-08dcc6ff48e7 |
| X-MS-Exchange-CrossTenant-AuthSource | SJ0PR13MB5894.namprd13.prod.outlook.com |
| X-MS-Exchange-CrossTenant-AuthAs | Internal |
| X-MS-Exchange-CrossTenant-OriginalArrivalTime | 28 Aug 2024 01:18:21.3156 (UTC) |
| X-MS-Exchange-CrossTenant-FromEntityHeader | Hosted |
| X-MS-Exchange-CrossTenant-Id | 99903e1e-8c61-4118-830a-1b3d999ed1c4 |
| X-MS-Exchange-CrossTenant-MailboxType | HOSTED |
| X-MS-Exchange-CrossTenant-UserPrincipalName | 0Eh8gLKWGUPhf3RpLcb7uVwsOGwu/IX7RIspq+nMY4Xw46Y8MeISQv316qJ0lux7uf4l0O+C/i7L7ZhRBuugf9iw1xygmUpbkD5A3kH446c= |
| X-MS-Exchange-Transport-CrossTenantHeadersStamped | PH7PR13MB6296 |
| X-IPL-Priority-Group | 24-4206 |
| X-IPL-VerifiedSender | melanie.santiago@uttn.mx |
| X-IPL-SAS-SPAS2 | 4.8000 |
| X-IPL-DKIM-Verified | No |
| X-IPL-DMARC | adkim=fail header.i=uttn.onmicrosoft.com header.s=selector2-uttn-onmicrosoft-com; aspf=fail smtp.mailfrom=uttn.mx; dmarc=pass(p=unspecified) header.from=uttn.mx; |
| X-Interia-Antivirus | OK |
| X-IPL-SAS-UREP-PRIV | MTB |
| X-IPL-SAS-UREP | MTB |
| X-IPL-SAS | -4.8 |
| X-IPL-Envelope-To | [redacted]@interia.pl |

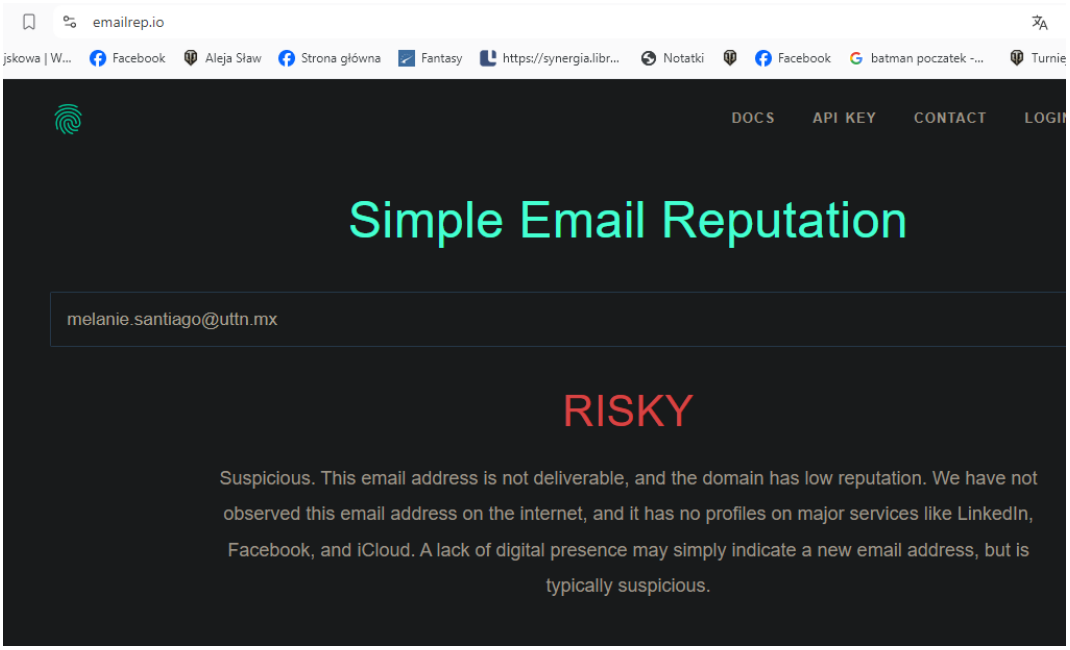
Dalsza naliza potwierdza nam że zweryfikowanym nadawcą jest **„melanie.santiago@uttn.mx”**

Natomiast wiadomość nie przeszła poprawnej weryfikacji SPF i DKIM co informuje nas  że wiadomość nie pochodzi z autoryzowanego serwera oraz nie zostałą podpisana cyfrowo przez prawidłową domenę.

Teraz korzystamy z narzędzi i wyszukujemy informacje o domenie.

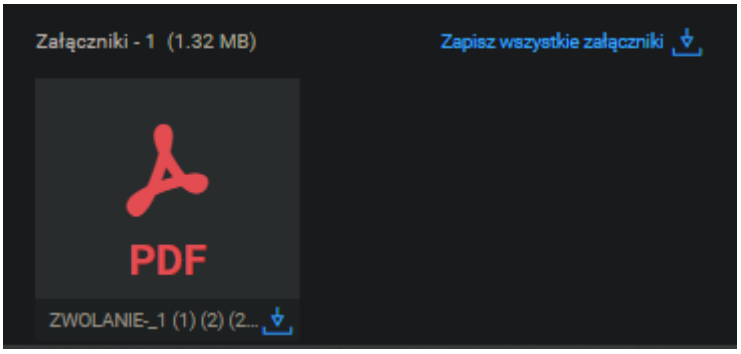


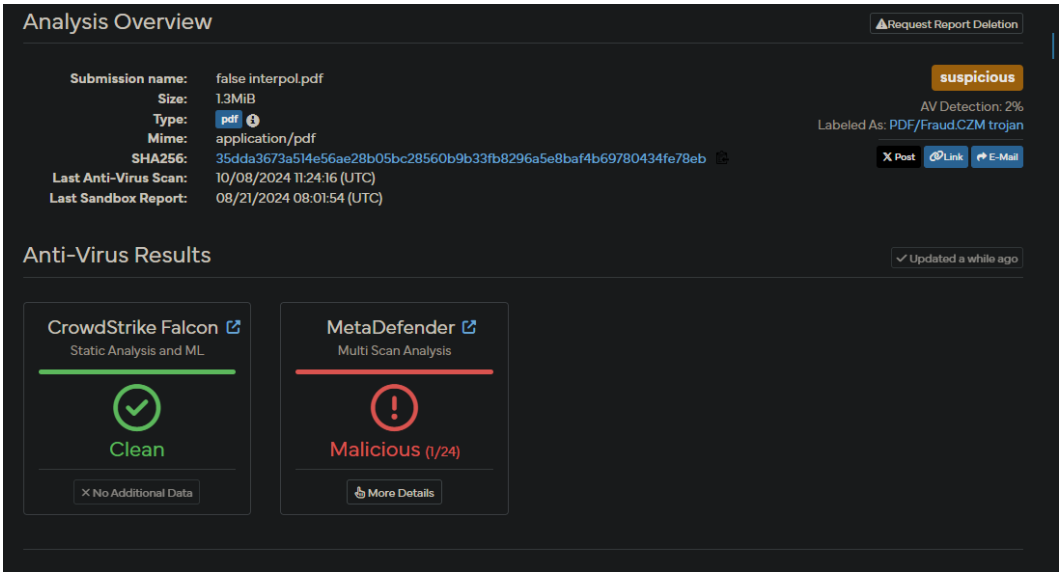


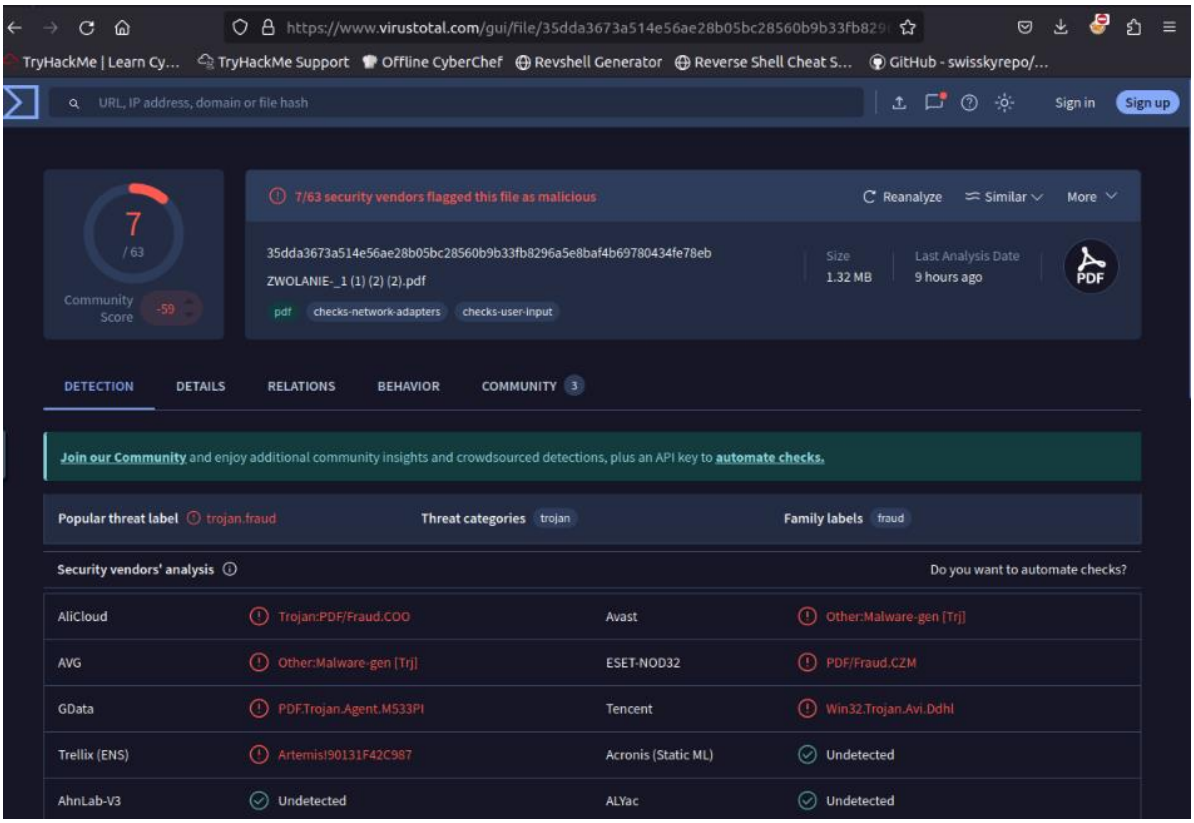

Analiza tekstu oraz polityki SPF/DKIM, skorzystanie z narzędzi potwierdza nam że jest to wiadomość phishingowa a domena ma słabą reputację.

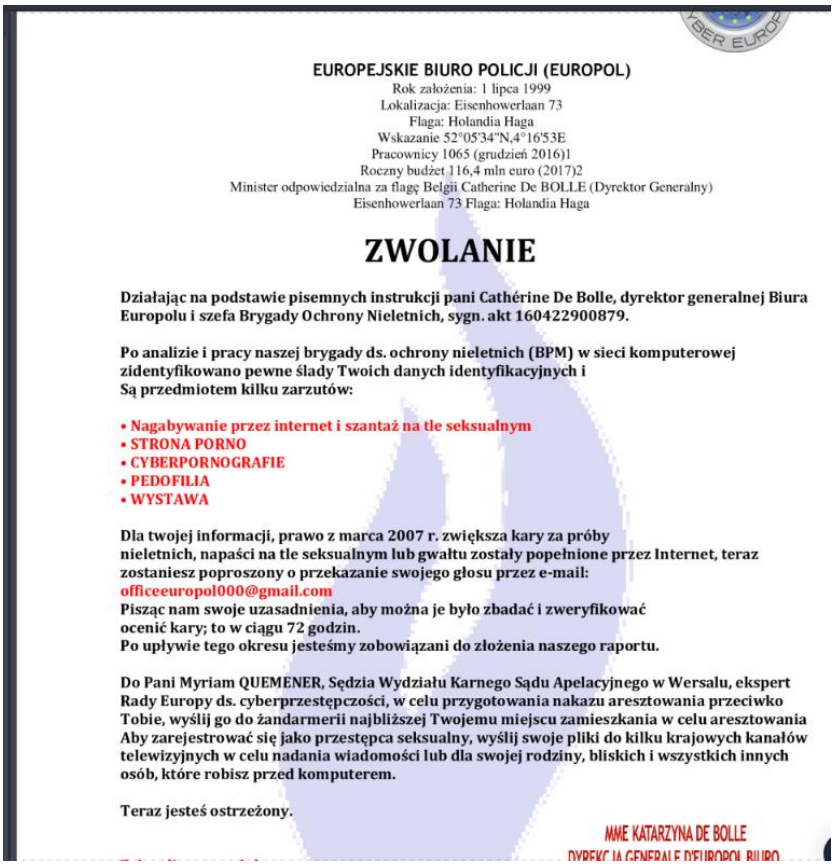
Teraz kolej na zweryfikowanie co jest w załączniku, co ma za zadanie i co to za plik.




Wrzucając plik w Virustotala lub innego zewnętrznego Sandboxa dowiadujemy się żę jest to trojan.





EUROPEJSKIE BIURO POLICJI (EUROPOL)

Rok założenia: 1 lipca 1999
Lokalizacja: Eisenhowerlaan 73
Flaga: Holandia Haga
Wskazanie 52°05'34"N,4°16'53E
Pracownicy 1065 (grudzień 2016)1
Roczny budżet 116,4 mln euro (2017)2
Minister odpowiedzialna za flagę Belgii Catherine De BOLLE (Dyrektor Generalny)
Eisenhowerlaan 73 Flaga: Holandia Haga

# ZWOLANIE

**Działając na podstawie pisemnych instrukcji pani Cathérine De Bolle, dyrektor generalnej Biura Europolu i szefa Brygady Ochrony Nieletnich, sygn. akt 160422900879.**

**Po analizie i pracy naszej brygady ds. ochrony nieletnich (BPM) w sieci komputerowej zidentyfikowano pewne ślady Twoich danych identyfikacyjnych i Są przedmiotem kilku zarzutów:**

- **Nagabywanie przez internet i szantaż na tle seksualnym**
- **STRONA PORNO**
- **CYBERPORNOGRAFIE**
- **PEDOFILIA**
- **WYSTAWA**

**Dla twojej informacji, prawo z marca 2007 r. zwiększa kary za próby nieletnich, napaści na tle seksualnym lub gwałtu zostały popełnione przez Internet, teraz zostaniesz poproszony o przekazanie swojego głosu przez e-mail:**
**officeeuropol000@gmail.com**
**Pisząc nam swoje uzasadnienia, aby można je było zbadać i zweryfikować ocenić kary; to w ciągu 72 godzin.**
**Po upływie tego okresu jesteśmy zobowiązani do złożenia naszego raportu.**

**Do Pani Myriam QUEMENER, Sędzia Wydziału Karnego Sądu Apelacyjnego w Wersalu, ekspert Rady Europy ds. cyberprzestępczości, w celu przygotowania nakazu aresztowania przeciwko Tobie, wyślij go do żandarmerii najbliższej Twojemu miejscu zamieszkania w celu aresztowania Aby zarejestrować się jako przestępca seksualny, wyślij swoje pliki do kilku krajowych kanałów telewizyjnych w celu nadania wiadomości lub dla swojej rodziny, bliskich i wszystkich innych osób, które robisz przed komputerem.**

**Teraz jesteś ostrzeżony.**

MME KATARZYNA DE BOLLE

Wynik: Plik zawiera w sobie złośliwe makra.

**Podsumowanie:**

W analizowanym przypadku phishingu, jako analityk SOC należy podjąć kilka kluczowych kroków. Po potwierdzeniu, że wiadomość jest próbą phishingu, pierwszym działaniem powinno być **zablokowanie złośliwej domeny**, aby zapobiec dalszym atakom. Następnie należy przeprowadzić szczegółową inspekcję, aby ustalić, które adresy e-mail w organizacji otrzymały wiadomość oraz czy któryś z użytkowników otworzył załączniki lub kliknął w złośliwe linki czy podał wrażliwe dane.

W przypadku, gdy użytkownik pobrał lub uruchomił podejrzany plik, należy **natychmiast odłączyć jego system od sieci**, aby ograniczyć potencjalne rozprzestrzenianie się zagrożenia. Kolejnym krokiem jest przywrócenie **kopii zapasowej systemu** oraz przeprowadzenie dokładnej analizy, aby upewnić się, że nie doszło do trwałej infekcji.

Na koniec, kluczowym elementem reakcji na taki incydent powinno być **przeszkolenie użytkownika**. Dzięki temu zminimalizuje się ryzyko wystąpienia podobnych incydentów w przyszłości i zwiększy świadomość zagrożeń w organizacji.