

Scenariusz „ analiza Phishingowego emaila”

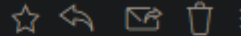
Email który otrzymaliśmy

Konieczność Zaktualizowania Informacji Konta

Netflix

do Ja

10 sty



Wykryliśmy problem z danymi rozliczeniowymi powiązanymi z Państwa kontem.

Witam!

Niestety, nie mogliśmy zatwierdzić płatności za kolejny cykl rozliczeniowy Państwa subskrypcji, co spowodowało tymczasowe zawieszenie członkostwa. Jednak obecna subskrypcja pozostaje aktywna do czasu jej wygaśnięcia.

Aby utrzymać nieprzerwany dostęp do najlepszych programów telewizyjnych i filmów, prosimy o zaktualizowanie swoich danych, klikając poniższy przycisk.

Kliknij, aby zaktualizować swoje konto

* Link wygasa po 15 minutach.

Zabezpiecz konto: Jeśli nie wiesz, kto przesłał prośbę, najlepiej bezzwłocznie wyloguj się ze wszystkich urządzeń, których nie rozpoznajesz. Możesz także zmienić hasło.

Chętnie odpowiemy na Twoje pytania

Odwiedź Centrum pomocy, aby uzyskać więcej informacji.

Zespół Netflix

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”

Netflix
do Ja
10 sty

Data: Wed, 10 Jan 2024 07:51:46 +0000

Od: Netflix <kontakt@krmeni.pl>

Do: [redacted]

Received: from fmx21.pf.interia.pl (localhost [127.0.0.1]) by fmx21.pf.interia.pl (Postfix) with ESMTP id 061822008D40E for <[redacted]@interia.pl>; Wed, 10 Jan 2024 08:52:23 +0100 (CET)

X-Envelope-From: <bounce@krmeni.pl>

Received: from dedicated-aie71.rev.nazwa.pl (dedicated-aie71.rev.nazwa.pl [77.55.212.71]) (using TLSv1.2 with cipher ECDHE-ECDSA-AES256-GCM-SHA384 (256/256 bits)) (No client certificate requested) by fmx21.pf.interia.pl (Postfix) with ESMTPS for [redacted]@interia.pl; Wed, 10 Jan 2024 08:52:21 +0100 (CET)

DKIM-Signature: v=1; a=rsa-sha1; c=relaxed/relaxed; s=key; d=krmeni.pl; h=Date:To:From:Reply-To:Subject:Message-ID:List-Unsubscribe:MIME-Version:Content-Type; i=kontakt@krmeni.pl; bh=cnrZoo9HWGQAJOXWgli4dtAajHg=; b=Rs3qEjF4r/YO6ixSEY6XF2tag7EP0Pn+Titrm+n91AEaSu7Pp+CnT1iWKIS8/KMTVICRegaDCXl9HPwKtrjUJ4K5NaDSPIQ5f8y6ZXSZRZnhmclC9MxIdzXt01Y00b0XEqnWpm3uuSonAxC/FTZXRFwv76NHKHS/L/EarmUvdHD+Q=

DomainKey-Signature: a=rsa-sha1; c=nores; q=dns; s=key; d=krmeni.pl; b=RW3wJIGECdegv3RS/10coAkKIdgZ9H8+GEzNOYsL04esVRdvpJm7xOG4iJ8r1NT+NIQsQl8lQTOHqb1bdhx9OZQ20N5duvqoPyRoHAuLGE1hxaywkamccEWfQy0eORAXLeCmK7kvPphASO6XJ+R1z7cFOhV4xOV7M8yg1mgAb4=;

Reply-To: kontakt@krmeni.pl

Subject: =?UTF-8?Q?Konieczno=C5=9B=C4=87_Zaktualizowania_Info rmacji_Konta?=

Message-ID: <e1e5bf41c2e4fdc7dc967b6d84b1e65@amdgrupas.pl>

List-Unsubscribe: <https://amdgrupas.pl/unsubscribe.php?id=PGUxZTViZjQxYzJINGZkY2Y3ZGM5NjdiNmQ4NGlxZTY1QGfZGdydXBhcy5wbD4%3D>

Tracking-ID: <e1e5bf41c2e4fdc7dc967b6d84b1e65@amdgrupas.pl>

Precedence: bulk

MIME-Version: 1.0

Content-Type: multipart/alternative; boundary="b1_d2a7730db699c113db01b89f88e bbb37"

X-IPL-Priority-Group: 24-1708

X-IPL-VerifiedSender: bounce@krmeni.pl

X-IPL-SAS-SPAS2: 8.0605

X-IPL-DKIM-Verified: Yes

X-IPL-DMARC: adkim=pass header.i=krmeni.pl header.s=key; aspf=pass smtp.mailfrom=krmeni.pl; dmarc=pass(p=none) header.from=krmeni.pl;

X-Interia-Antivirus: OK

X-IPL-SAS-UREP: -1

X-IPL-SAS-UREP-PRIV: 0

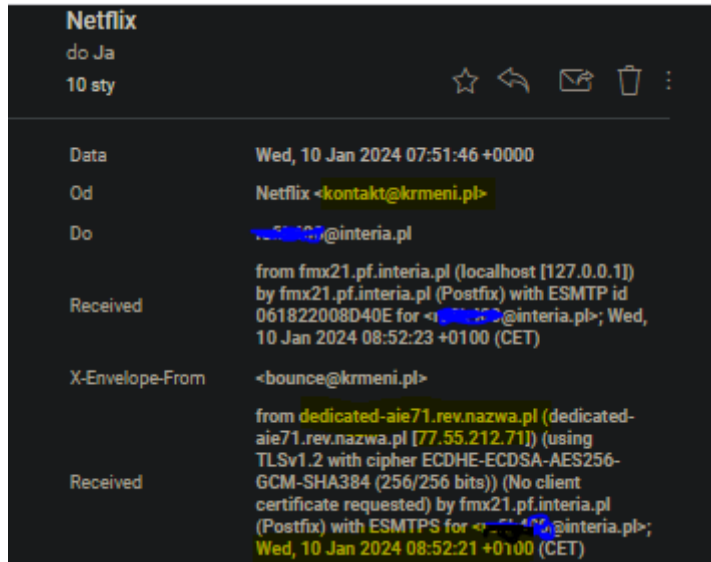
X-IPL-SAS: -9.061

Zabezpiecz konto.

Analiza techniczna

„Nagłówki wiadomości”

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 Netflix 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

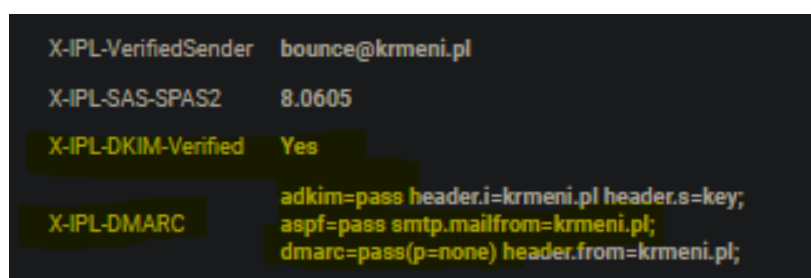
Następnie sprawdzamy nagłówki SPF/DKIM/DMARC

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.

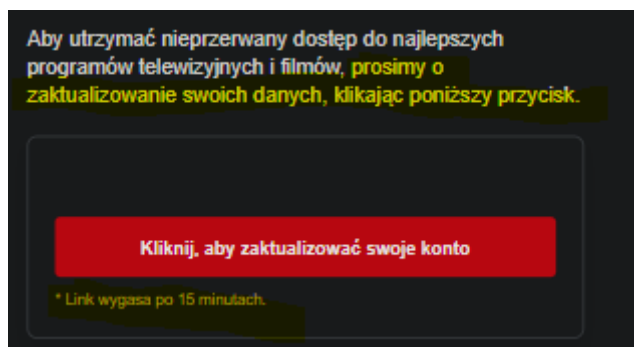
SPF (aspf=pass) wskazuje, że serwer SMTP wysyłający wiadomość jest autoryzowany przez domenę krmeni.pl. To sugeruje, że serwer jest uprawniony do wysyłania e-maili z tej domeny, ale nie gwarantuje, że sama domena jest legalna. Atakujący mogą skonfigurować serwery SMTP, które przechodzą weryfikację SPF, 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 Netflix'a udowodniliśmy sprawdzając poprawną domenę którą używa Netflix) założmy że przeoczyliśmy jedną literówkę w emailu albo że adres 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 dane czy URLów prowadzących do zewnętrznych 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](https://motofuria[.]bernadetalena[.]pl/patrykkewin/tumójemailnteria[.]pl)

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

Dla przykładu wynik który pierwotnie powinniśmy otrzymać z Virustotala.

Security vendors' analysis ⓘ		Do you want to automate checks?
BitDefender	⚠ Malware	
CRDF	⚠ Malicious	
CyRadar	⚠ Malicious	
Fortinet	⚠ Malware	
G-Data	⚠ Phishing	
Lionic	⚠ Malicious	
Sophos	⚠ Malware	
Spamhaus	⚠ Phishing	
ADMINUSLabs	✓ Clean	
AlienVault	✓ Clean	
Antiy-AVL	✓ Clean	
Artists Against 419	✓ Clean	
Avira	✓ Clean	
BADWARE.INFO	✓ Clean	

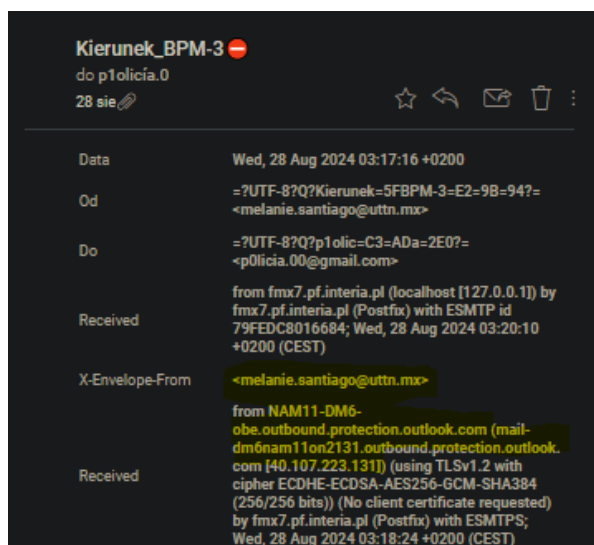
Analiza Techniczna

Scenariusz: 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 postępowania.” 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 nadawcę w tym przypadku będzie to „**melanie.santiago@uttn.mx**”

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

oraz odbiorce w tym przypadku **”policia.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.

	<pre>04KTwtvdHg287Ziq187qT6l6duTqWpezF+Gcvw == 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=fae9Msoah7JV7tjwWbFh8V/q+C/R+z83wki C6xdJMQ=; b=oacscnZ6aXV1MvvAK7zLq+12XfWxCdz/EShk rtP0LBKX8hSPeNcl1R1M32600DfZax+fCjxfLKH 5funMeskn903tnJ+oRdpUwdjldvFWJtTxLY+szw6 OwvvV6iWKWp4JXtMktEUxhkjMK408X9GcK2c vIZM/ISD7H2Sr49WFqdRg2r56GGTXInFmPiroct Y0VonHkPOqyl7lk1rO49HW/J7yhz7y7/x1+V63M CDuAE2o7KeitxIDcBkjEamOm3sFuui2sLE9rJJvX eN4TGGAY4XRQ0ptgPOK/ltQvPc9lfvwrth262ua R4D6ssN3lbVFAIFWqCOyZnPg2yKtWHA==</pre>
ARC-Message- Signature	
ARC-Authentication- Results	<pre>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</pre>
DKIM-Signature	<pre>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=fae9Msoah7JV7tjwWbFh8V/q+C/R+z83wki C6xdJMQ=; b=hrV43GOr7tl/IMJ4ILTNYo9leMAWhgGwMPHE 7EQHL2qUtu699ftrSYzca3C25GtHeSaNkgmIEPK De+N7lbNd/+9kxNO/PkQOO7YE6cRptZQKPWL5 SynTajSJ/7Gk6XoeZa01TSC0iW4I047Zwgle5qiN fZcPuO3laP2gfjVhypE=</pre>
Authentication- Results	<pre>dkim=none (message not signed) header.d=none;dmarc=none action=none header.from=uttn.mx;</pre>
Received	<pre>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</pre>
Received	<pre>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</pre>

Widzimy że wiadomość najpierw posiada autoryzację SPF, SMTP, DKIM a później nie, czym to jest spowodowane, co to oznacza i dalszego 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 (ffe80::135e:fd02:af74:892a) by SJ0PR13MB5894.namprd13.prod.outlook.com (ffe80::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=B47=
Message-ID	<NylWBi4ed3IPus7J7TrEgbE2DuJR27mTphM00 hM@LAPTOP-54QPVHAK>
X-Mailer	PHPMailer 6.8.0 (https://github.com/PHPMailer/PHPMailer)
Content-Type	multipart/mixed; boundary="b1=_NylWBi4ed3IPus7J7TrEgbE2DuJ R27mTphM00hM"
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_JPH7PR13MB6296: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 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+nMY4Xw46Y8MeISQv316qJ0lux7uf4i0O+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	54QPVHAK@interia.pl

Dalsza analiza 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 została podpisana cyfrowo przez prawidłową domenę.

Teraz korzystamy z narzędzi i wyszukujemy informacje o domenie.

whois.com/whois/uttn.mx

Facebook Aleja Sław Strona główna Fantasy https://synergia.lib... Notatki Facebook batman poczatek ~... Turnieje

Whois Domains Hosting Servers Email Security Whois Deals Enter Domain or IP WHOIS

Billing Contact

Name: Asesoría Computacional Empresarial SA de CV
City: Victoria
State: Tamaulipas
Country: Mexico

Raw Whois Data

Domain Name: uttn.mx
Created On: 2015-06-02
Expiration Date: 2028-06-02
Last Updated On: 2023-04-28
Registrar: AKKY ONLINE SOLUTIONS, S.A. DE C.V.
URL: http://www.akky.mx
Whois TCP URI: whois.akky.mx
Whois Web URL: http://www.akky.mx/herramientas/whois.jsf

Registrant:
Name: Asesoría Computacional Empresarial SA de CV
City: Victoria
State: Tamaulipas
Country: Mexico

Administrative Contact:
Name: Asesoría Computacional Empresarial SA de CV
City: Victoria
State: Tamaulipas
Country: Mexico

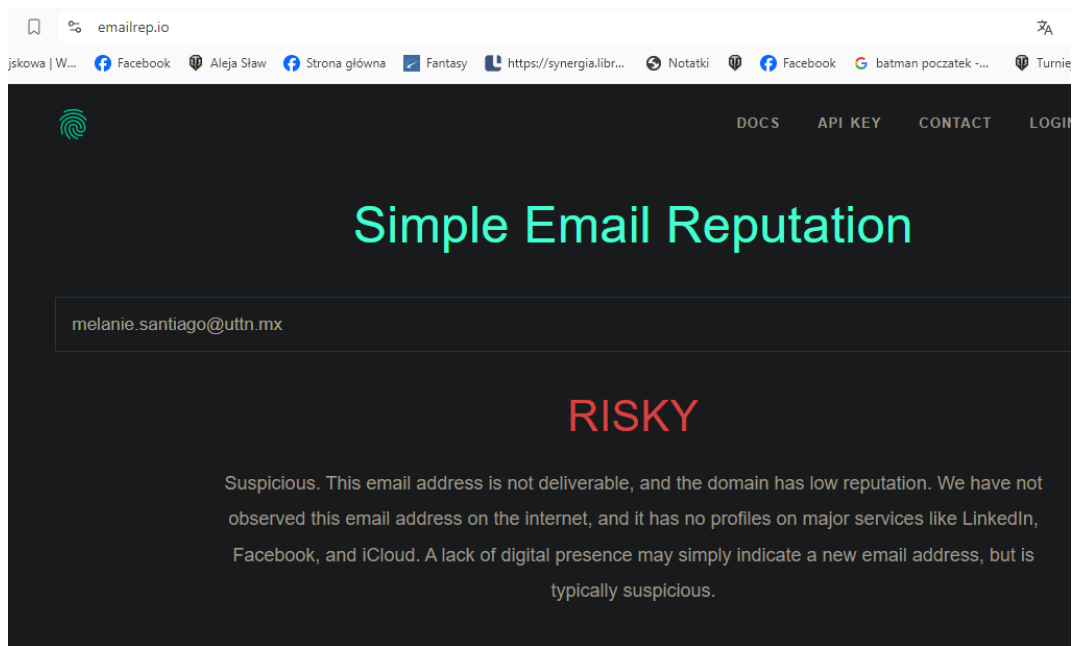
Technical Contact:
Name: Jorge Garcia
City: Victoria
State: Tamaulipas
Country: Mexico

Billing Contact:
Name: Asesoría Computacional Empresarial SA de CV
City: Victoria
State: Tamaulipas
Country: Mexico

Name Servers:
DNS: ns-cloud-b1.googledomains.com
DNS: ns-cloud-b2.googledomains.com
DNS: ns-cloud-b3.googledomains.com
DNS: ns-cloud-b4.googledomains.com

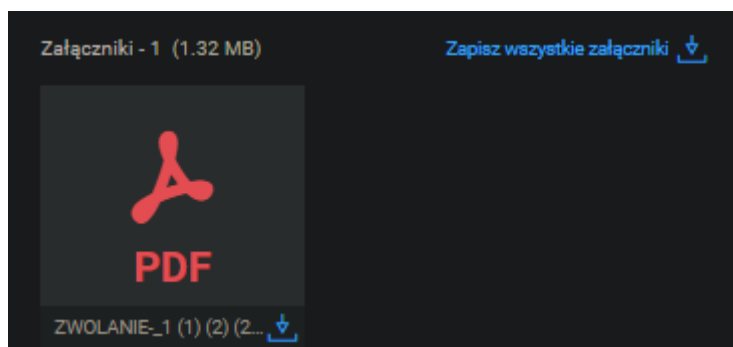
DNSSEC DS Records:

Pref	Hostname	IP Address	TTL	
10	uttn-mx.mail.protection.outlook.com	52.101.194.12 Microsoft Corporation (AS8075)	5 min	Blacklist Check SMTP Test
	Test	Result		
✖	DMARC Record Published	No DMARC Record found		More Info
⚠	DMARC Policy Not Enabled	DMARC Quarantine/Reject policy not enabled		More Info
✔	DNS Record Published	DNS Record found		
Your email service provider is "Microsoft Office" Need Bulk Email Provider Data?				

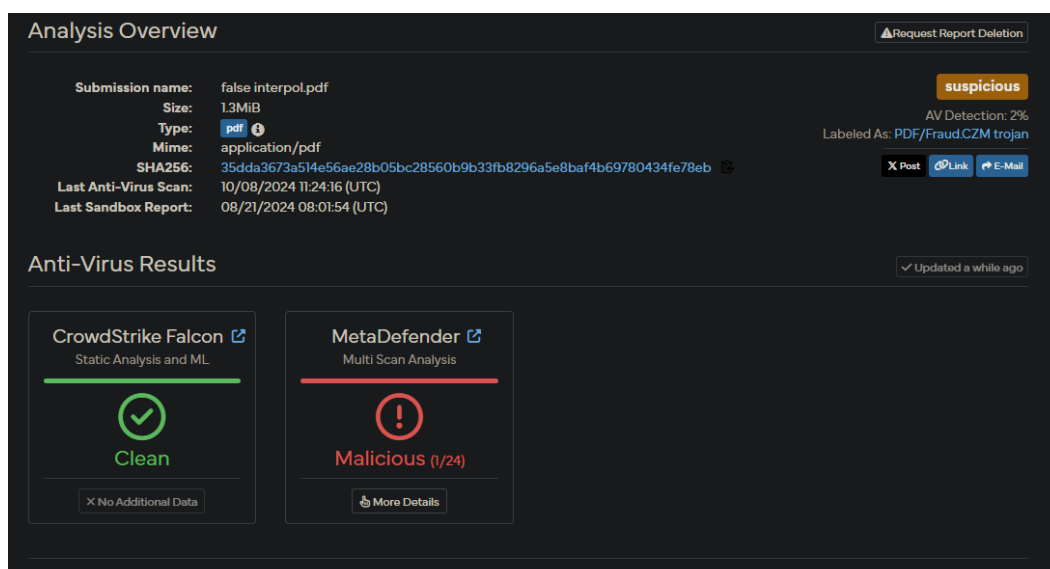


Analiza tekstu oraz polityki SPF/DKIM, skorzystanie z narzędzi potwierdza nam że jest to wiadomość phishingowa a domena ma słabą reputację.

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 że jest to trojan.



← → ↻ 🏠 🔒 https://www.virustotal.com/gui/file/35dda3673a514e56ae28b05bc28560b9b33fb8291... 📄 ⬇️ 📁 📄 📄 📄

TryHackMe | Learn Cy... TryHackMe Support 📞 Offline CyberChef 🌐 Revshell Generator 🌐 Reverse Shell Cheat S... 📄 GitHub - swisskyrepo/...

🔍 URL, IP address, domain or file hash | 📄 📄 📄 📄 📄 Sign in Sign up

Community Score: 7/63

-59

🚫 7/63 security vendors flagged this file as malicious

Reanalyze Similar More

35dda3673a514e56ae28b05bc28560b9b33fb829a5e8baf4b69780434fe78eb

Size: 1.32 MB Last Analysis Date: 9 hours ago

PDF

pdf checks-network-adapters checks-user-input

DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY 3

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Popular threat label: trojan.fraud Threat categories: trojan Family labels: fraud

Security vendors' analysis: Do you want to automate checks?

AliCloud	🚫 Trojan:PDF/Fraud.COO	Avast	🚫 Other:Malware-gen [Tri]
AVG	🚫 Other:Malware-gen [Tri]	ESET-NOD32	🚫 PDF/Fraud.C2M
GData	🚫 PDF.Trojan.Agent.M533PI	Tencent	🚫 Win32.Trojan.Avi.Ddhl
Trellix (ENS)	🚫 ArtemisI90131F42C987	Acronis (Static ML)	✅ Undetected
AhnLab-V3	✅ Undetected	ALYac	✅ Undetected

EUROPEJSKIE BIURO POLICJI (EUROPOL)

Rok założenia: 1 lipca 1999
Lokalizacja: Eisenhowerlaan 73
Flaga: Holandia Haga
Wskazanie 52°05'34"N, 4°16'53"E
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 Catherine 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
DYREKTOR GENERALNA BUREAU EUROPEEN DE POLICE

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.