MP Legal
Mielech Panek i wspólnicy sp.k.

15.10.2024 r.

KOMUNIKAT IOD

-

ANALIZA NAJNOWSZYCH SZTUCZEK CYBEROSZUSTÓW

MP LEGAL MIELECH, PANEK I WSPÓLNICY SP.K.
Kontakt telefoniczny 00 48 17 200 08 85
Adres e-mail biuro@mpls.com.pl
Dane adresowe: ul. Kreczmera 4/4, 35-065 Rzeszów

NIP: 8133900675 **KRS:** 0001046158, Sąd Rejonowy w Rzeszowie, XII Wydział Krajowego Rejestru Sądowego
Oddział Kraków: ul. Mazowiecka 25, 30-019 Kraków, **Oddział Gdańsk**: ul. Zwycięstwa 13A, 80-219 Gdańsk

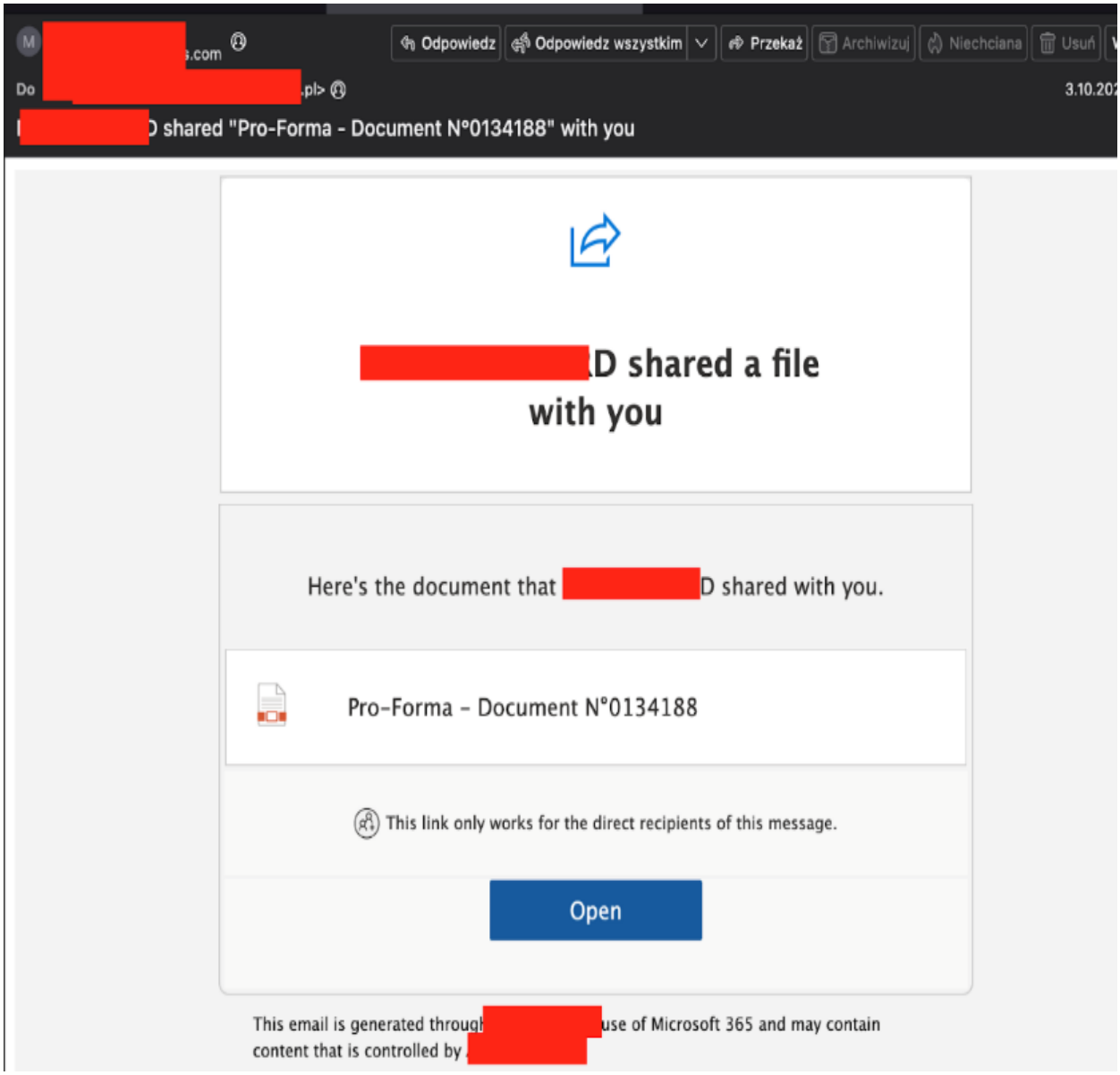
I. Wstęp.

Phishing to rodzaj cyberataku, w którym oszuści podszywają się pod zaufane instytucje lub osoby, aby wyłudzić poufne dane, takie jak hasła czy informacje bankowe. Atak zwykle rozpoczyna się od fałszywego e-maila lub wiadomości z linkiem do strony imitującej autentyczną witrynę. Użytkownik, sądząc, że loguje się na prawdziwej stronie, wprowadza dane, które trafiają do cyberprzestępców. Celem phishingu jest kradzież tożsamości lub danych finansowych ofiary.

Większość z nich ma na celu wyłudzenie danych logowania, informacji finansowych i danych osobowych. Ten rodzaj ataków nieustannie rośnie i wykorzystuje coraz bardziej zaawansowane techniki, w tym sztuczną inteligencję oraz skomplikowane schematy podszywania się pod zaufane osoby. W porównaniu, inne formy cyberataków, takie jak ransomware czy ataki typu denial-of-service, stanowią znacznie mniejszy odsetek, przy czym ransomware to około 2-3% ataków w sektorach biznesowym i charytatywnym. Powszechne występowanie phishingu w różnych branżach i regionach podkreśla konieczność wprowadzenia bardziej zaawansowanych szkoleń i systemów ochrony w organizacjach, aby zmniejszyć ryzyko naruszenia danych i strat finansowych.

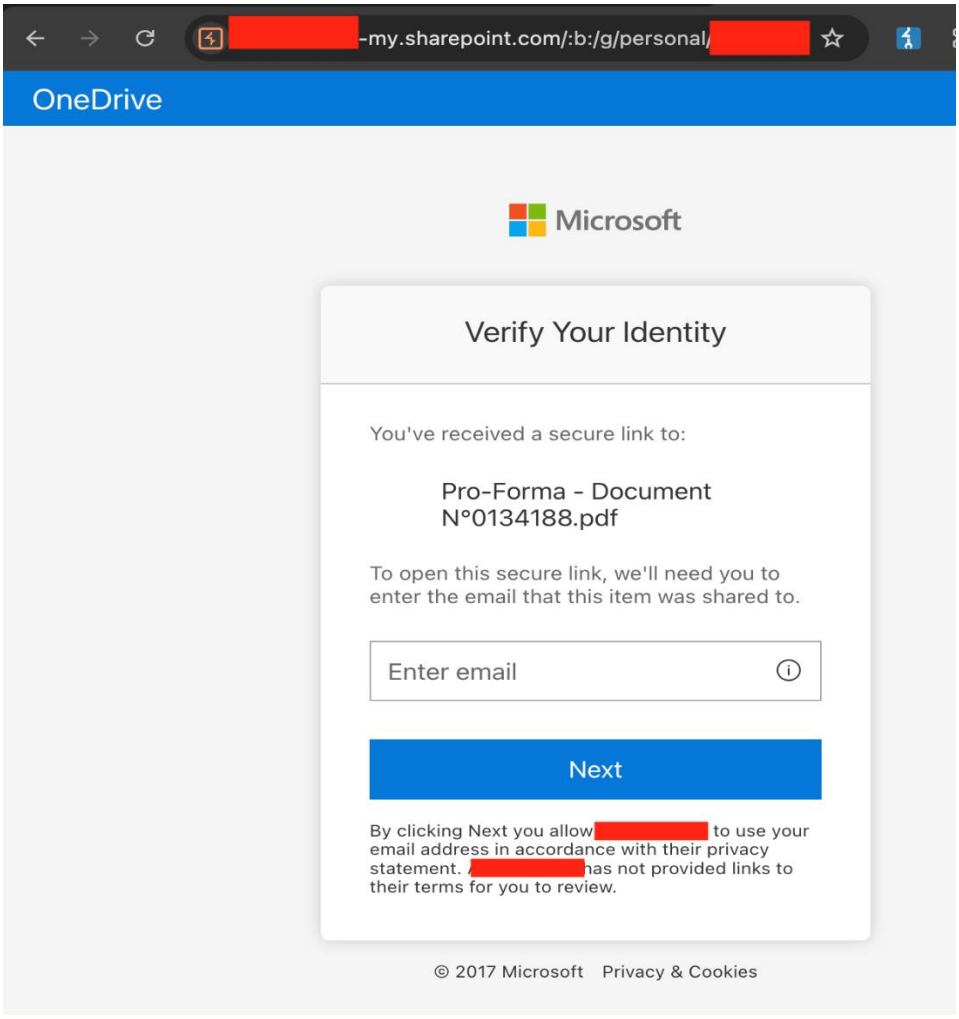
II. Analiza najnowszych sztuczek cyberoszustów

- **Podejrzana treść wiadomości elektronicznej:** Adresat zweryfikował błąd w numeracji faktur, która odbiegała od standardu używanego z Organizacji. Wysłał maila do analizy analitykom bezpieczeństwa.
  Poniżej znajduje się treść maila:

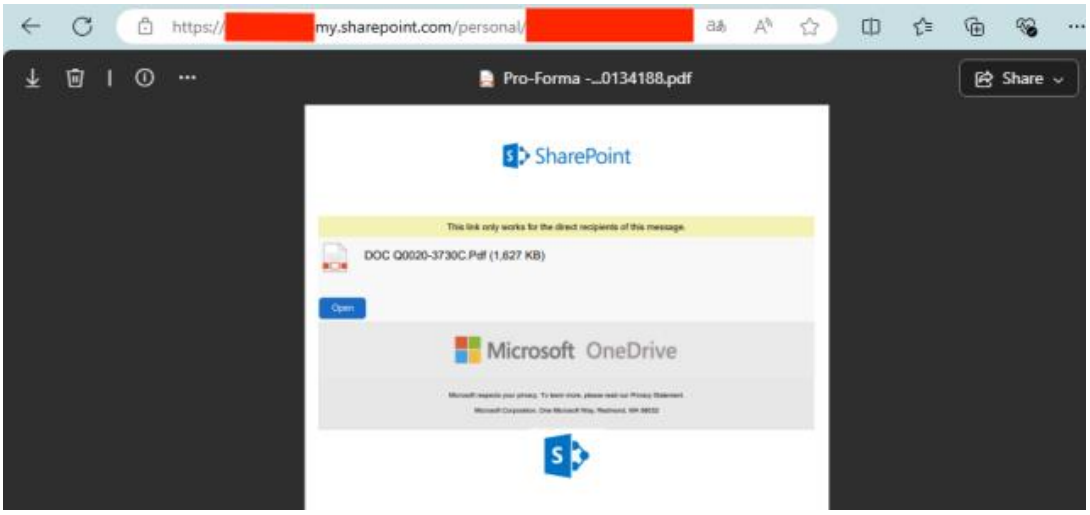


- **Nadawca wiadomości:** Wiadomość elektroniczna nie trafiła do SPAMU. gdyż wysłano go z realnego środowiska Microsoft, tj. istniejącej organizacji na platformie Microsoft 365. Prawdopodobnie adres e-mail kontrahenta został już wcześniej przejęty przez atakujących, co znacząco podnosiło wiarygodność przygotowanego ataku.

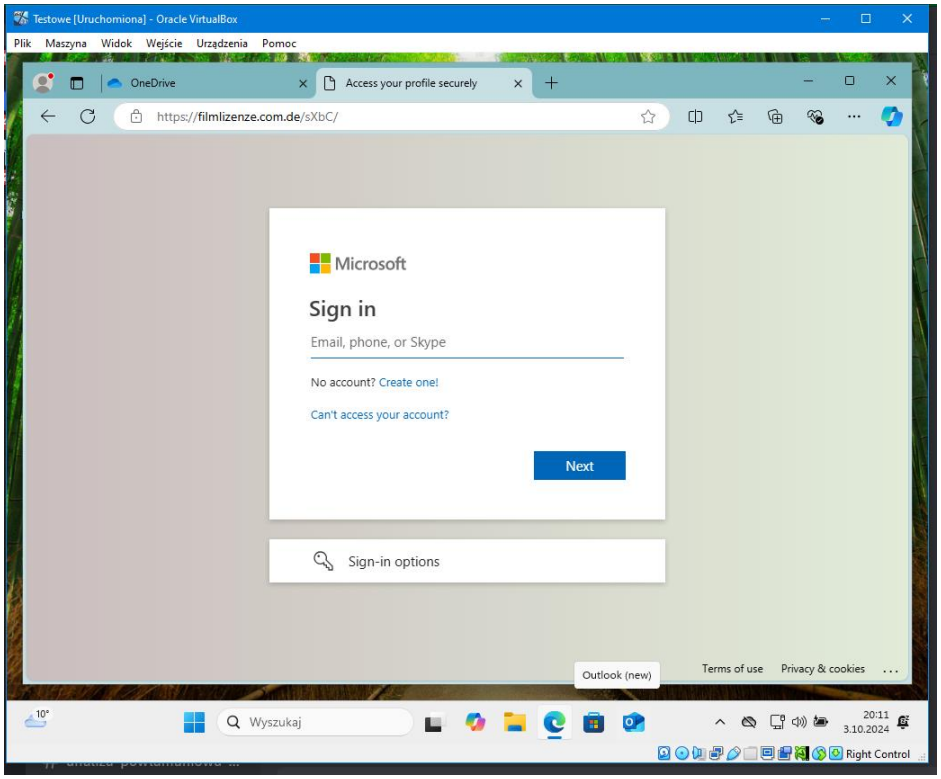
- **Analiza kampanii phishingowej:** Odnośnik w wiadomości odsyła do strony do uwierzytelnienia, która prosi o potwierdzenie tożsamości z wykorzystaniem jednorazowego kodu, wysyłanego na adres e-mail podany przez użytkownika.



Otwierana strona wzbudza zaufanie użytkownika poprzez wykorzystanie systemu Microsoft. Działanie to ma za zadanie uśpić czujność ofiary. Po zweryfikowaniu kodem, aplikacja otwiera dokument PDF w oknie przeglądarki. Dochodzimy do punktu kulminacyjnego ataku – przestępca używa dokumentu wyglądającego jak strona platformy Sharepoint, zachęcającą do otwarcia pliku poprzez kliknięcie w przycisk Open.



Kliknięcie przycisku powoduje uruchomienie rzeczywistej strony phishingowej.



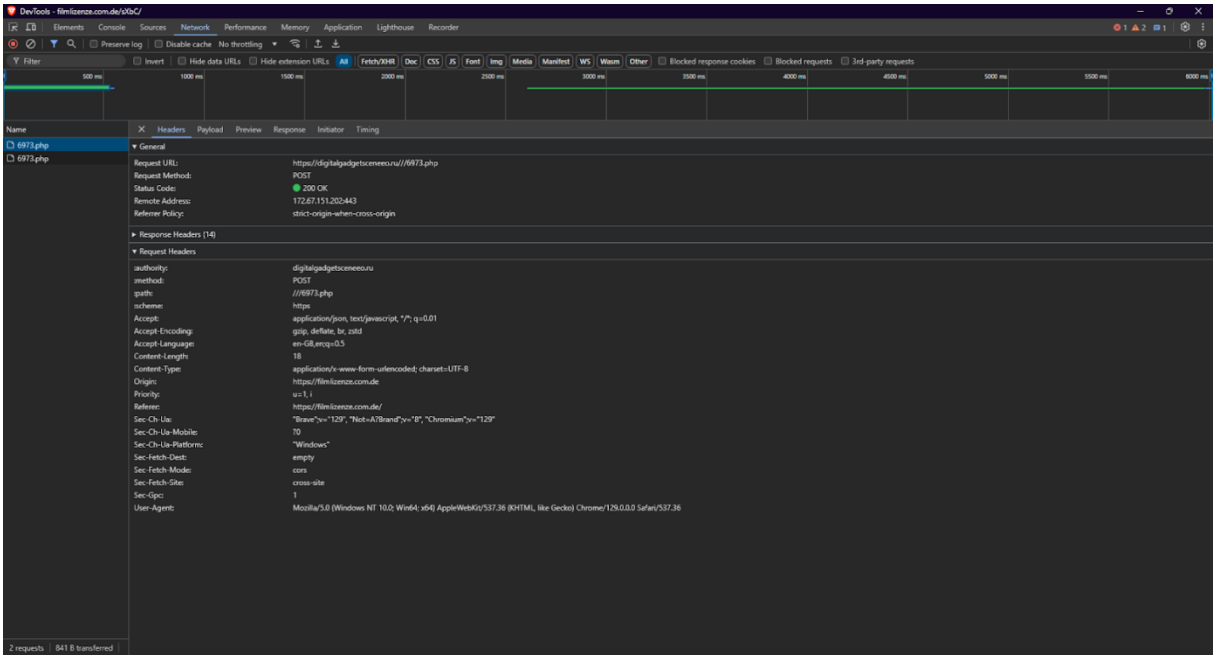
W pasku adresu tym razem widać adres inny od oryginalnych hostów usług Microsoft.

Po analizie podszytej strony internetowej wynika, że:

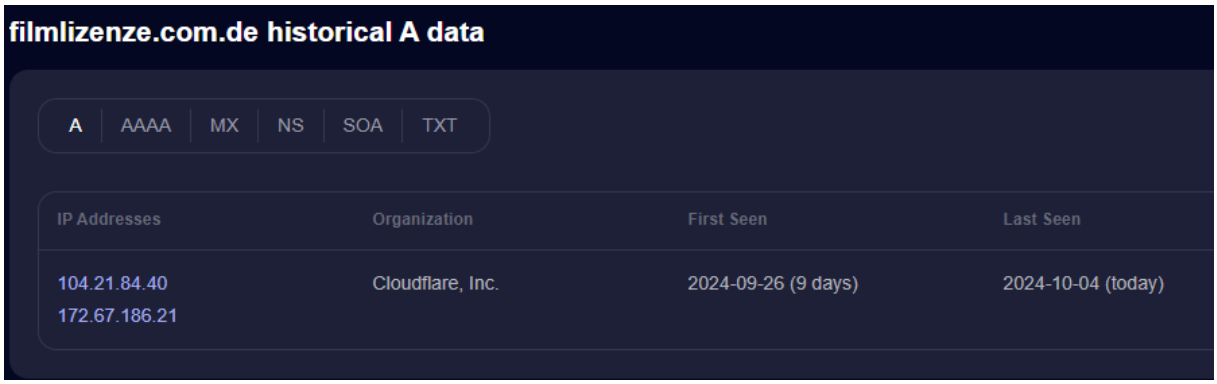
- pierwsze, co użytkownik zobaczył po wejściu w kopię strony, to animacja ikony niebieskiego listu;
- cała strona jest w pełni responsywna i nie ma odnośników do innych usług MS;
- w źródle strony kod odpowiedzialny za wygląd i mechanikę panelu logowania jest obfuskowany w JavaScript;
- w źródle strony sporo informacji zawierających treści udające legalną witrynę internetową ukryto za pomocą CSS (display: none) w celu ominięcia heurystyki silników wykrywających strony phishingowe;
- użyte zostały biblioteki szyfrujące (obfuskacja) – tzn. Zaciemnianie kodu to technika przekształcania programów, która zmienia składnię, ale zachowuje ich semantykę, co znacząco utrudnia ich zrozumienie. Istnieją również narzędzia (obfuskatory) modyfikujące kod źródłowy, pośredni bądź binarny w celu utrudnienia inżynierii wstecznej programu.
- Podglądając ruch sieciowy po uruchomieniu podszytej strony, udało się ustalić, że szyfrowana zawartość (zawierająca finalny widok panelu logowania) pobierana była z serwera, którego domena wskazuje na rosyjskie pochodzenie (ta jednak, jak i pozostałe, była obsługiwana przez Cloudflare).

#	Host	Metho	URL	Params	Edited	Status co	Length	MIME ty	Exte
4901	https://filmlizenze.com.de	POST	/sXbC/	✓		200	567	HTML	
4900	https://filmlizenze.com.de	GET	/sXbC/,			404	1871	HTML	
4899	https://code.jquery.com	GET	/jquery-3.6.0.min.js			200	90097	script	js
4898	https://filmlizenze.com.de	GET	/sXbC/,			404	1869	HTML	
4897	https://digitalgadgetsceneeo.ru	POST	//	✓		200	1824...	JSON	
4896	https://cdnjs.cloudflare.com	GET	/ajax/libs/crypto-js/4.0.0/crypto-js.min.js			200	48945	script	js
4895	https://filmlizenze.com.de	POST	/sXbC/	✓		200	7097	HTML	

- Podczas próby logowania fałszywymi danymi, JavaScript wysyła login i hasło do tego samego serwera, z którego pobrany był wygląd panelu.

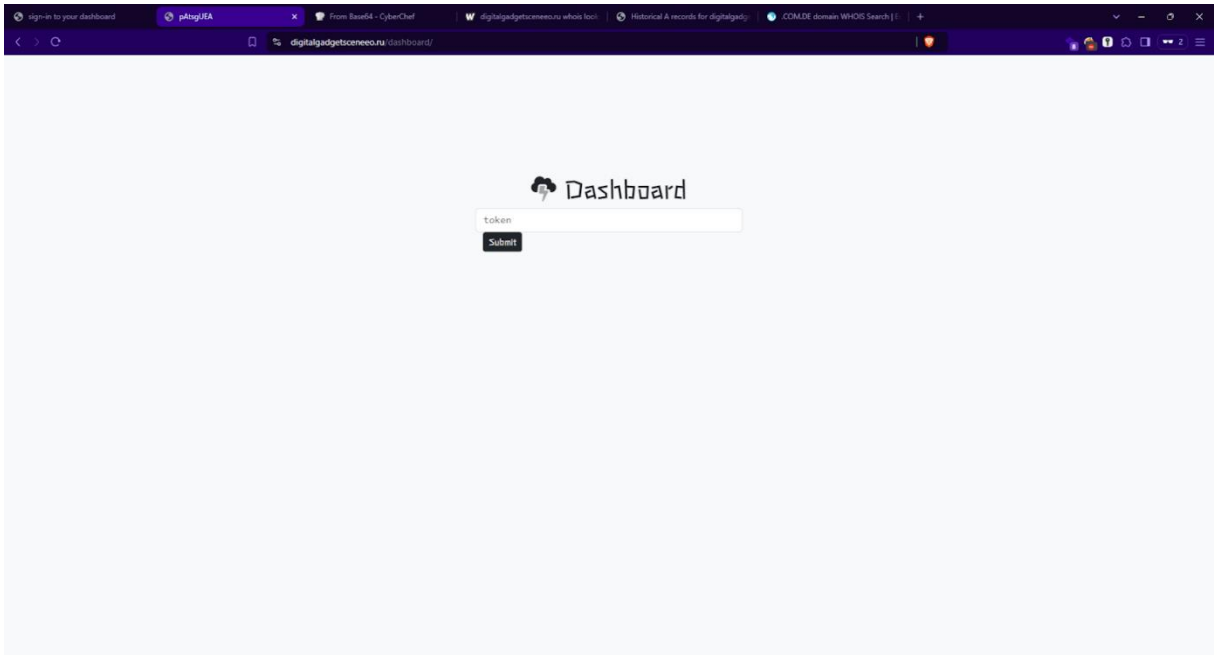


- Dzięki analizie aplikacji zebrano kilka hostów, które, niestety, były ukryte za Cloudflarem, co uniemożliwia ich geolokalizację. Dodatkowo widzimy, że domena została zarejestrowana niedługo przed rozpoczęciem kampanii phishingowej.

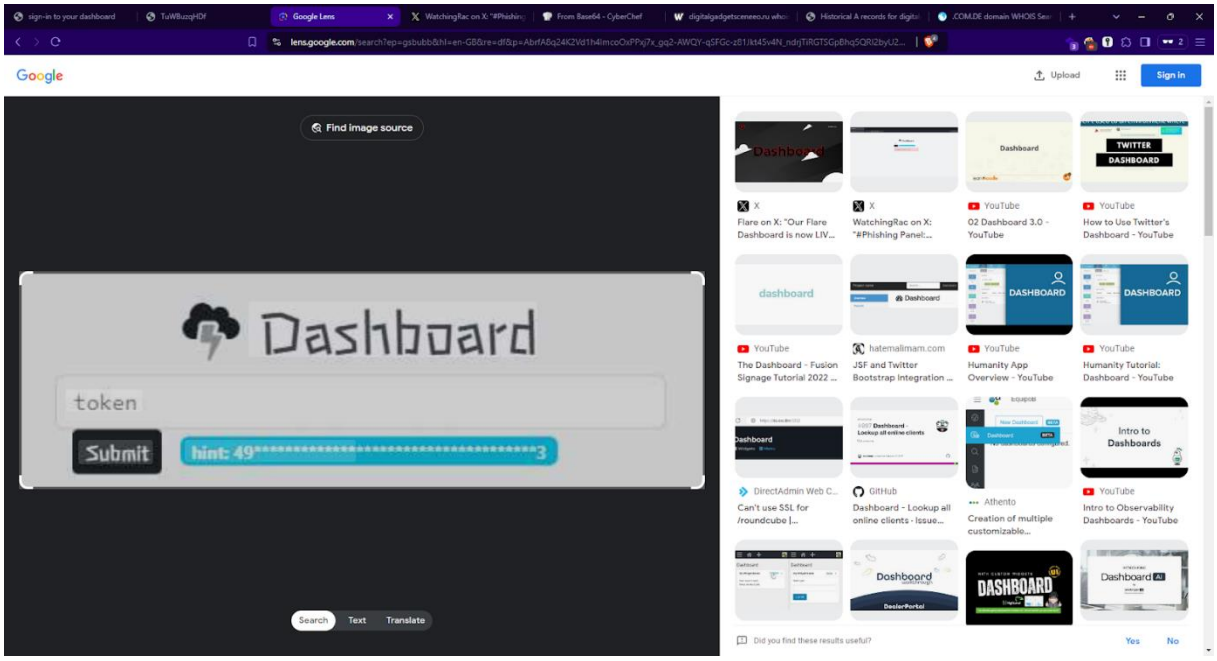


- Weryfikacja strony internetowej utrzymywanej na rosyjskiej domenie wynika, że jest ona tzw. zaślepką, mającą na celu prawdopodobnie uniknięcie potencjalnej detekcji jako strony niebezpiecznej, jako że nic na niej nie działa. Po głębszej analizie okazało się, że

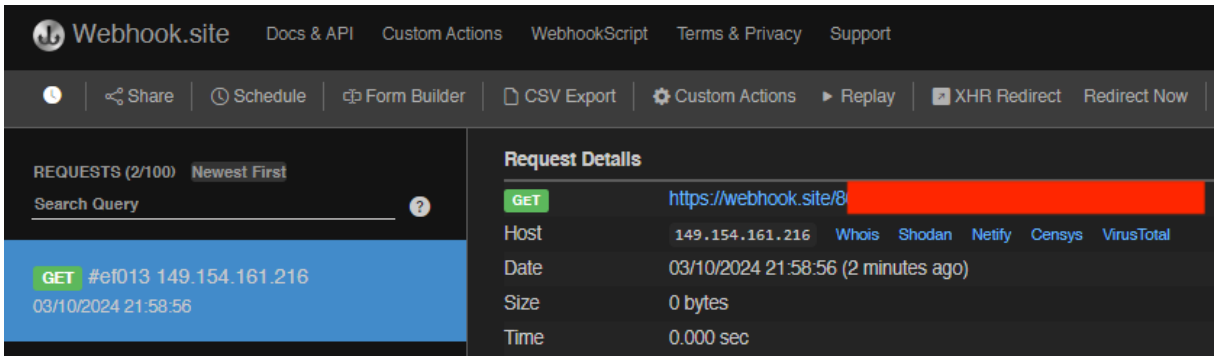
na serwerze znajduje się katalog /dashboard. Niestety nie udało się odnaleźć żadnych pomocnych informacji w źródłach panelu logowania czy przy pomocy dorków.



- Wyszukiwanie za pomocą obrazu po logo panelu pokazało ciekawe rezultaty. Udało się odnaleźć wpis innego badacza z września tego roku, który spotkał się z podobnym atakiem, ale na innej domenie. Niestety, tutaj również nie było zbyt wiele danych o samych atakujących, czy ich celach i motywacji.



- W dalszych krokach logowania na podszytej stronie internetowej uznano, że warto wykonać próbę ataku HTML injection, na wypadek gdyby przestępca przeglądał dane logowania w postaci HTML. Ku zaskoczeniu w parę sekund po wprowadzeniu payloadu otrzymaliśmy informację zwrotną na przygotowany wcześniej webhook.



- Zweryfikowano informacje o adresie IP, z którego nastąpiła interakcja z naszym webhookiem.

- Okazało się, że adres IP należy do puli adresów aplikacji Telegram. Można podejrzewać, że przestępcy używają aplikacji, która powiadamia ich o pomyślnym przeprowadzeniu ataku – otrzymaniu danych.

III. Podsumowanie

Analizując cały scenariusz oraz przepływ informacji, możemy ustalić następujący przebieg wydarzeń:

- atakujący przejęli atakiem dane logowania kontrahenta atakowanej firmy członka Sekurak Academy;
- wykorzystując przechwycone dane, utworzyli zasób w Sharepoincie zaatakowanej wcześniej firmy;
- zasób został udostępniony między innymi naszemu członkowi Sekurak Academy;
- otworzenie zasobu pokazywało zawartość PDF zawierającego link do rzeczywistej strony phishingowej na domenie z tld "com.de" – utrzymywanej za Cloudflare;
- wprowadzenie danych na złośliwej stronie przekazywało je do kolejnej aplikacji na domenie z tld ".ru";
- przekazywane dane były finalnie pobierane przez bota na Telegramie i prawdopodobnie dostarczane już bezpośrednio do atakującego.

Dodatkowo przeskanowano plik PDF narzędziem ANY.RUN (przy czym jest to platforma związana z Federacją Rosyjską, dlatego trzeba brać poprawkę na wyniki zwłaszcza wschodnich kampanii), które wskazało na brak zagrożeń, co sugeruje, że samo otworzenie pliku nie było niebezpieczne. Dopiero celowe kliknięcie w przycisk Open uruchamiało złośliwą procedurę. Natomiast VirusTotal oznaczał już stronę z linka jako złośliwą.

Wszelkie wnioski wskazują na fakt, iż za atak odpowiedzialna jest prawdopodobnie grupa APT zza wschodniej granicy.

Pamiętajmy zatem, żeby weryfikować wszelkie wiadomości przychodzące na naszą skrzynkę pocztową. Jeżeli nie jesteśmy pewni, czy treść jest bezpieczna, nie bójmy się zapytać kogoś doświadczonego (np. pracowników działu IT). Wszelkie przypadki wykrycia phishingu czy scamu warto również zgłaszać do CERT-u (https://incydent.cert.pl/domena#!/lang=pl).

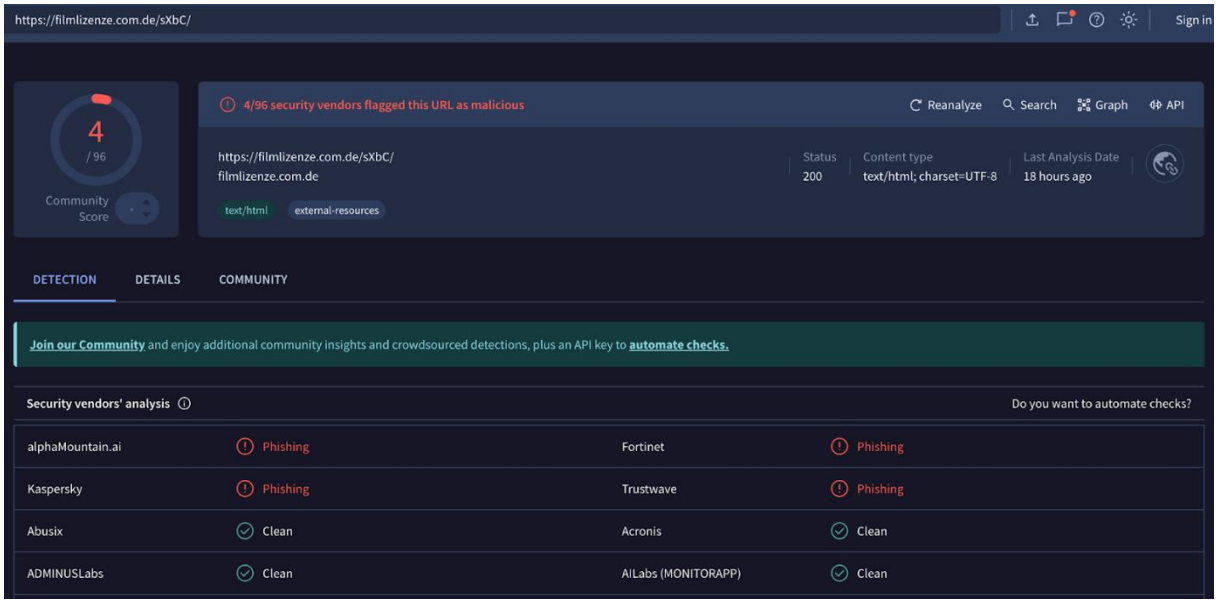
ANY RUN
INTERACTIVE MALWARE ANALYSIS

General Behavior MalConf Static information Video Sc

General Info

File name:	Pro-Forma - Document NÂ°0134188.pdf
Full analysis:	https://app.any.run/tasks/daed7ae7-f59b-4dfb-af20-653538f92f10
Verdict:	No threats detected
Analysis date:	October 03, 2024 at 21:34:34
OS:	Windows 10 Professional (build: 19045, 64 bit)
Indicators:	
MIME:	application/pdf
File info:	PDF document, version 1.6
MD5:	0F30B0BE65BC211264B030E0149723C2
SHA1:	99839660EBF6D9921DE25CC9A6178130C615BF7F
SHA256:	C3DFA0940D2CB23F2FA3FAE74E7C465CBFE537BA3FF881F17E644C2BC7683103
SSDEEP:	1536:JLn73DMjTQvxFCoAScBo60fXQcQR8PK1e1r4DomLrtfSqDMhi9iJ3/M6z:Zn73gUaSHPQcG8SE1HmD9iJxz

ANY.RUN is an interactive service which provides full access to the guest system. Information in this report could be distorted by us
ANY.RUN does not guarantee maliciousness or safety of the content.


https://filmlizenze.com.de/sXbC/
Sign in
4
/ 96
Community Score
4/96 security vendors flagged this URL as malicious
Reanalyze
Search
Graph
API
https://filmlizenze.com.de/sXbC/
filmlizenze.com.de
text/html
external-resources
Status
200
Content type
text/html; charset=UTF-8
Last Analysis Date
18 hours ago
DETECTION
DETAILS
COMMUNITY
Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.
Security vendors' analysis
Do you want to automate checks?
alphaMountain.ai
Phishing
Fortinet
Phishing
Kaspersky
Phishing
Trustwave
Phishing
Abusix
Clean
Acronis
Clean
ADMINUSLabs
Clean
AILabs (MONITORAPP)
Clean