vade

Romain Basset
Directeur des services clients

“Cyber-fièvre” à l’hôpital

APSSIS

3èmes rencontres SSI Santé


1.4 Milliard
de Boites Mail
Protégées
vade

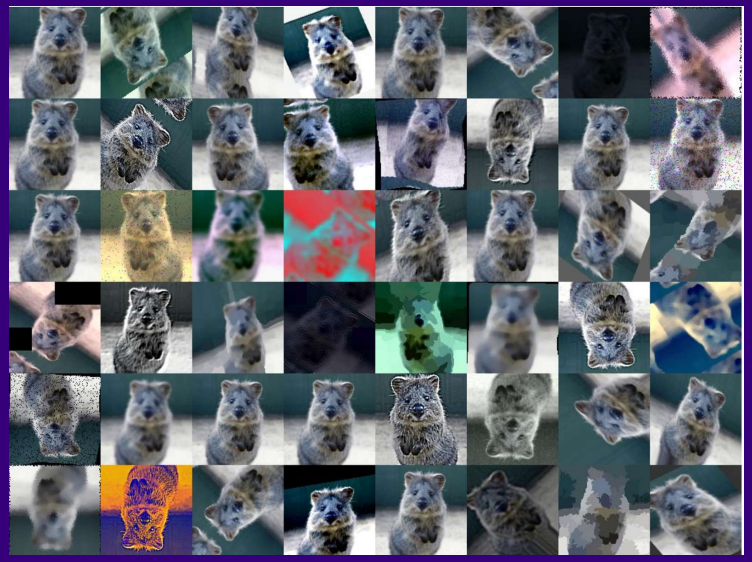
3èmes rencontres SSI Santé APSSIS

Technologies Vade

Image Data Augmentation

3èmes rencontres SSI Santé APSSIS

Technologies Vade



- Shift
- Translate
- Zoom
- Rotate
- Shear
- Flip
- Shade
- Distort
- Add noise
- Change style
- Segment
- Interpolate

3èmes rencontres SSI Santé APSSIS

Technologies Vade

Email textual content dissection

Technologies Vade

Category	Content
greeting	Hi John,
paragraph	I'm stuck in meetings all day, would you be available to help me? I cannot pick the phone, email will do just fine.
closing	Looking forward to hearing from you soon
signature	[First Name] [Last Name] [Title]
unauthorized	This email is confidential and should not be reshared without prior authorization from its owner

Aux avants-postes de la “cyber-intelligence”

Traquer les acteurs malveillants pour protéger nos clients

3èmes rencontres SSI Santé APSSIS

Cyber-intelligence

New Phishing Attack Leverages Google Translate and IPFS Decentralized Network

Nicolas Joffre — April 20, 2023 — 5 min read

3èmes rencontres SSI Santé APSSIS

Cyber-intelligence

Recherche

Détournement de Microsoft et Cloudflare au cours d'une nouvelle attaque de QRishing

Par Vade, le 21 septembre 2023

Vade a récemment détecté une attaque de phishing dirigée contre un MSP basé aux États-Unis. L'email malveillant, reçu...

Lire la suite

Cybermenaces dans la Santé

Contexte & chiffres

Tous secteurs d'activités

Vade observe

86

attaques
avancées

par organisation, par mois

Dans le secteur de la Santé

Vade observe

attaques
avancées

par organisation, par mois

Dans le secteur de la Santé

Vade observe

141

attaques
avancées

par organisation, par mois

Contexte et chiffres

- **Microsoft** est la marque la plus usurpée dans les tentatives de **phishing**
- Beaucoup de **malware** propagés par le biais de **fausses factures** avec des **fichiers HTML** en pièces jointes
- La majorité des tentatives de **spear-phishing** sont de type “**initial contact**”

Cybermenaces dans la Santé

Cas remarquables récents

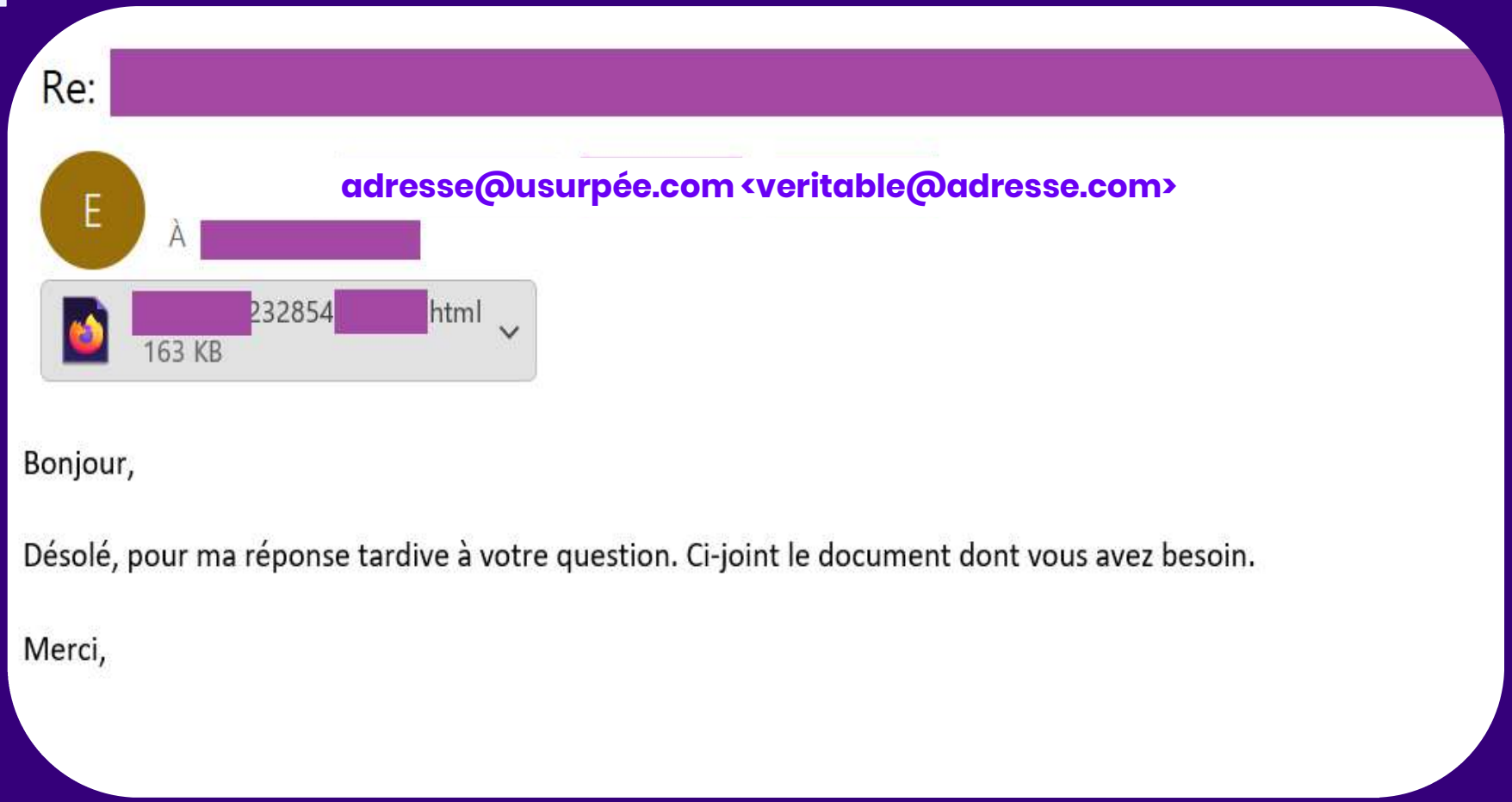
3èmes rencontres SSI Santé APSSIS

“La triple attaque”

- Attaque observée en Mars 2023
- Reçue par un établissement français du secteur de la santé
- Ne ciblait qu’un seul utilisateur
- Combinait trois techniques d’attaques par email

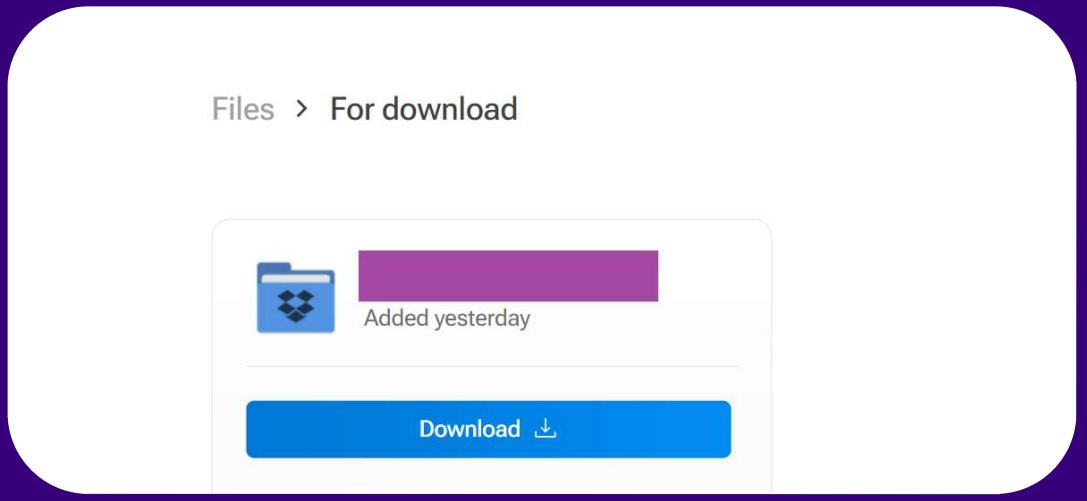
3èmes rencontres SSI Santé APSSIS

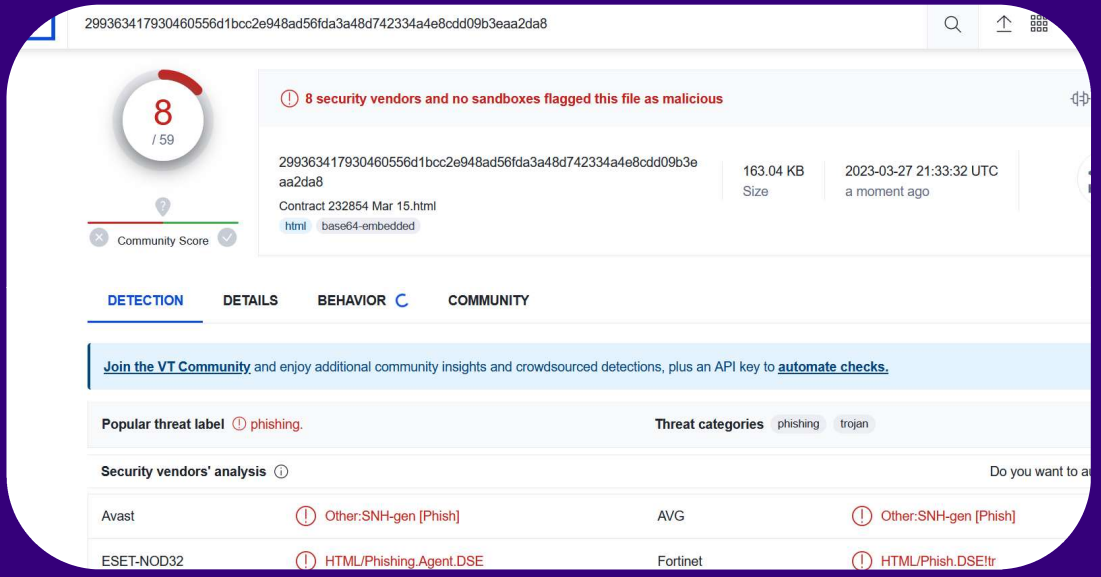
“La triple attaque”



3èmes rencontres SSI Santé APSSIS

“La triple attaque”

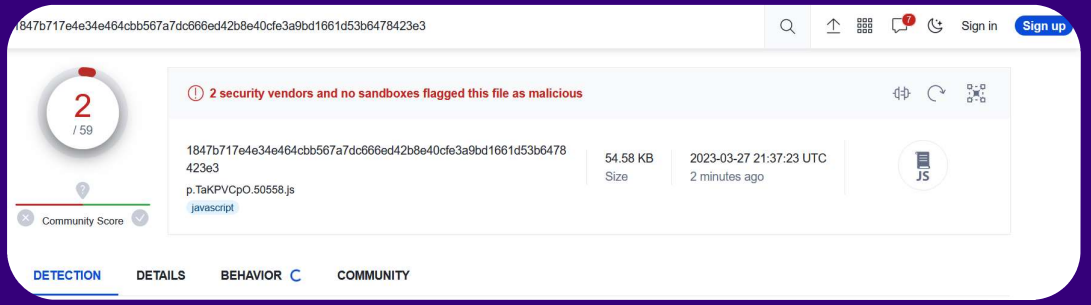




3èmes rencontres SSI Santé APSSIS

“La triple attaque”

```
    try {
        var unhumorousnessservilities = parseInt(likewiseness('0x318', '0x2e9', '0x330', '0x2ef', 0x345)) ,
        if (unhumorousnessservilities === cuproammonium) {
            break;
        } else {
            enchytraeid['push'](enchytraeid['shift']());
        }
    } catch (shortheadunniceness) {
        enchytraeid['push'](enchytraeid['shift']());
    }
}
(OneDrive0scrofulousnessduteously, -0x6057e + -0x83 * -0x1528 + 0x3312a));
unction OneDrive0hyponoias(scrofulousnessduteously, pearlspar) {
  var hyponoias = OneDrive0scrofulousnessduteously();
  OneDrive0hyponoias = function (enchainanubis, ectoentadiodopsins) {
      enchainanubis = enchainanubis - (0x17 * -0x11 + -0xc25 + 0xedf);
      var demotic = hyponoias[enchainanubis];
      if (OneDrive0hyponoias['abAIWT'] === undefined) {
          var unchemicallyunintersecting = function (outspeltembost) {
              var cognacs = 'abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789+/=';
              var allogamousderogative = '';
              var accessablebrachiate = '';
              for (var misorganizephonotypy = -0x22bd + 0x63 * 0xe + 0x1d53, hortensialsmudder, functionatings
                  functionatingsensualize = cognacs['indexOf'](functionatingsensualize);
              }
              for (var nonpariellorequicken = 0x4ef + -0x3 * 0x232 + 0x1a7, twanglersovercomable = allogamous
                  accessablebrachiate += '%' + ('00' + allogamousderogative['charCodeAt'](nonpariellorequick
              }
              return decodeURIComponent(accessablebrachiate);
```



3èmes rencontres SSI Santé APSSIS

L'attaque "tour du monde"

- Campagne de phishing en cours
- Prétexte un rappel d'activation du MFA
- Vise différentes entités des secteurs de la santé et caritatifs
- Propose une page de login M365 personnalisée

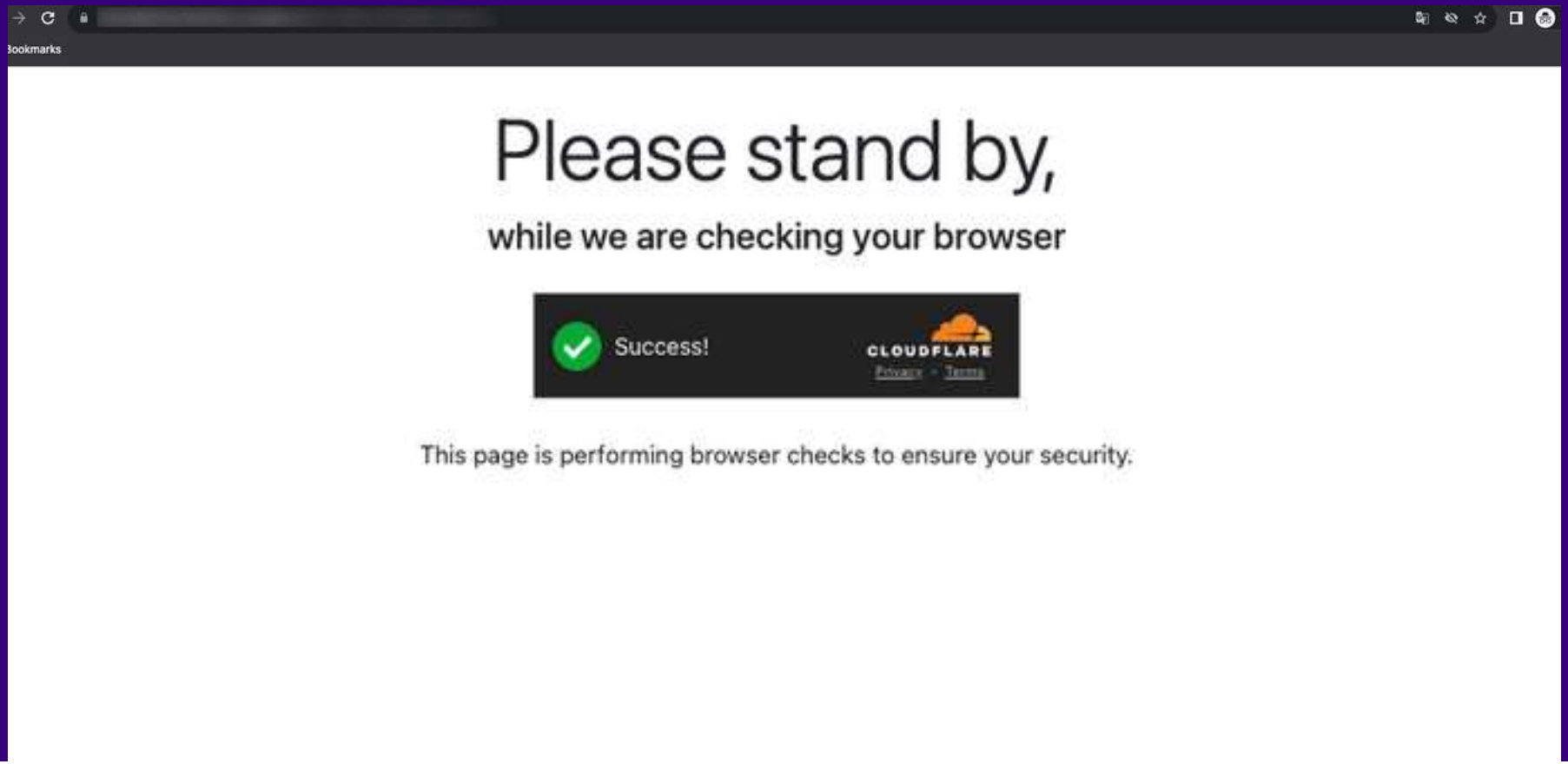
3èmes rencontres SSI Santé APSSIS

L'attaque "tour du monde"

https://api.site-légitime.com/api/click?id=XXX&url=https://autre-site-légitime-compromis.com.ar/bootstrap/imw8pr/hash-infos-cible

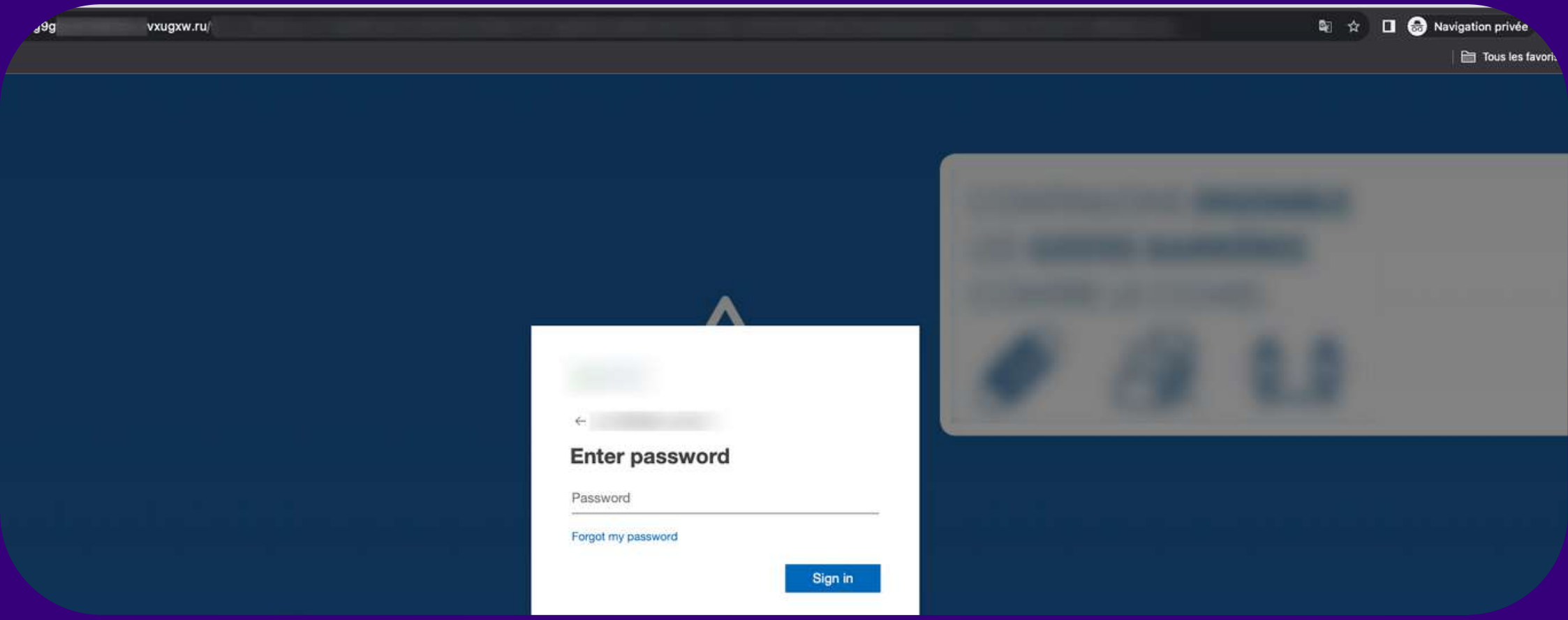
3èmes rencontres SSI Santé APSSIS

L'attaque "tour du monde"



3èmes rencontres SSI Santé APSSIS

L'attaque "tour du monde"



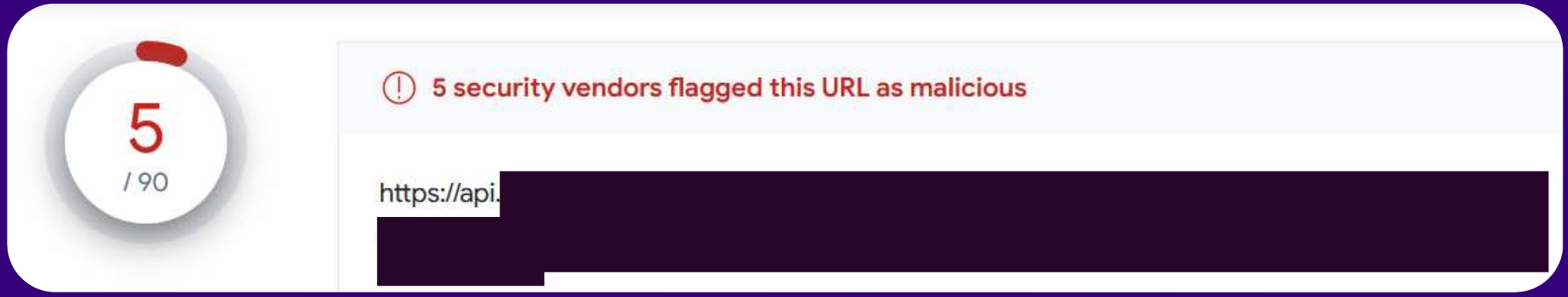
3èmes rencontres SSI Santé APSSIS

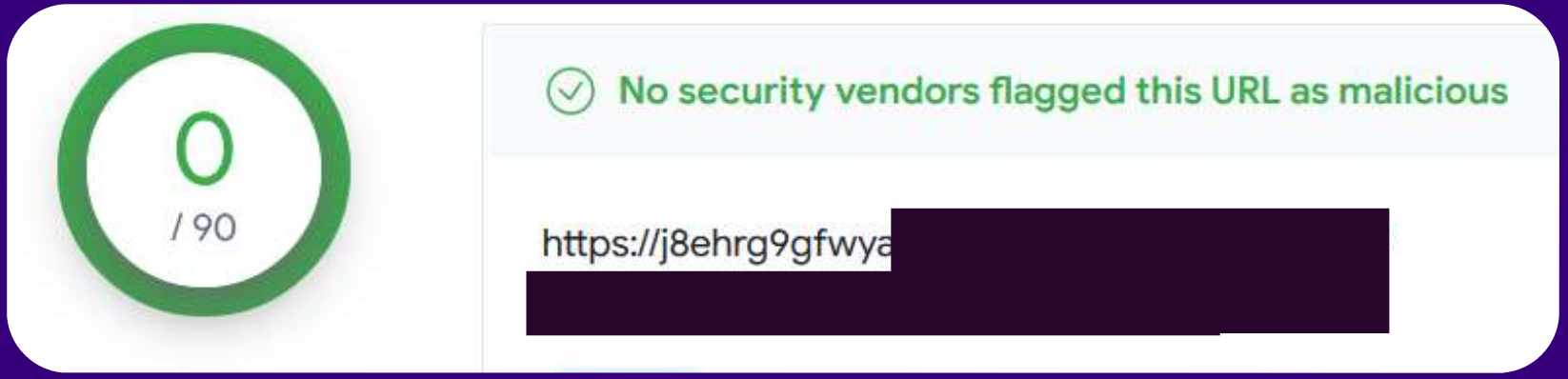
L'attaque "tour du monde"

État	Méth...	Domaine	Fichier	Initiateur	Type
200	GET	aadcdn.msauthima...	bannerlogo?ts=[redacted]	img	
200	GET	j8ehrg9gfwya24...	0csnaEagux0usbyMTDR8e227KHLYx7rt1jPTlIUDF	document	html
200	GET	j8ehrg9gfwya24...	st-88XFEkNINLsHIQrEF42uCsoGMAT8INIwJq3p8	javascript;base6...	css
200	GET	j8ehrg9gfwya24...	jq-WqcDJ7gOI8eyqaNNPXFAcZQvf9GNQAjXMKr	javascript;base6...	js

3èmes rencontres SSI Santé APSSIS

L'attaque "tour du monde"





Les solutions Vade

Les solutions

- Utiliser des technologies de détection basées sur l'IA
- Sensibiliser les utilisateurs aux cybermenaces contextualisées
- S'appuyer sur le signalement des utilisateurs
- Mettre en oeuvre des fonctionnalités de remédiation

3èmes rencontres SSI Santé APSSIS

Les solutions

vade FOR M365

Sécurité de l'email intégrée à Microsoft 365

vade CLOUD

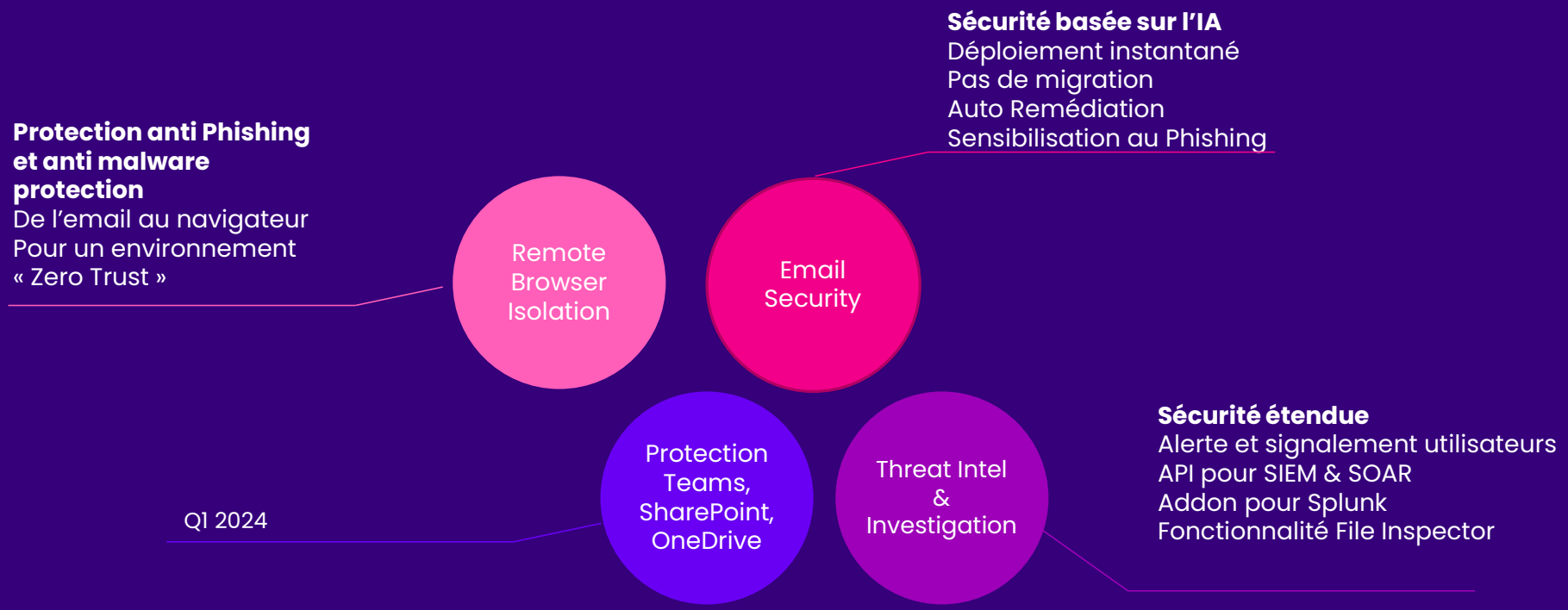
Sécurité de l'email proactive dans le cloud

vade FOR Google Workspace

Bientôt !

3èmes rencontres SSI Santé APSSIS

La solution de sécurité la plus complète pour M365



Merci !
Avez-vous des questions ?

romain.basset@vadesecure.com