



Romain Basset
Directeur des services clients



“Cyber-fièvre” à l’hôpital



3^{èmes} rencontres SSI Santé

1.4 Milliard

**de Boites Mail
Protégées**



3^{èmes} rencontres SSI Santé APSSIS

Technologies Vade

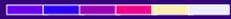
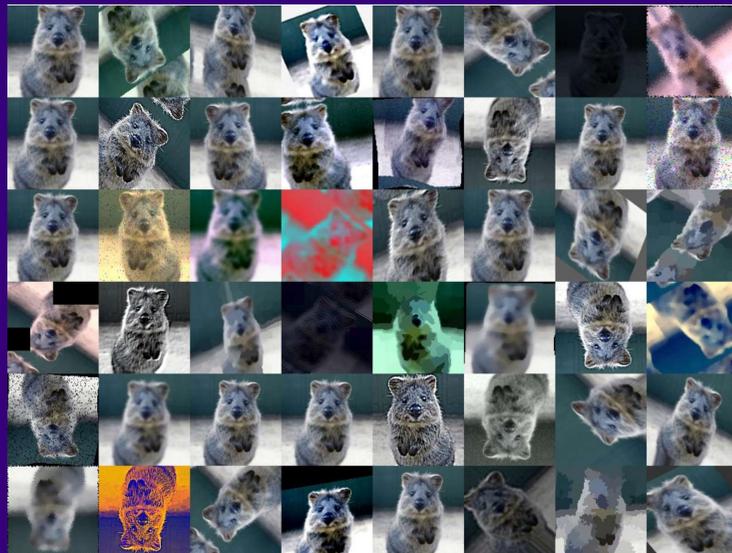


Image Data Augmentation

3^{èmes} rencontres SSI Santé APSSIS

Technologies Vade



Shift

Translate

Zoom

Rotate

Shear

Flip

Shade

Distort

Add noise

Change style

Segment

Interpolate

3^{èmes} 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

3^{èmes} rencontres SSI Santé APSSIS

Cyber-intelligence



New Phishing Attack Leverages Google Translate and IPFS Decentralized Network

Nicolas Joffre — April 20, 2023 — 5 min read



3^{èmes} 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

3^{èmes} 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

3^{èmes} rencontres SSI Santé APSSIS

“La triple attaque”



Re:



adresse@usurpée.com <veritable@adresse.com>

À



Bonjour,

Désolé, pour ma réponse tardive à votre question. Ci-joint le document dont vous avez besoin.

Merci,

3^{èmes} rencontres SSI Santé APSSIS

“La triple attaque”



Files > For download



Added yesterday

Download

299363417930460556d1bcc2e948ad56fda3a48d742334a4e8cdd09b3eaa2da8



8 security vendors and no sandboxes flagged this file as malicious

299363417930460556d1bcc2e948ad56fda3a48d742334a4e8cdd09b3eaa2da8

163.04 KB
Size

2023-03-27 21:33:32 UTC
a moment ago

Contract 232854 Mar 15.html

html base64-embedded

Community Score

DETECTION DETAILS BEHAVIOR C COMMUNITY

[Join the VT Community](#), and enjoy additional community insights and crowdsourced detections, plus an API key to [automate checks](#).

Popular threat label **phishing**.

Threat categories phishing trojan

Security vendors' analysis

Do you want to a

Avast	Other:SNH-gen [Phish]	AVG	Other:SNH-gen [Phish]
ESET-NOD32	HTML/Phishing.Agent.DSE	Fortinet	HTML/Phish.DSE!tr

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 (shortheadunnicens) {
  enchytraeid['push'](enchytraeid['shift']());
}
}

(function (OneDrive0scrofulousnessduteously, -0x6057e + -0x83 * -0x1528 + 0x3312a));
function 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 = 'abcdefghijklmnopqrstuvwxyABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789+/-';
        var allogamousderogative = '';
        var accessiblebrachiate = '';
        for (var misorganizephonotypy = -0x22bd + 0x63 * 0xe + 0x1d53, hortensialsudder, functionatings
          functionatingsensualize = cognacs['indexOf'](functionatingsensualize);
        }
        for (var nonpariellorequicken = 0x4ef + -0x3 * 0x232 + 0x1a7, twanglersovercomable = allogamous
          accessiblebrachiate += '%' + ('00' + allogamousderogative['charCodeAt'](nonpariellorequick
        }
      }
    }
    return decodeURIComponent(accessiblebrachiate);
  }
}
```

The screenshot shows a VirusShare analysis page for a JavaScript file. The file name is `p.TaKPVCpO.50558.js` and it is identified as `javascript`. The file size is 54.58 KB and it was uploaded 2 minutes ago on 2023-03-27 21:37:23 UTC. A red warning icon indicates that 2 security vendors and no sandboxes flagged the file as malicious. The page includes a 'Community Score' section and tabs for 'DETECTION', 'DETAILS', 'BEHAVIOR', and 'COMMUNITY'.

3^{èmes} rencontres SSI Santé APSSIS

L'attaque "tour du monde"



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

3^{èmes} rencontres SSI Santé APSSIS

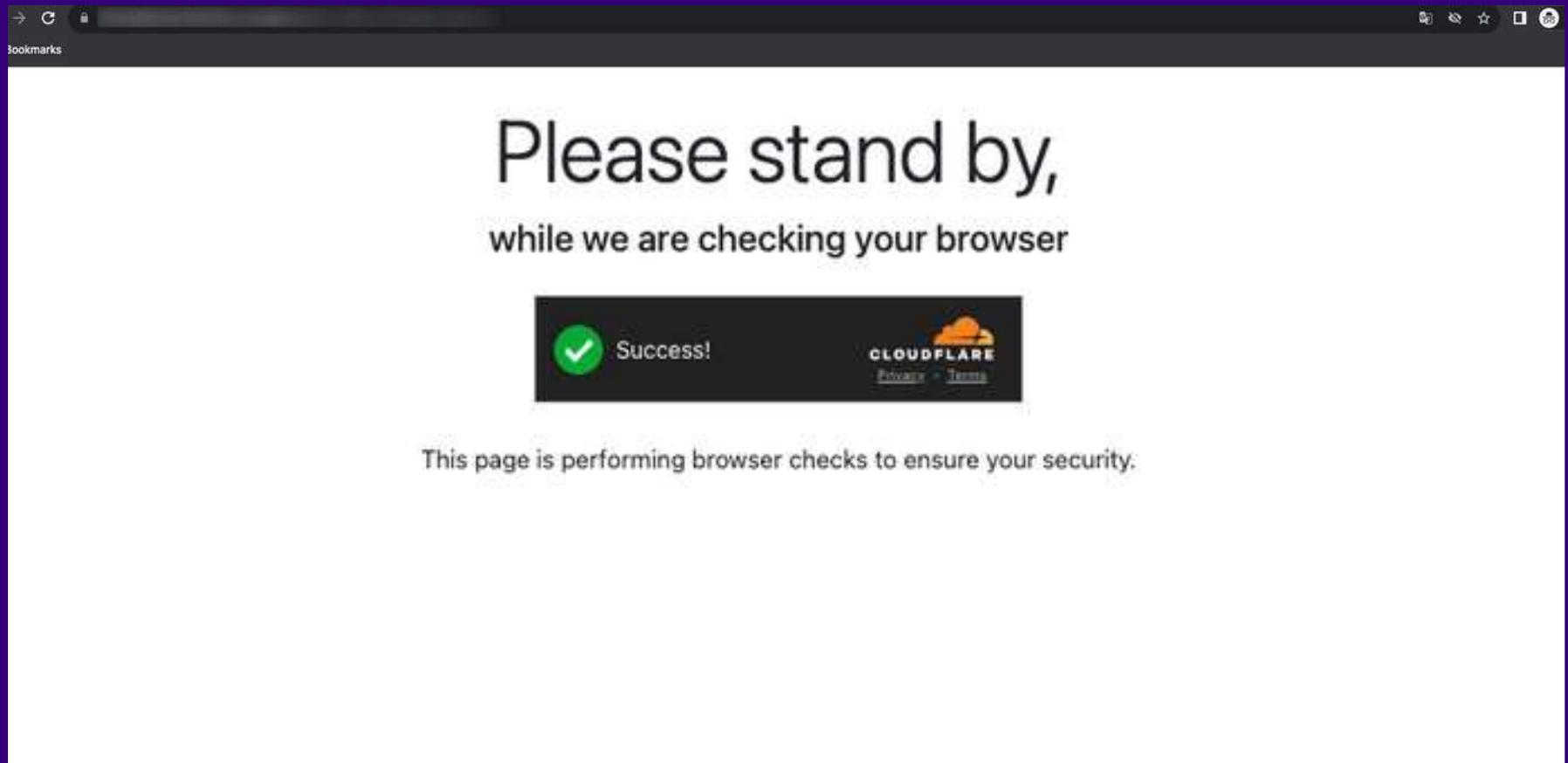
L'attaque "tour du monde"



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

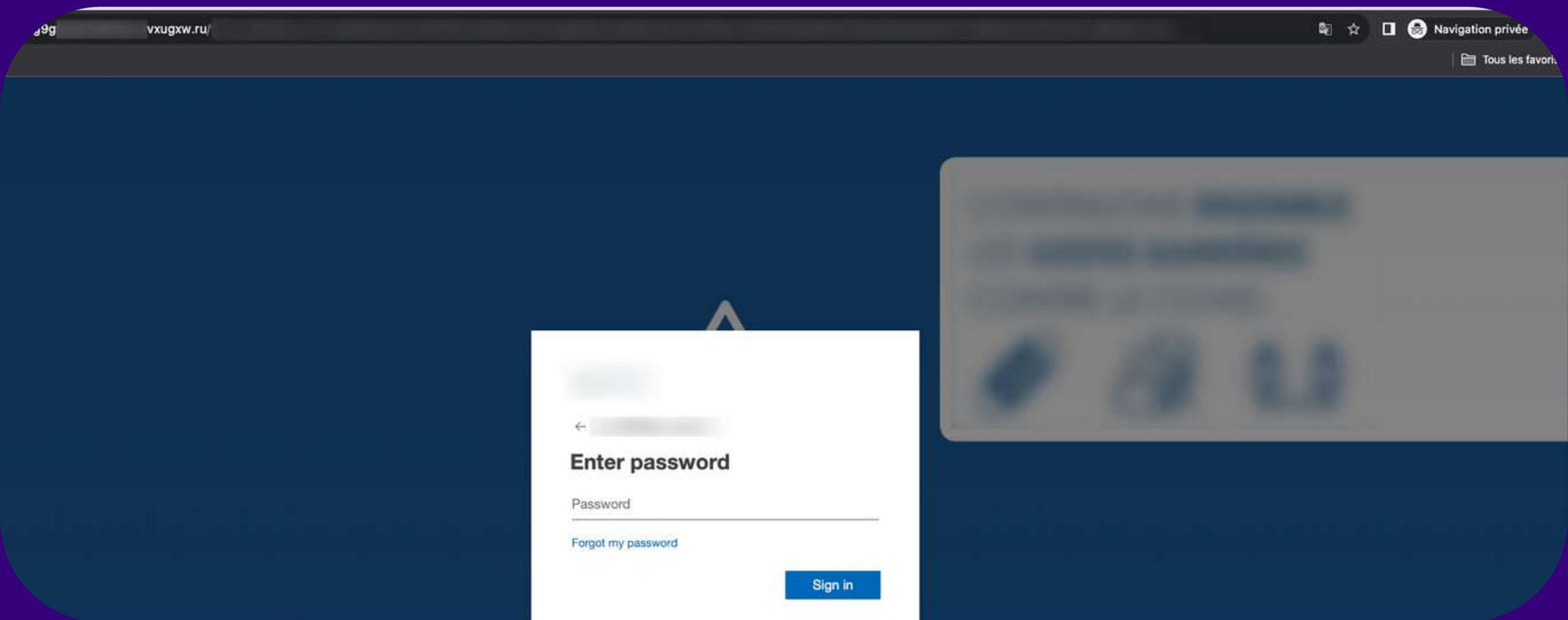
3^{èmes} rencontres SSI Santé APSSIS

L'attaque "tour du monde"



3^{èmes} rencontres SSI Santé APSSIS

L'attaque "tour du monde"



L'attaque "tour du monde"



État	Méth...	Domaine	Fichier	Initiateur	Type
200	GET	aadcdn.msauthima...	bannerlogo?ts=[REDACTED]	img	
200	GET	j8ehrg9gfwya24...	0csnaEagux0usbyMTDR8e227KHLYx7rt1jPTIIUDF	document	html
200	GET	j8ehrg9gfwya24...	st-88XFEkNINLsHIQrEF42uCsoGMAT8INlwJq3p8!	javascript;base6...	css
200	GET	j8ehrg9gfwya24...	jq-WqcDJ7gOI8eyqaNNPXFACZQvf9GNQAJXMKr	javascript;base6...	js

L'attaque "tour du monde"



5
/ 90

⚠ 5 security vendors flagged this URL as malicious

https://api. [REDACTED]

[REDACTED]

0
/ 90

✓ No security vendors flagged this URL as malicious

https://j8ehrg9gfwya [REDACTED]

[REDACTED]

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

3^{èmes} 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

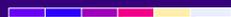


vade
FOR Google Workspace

Bientôt !

3^{èmes} rencontres SSI Santé APSSIS

La solution de sécurité la plus complète pour M365



Protection anti Phishing et anti malware protection

De l'email au navigateur
Pour un environnement
« Zero Trust »

Remote
Browser
Isolation

Email
Security

Sécurité basée sur l'IA

Déploiement instantané
Pas de migration
Auto Remédiation
Sensibilisation au Phishing

Protection
Teams,
SharePoint,
OneDrive

Threat Intel
&
Investigation

Sécurité étendue

Alerte et signalement utilisateurs
API pour SIEM & SOAR
Addon pour Splunk
Fonctionnalité File Inspector

Q1 2024

Merci !
Avez-vous des questions ?



romain.basset@vadecure.com