

# Covid-19 : le phishing se déplace sur le terrain de la visio

Que faire en ce moment face aux noms de domaines qui contiennent des mots-clés de type « coronavirus » ou « covid » ?

Les nombreuses [alertes](#) aux sites malveillants [émises](#) ces dernières semaines imposent de redoubler de vigilance.

On n'oubliera cependant pas de surveiller d'autres mots-clés. En particulier **ceux associés aux logiciels de visioconférence**. Et pour cause : les domaines qui en comportent peuvent abriter des pages de *phishing*.

L'entreprise américaine Abnormal Security, spécialisée dans la protection des messageries électroniques, a recensé plusieurs de ces pages. Point commun : les victimes y parviennent en cliquant sur une fausse notification.

Les notifications en question, envoyées par mail, semblent provenir d'un logiciel de visioconférence. Elles instaurent généralement un **sentiment d'urgence chez l'utilisateur**.

Il y a notamment ce [rappel de réunion Zoom](#) avec les RH en vue d'une suspension, voire d'une fin de contrat. L'employé visé arrive sur la page, qui lui demande de saisir ses login et mot de passe.

Subject: [REDACTED] Offer Letter Review Meeting

Sender: Meeting Reminder <zoom-service@jason-sg.com>

Recipient: [REDACTED]

To: [REDACTED]

Apr 20th 01:44 AM PDT

[View Original Email Headers](#)

Reminder! Zoom meeting between you and the remaining members of...

ZOOM

Hello [REDACTED],

**Meeting Reminder with [REDACTED] Team on Zoom!**

This is a reminder that your scheduled zoom meeting with **Human Resources and Payroll Administrative Head** will start in few minutes.

Your presence is crucial to this meeting and equally required to commence this **Q1 performance review** meeting

[Join this Live Meeting](#)

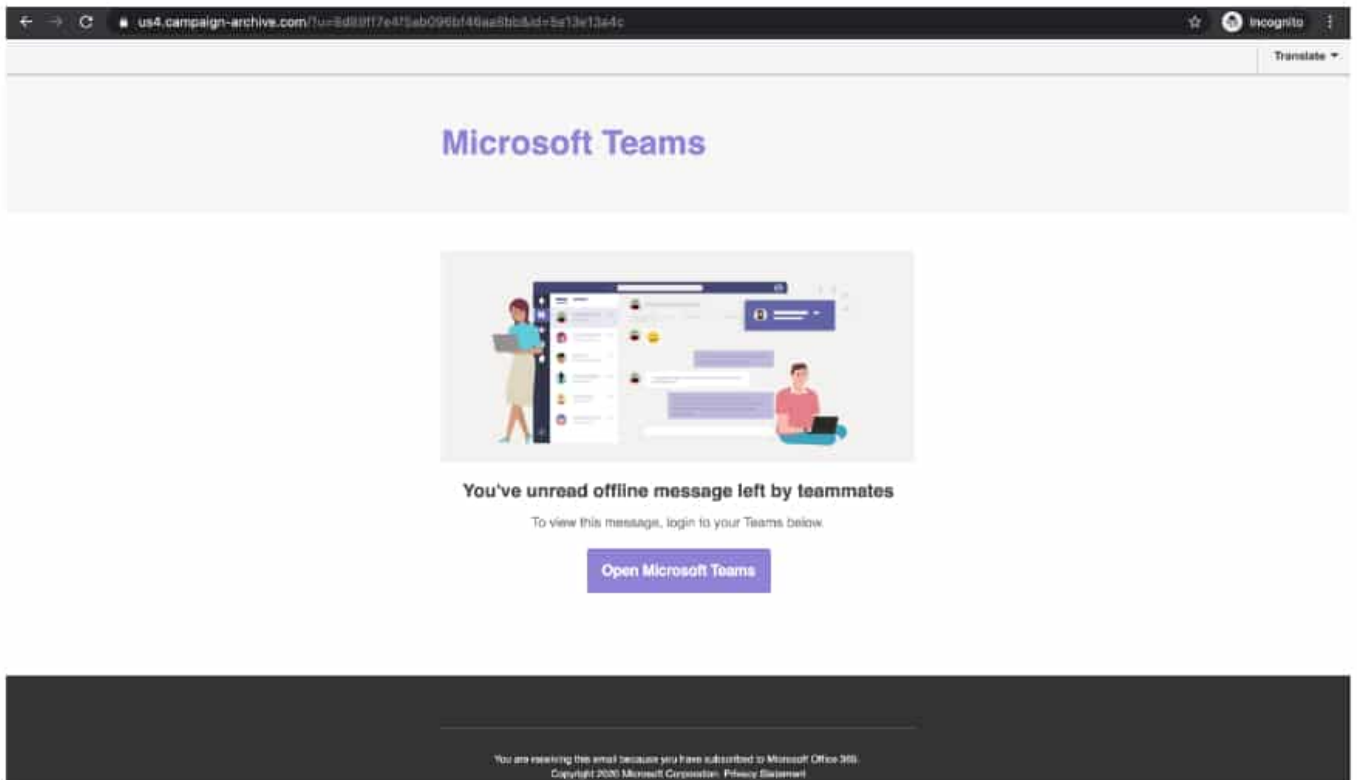
**Meeting Purpose:** : Contract Suspension / Termination Trial

## Vous avez des messages

Teams n'est pas épargné.

Cette fois, pas de rendez-vous RH, mais des [messages audio en attente](#).

Le lien malveillant peut acheminer vers plusieurs destinations. Mais dans tous les cas, on n'atteint cette dernière qu'après une série de redirections.



Pour les utilisateurs de Webex, l'urgence est liée à un prétendu blocage de compte. Aussi leur est-il [demandé de se reconnecter](#).

Subject: Important: Webex Meetings SSL certificate error. Verify your account.

Sender: Cisco Webex <bruno@cotrisel.com.br>

Recipient: [redacted]

To: [redacted]

Apr 29th 02:52 PM PDT

[View Original Email Headers](#)

**Important note: If you already have a certificate installed, the system warns you that importing a new certificate will overwrite it.**

- Private Key
- Certificate matched to the Private Key
- Intermediate/Chain Cert.

You cannot start or join meetings because we cannot validate the security certificate of your Webex site. This error can occur because we cannot access the digital signature site, your firewall has blocked external access to a revocation server, or is a problem connecting to the network.

Verify your Account. Your account is blocked by your site administrator.

[Log in](#) sign in and unlock your account.

Delivering the power of collaboration

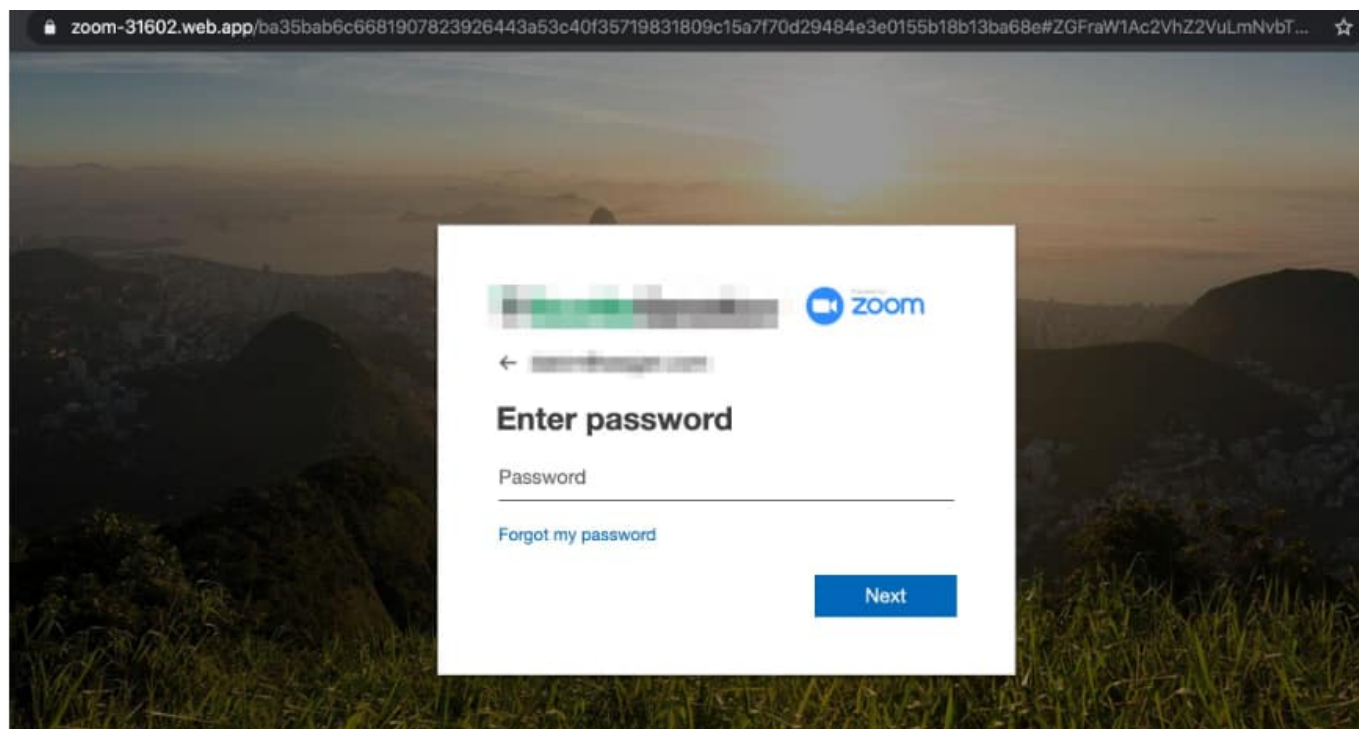
Cisco WebEx Team



Toujours sur Zoom, il y a la technique des réunions loupées. Heureusement, [un lien est disponible](#)

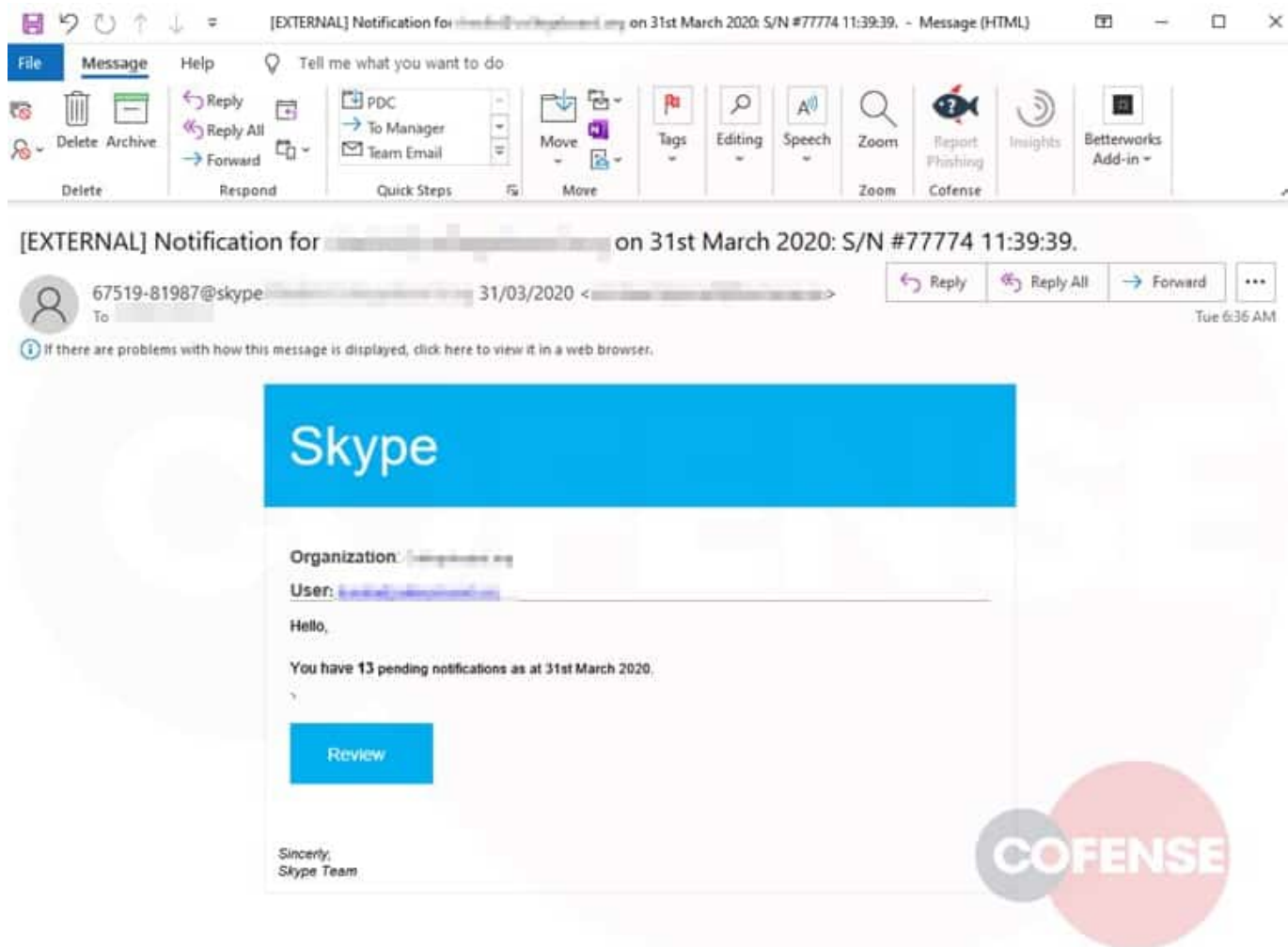
pour accéder à l'enregistrement... toutefois conservé 48 heures seulement.

La page d'atterrissage se veut rassurante. Elle contient le nom de la victime et le logo de son entreprise. Pas de demande de connexion à Zoom néanmoins, mais à un compte Microsoft.



Skype [n'échappe pas à la déferlante](#). Le levier : des notifications en attente.

Pour paraître plus légitime, le mail émane de comptes compromis. La page de *phishing* se cache derrière une autre qui utilise l'extension de nom de domaine .app, [dont Google a la gestion](#). Là encore, elle comporte le logo de l'entreprise de la victime. S'y adjoint un « sceau d'authenticité » et un remplissage automatique du login.



Trend Micro a signalé à plusieurs reprises une autre pratique : la mise à disposition d'installateurs de Zoom modifiés pour inclure un logiciel malveillant. Entre autres, des [outils de contrôle à distance](#) et des [mineurs de cryptomonnaies](#).

La méthode est parfois plus directe. Check Point l'a démontré sur Teams. Une notification – reçue par e-mail – d'ajout à un groupe contient un bouton cliquable. L'effet ? Le téléchargement d'un *malware*.

*Illustration principale © Ivelin Radkov – Shutterstock*