Alerte Arnaque à l'enregistrement de noms de domaine en Chine!!!

Plusieurs mails ou messages d'arnaque sont en train d'être envoyés concernant l'enregistrement des noms de domaines.
Cette **arnaque sur l'enregistrement de noms de domaine en Chine (.cn)** est pratiquée par des escrocs. Bien que cette escroquerie ait été signalée pour la première fois en 2010, les fraudeurs qui en sont à l'origine trouvent toujours un moyen d'essayer de tromper leurs victimes en leur faisant payer un nom de domaine dont ils n'ont pas besoin. Ainsi depuis quelques jours, **CERT.tg** a détecté une augmentation préoccupante des escroqueries liées à l'enregistrement de noms de domaine, ciblant des propriétaires de sites web.

Comment ça marche ?
Des individus malveillants orchestrent actuellement une escroquerie d'enregistrement de noms de domaine, se concentrant principalement sur les domaines en .cn. Ces escroqueries impliquent fréquemment des courriels frauduleux, des appels téléphoniques ou des sites web trompeurs se faisant passer pour des bureaux d'enregistrement légitimes, dans le but de tromper les propriétaires de domaines en leur faisant effectuer des paiements inutiles ou en leur fournissant des informations sensibles.
En résumé, le détenteur d'un nom de domaine est informé qu'une "société" tente d'enregistrer les équivalents de ses noms de domaine et de ses mots clés en chinois et dans d'autres domaines de premier niveau liés à l'Asie. Le titulaire est alors invité à vérifier si la société qui tente d'enregistrer les domaines est ou non son distributeur ou un partenaire commercial en Chine. Les coordonnées des détenteurs de domaines sont copiées à partir du registre Whois ou, dans certains cas, à partir des sites web directement associés aux noms de domaines contestés. Souvent, les titulaires sont poussés à enregistrer leurs noms de domaine auprès de ce **"centre d'enregistrement de domaines chinois"** afin de protéger leur propriété intellectuelle.

Ci-dessous quelques courriels liés à cette anarque d'enregistrement de nom de domaine.

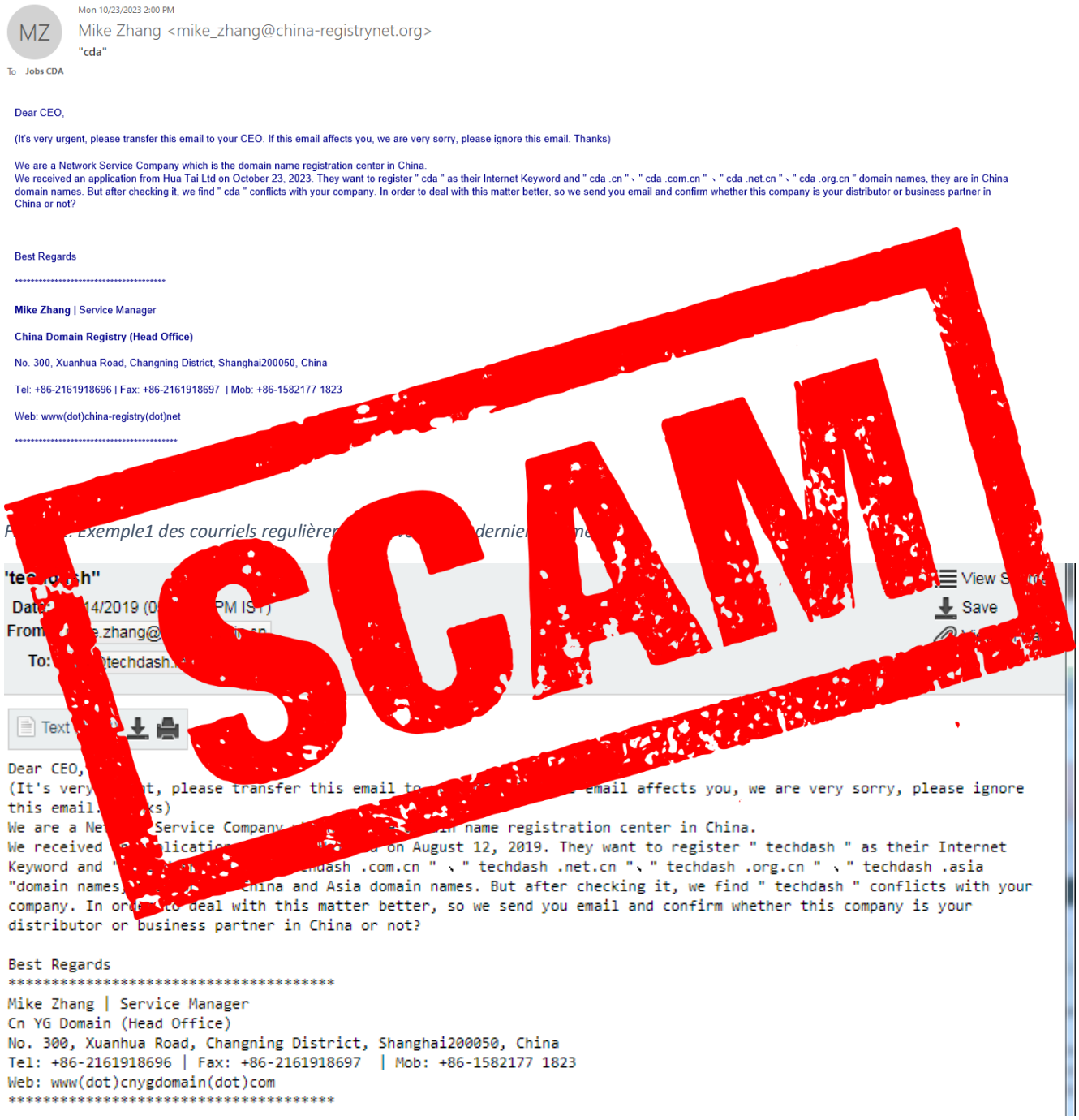

Figure 2: Exemple 2 des courriels regulièrement envoyé courant 2019

Comment identifier cette anarque ?

L'usurpation d'identité d'entités légitimes : Ces escrocs peuvent se faire passer pour des bureaux d'enregistrement de domaines ou des autorités dignes de confiance, en utilisant une marque similaire et un langage officiel.

Urgence et menaces : Ils créent souvent un sentiment d'urgence, exigeant une action immédiate pour éviter les conséquences supposées.

Demandes de paiement non conventionnelles : Ils peuvent demander à être payés par des méthodes non conventionnelles ou insister sur l'utilisation de processeurs de paiement non standard.

Messages mal rédigés : Méfiez-vous des fautes de grammaire, d'orthographe ou des formules de politesse génériques, ils souvent sont des indicateurs courants d'escroquerie.

Quelques mesures préventives à adopter :

Signalez toute activité suspecte tout en suivant les conseils suivants :

- **Conseil 1** : Vérifiez toujours la communication officielle : Vérifiez toujours l'authenticité de toute communication concernant l'enregistrement de votre domaine. Contactez directement votre registraire de domaine en utilisant les coordonnées officielles.
- **Conseil 2** : Ignorer les courriers électroniques provenant de **.cn** et mentionnant un conflit de domaine.
- **Conseil 3** : Évitez les décisions hâtives : Résistez à la pression qui vous pousse à agir rapidement, surtout lorsque vous êtes confronté à des menaces de conséquences immédiates, veuillez le signaler directement sur le site https://cert.tg/ dans la rubrique « déclarer un incident » et remplissez le formulaire.
- **Conseil 4** : Maintenez vos logiciels à jour : assurez-vous que votre hébergement web et votre logiciel de gestion de domaine sont à jour afin de réduire les vulnérabilités.
- **Conseil 5** : Utilisez une authentification forte : Mettez en place une authentification à plusieurs facteurs pour vos comptes de registraire de domaine.