

SDR : Foire aux questions de maturité d'expéditeur

Contenu

[Introduction](#)

Q. [Que la « maturité d'expéditeur » signifie-t-elle ?](#)

Q. [Talos peut-il manuellement changer la maturité d'expéditeur ?](#)

Q. [Pourquoi est-ce qu'un domaine a une maturité différente d'expéditeur après une courte période ?](#)

Introduction

L'expéditeur de Cisco Talos que la réputation de domaine (SDR) est un service en nuage qui fournit un verdict de réputation pour des messages électroniques basés sur le domaine d'un expéditeur et autre attribue. Cette analyse basée sur domaine de réputation active un taux de capture plus élevé de Spam par le regard au delà de la réputation des adresses IP partagées, l'accueil ou les fournisseurs d'infrastructure, et dérive des verdicts basés sur des caractéristiques associées avec les noms de domaine complet (FQDN) et d'autres informations d'expéditeur dans les en-têtes de conversation et d'email de Protocole SMTP (Simple Mail Transfer Protocol).

Q. Que la « maturité d'expéditeur » signifie-t-elle ?

A. L'âge de domaine est un terme fallacieux et a été récemment changé à la maturité d'expéditeur (voyez plus défunt [Livre blanc de SDR](#)). Nous disons qu'il est fallacieux parce qu'il n'égal pas en fait à l'âge d'un domaine comme reflété d'ici la date de l'enregistrement de domaine. La maturité d'expéditeur continue à être étiquetée comme âge de domaine dans l'ESA dépistant le log pour l'instant, bien que ceci pourrait changer dans une version future. Talos emploie de plusieurs sources internes de données pour dériver la maturité d'expéditeur.

Remarque: Talos ne peut pas révéler des détails au sujet des sources utilisées pour dériver la maturité de domaine, en dehors de des informations qui ont été déjà éditées dans plus défunt Livre blanc de SDR, en tant que ceci constitue l'information propriétaire de Cisco Talos.

Q. Talos peut-il manuellement changer la maturité d'expéditeur ?

A. Non, Talos ne change pas manuellement la maturité de l'expéditeur d'un domaine. La maturité d'expéditeur change automatiquement basé sur des changements du contexte de données internes disponible pour le domaine à un moment.

Q. Pourquoi est-ce qu'un domaine a une maturité différente d'expéditeur après une courte période ?

Les premiers affichages de message une maturité d'expéditeur de 10 mois :

02 Apr 2020 09:40:38 (GMT +02:00)

Message 82366447 Domains for which SDR is requested: reverse DNS host: xxxxxxxx.com, helo: xxxxxxxx.com, env-from: xxxxxxxx.net, header_from: xxxxxxxx.net, reply_to: Not Present

02 Apr 2020 09:40:38 (GMT +02:00)

Message 82366447 Consolidated Sender Reputation: Neutral, Threat Category: N/A. Youngest **Domain Age: 10 months 15 days** for domain: xxxxxxxx.net

Les deuxièmes affichages de message une maturité d'expéditeur de 13 jours - quoique c'est le même domaine :

12 May 2020 09:54:12 (GMT +02:00)

Message 86558836 Domains for which SDR is requested: reverse DNS host: xxxxxxxx.com, helo: xxxxxxxx.com, env-from: xxxxxxxx.net, header_from: xxxxxxxx.net, reply_to: Not Present

12 May 2020 09:54:12 (GMT +02:00)

Message 86558836 Consolidated Sender Reputation: Weak, Threat Category: N/A. Youngest **Domain Age: 13 days** for domain: xxxxxxxx.net

A. Les utilisations de Talos de sources pour dériver la maturité d'expéditeur peuvent changer basé sur des changements du contexte de données internes au sujet d'un domaine. Ceci peut avoir en voyant différentes étiquettes d'âge de domaine pour un domaine donné dans le message ESA dépistant le log comme dans l'exemple ci-dessus. Tandis que rares, de telles modifications doivent être prévues et n'exigent pas l'intervention.