Baromètre du Spam

AVRIL/MAI/JUIN 2023

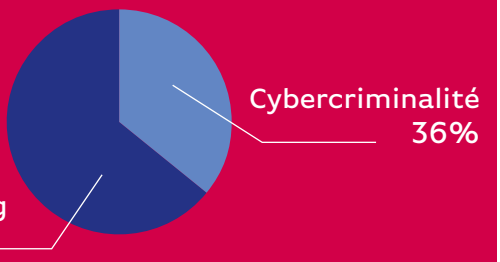
signal spam
SIGNALER, **C'EST AGIR !**

Association à but non lucratif, Signal Spam met à disposition des outils de signalement permettant aux internautes de signaler tout e-mail qu'ils jugent indésirable. Sur la base de ces signalements, Signal Spam alimente les acteurs de l'économie numérique et les autorités publiques en informations permettant d'agir contre le spam et les menaces associées à la cybercriminalité.

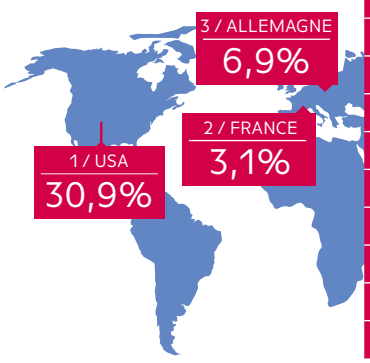
SIGNALEMENTS TRIMESTRIEL D'AVRIL À JUIN 2023

7 068 559 SIGNALEMENTS

RÉPARTITION MARKETING / CYBERCRIMINALITÉ



PROVENANCE GÉOGRAPHIQUE DU SPAM SIGNALÉ



1	USA	30,9%
2	FRANCE	23,1%
3	ALLEMAGNE	6,9%
4	CANADA	5,7%
5	ROUMANIE	3,5%
6	RUSSIE	3,4%
7	POLOGNE	2,6%
8	ROYAUME-UNI	2,4%
9	MONACO	1,8%
10	UKRAINE	1,4%

160 000

C'EST LE NOMBRE D'OUVERTURES DE **PAGES DE PHISHING BLOQUÉES** GRÂCE AUX **MODULES SIGNAL SPAM**

UTILISATEURS DE SIGNAL SPAM

NOMBRE TOTAL :

200 K

NOMBRE DE NOUVEAUX UTILISATEURS DANS CE TRIMESTRE :

26 195

TOP 10 DES SUJETS

Professionnels, profitez de l'installation offerte
Offre d'essai prospection : 10 000 mail pour 19,90 euros
Ne jetez pas vos factures impayées
Téléchargez le Guide de la gestion de la paie avec S***
Mobility Business, des services sur-mesure pour vos véhicules pro
Vérifiez votre visibilité sur internet
IMPRIMANTES - ENCRES - TONERS : profitez des meilleurs tarifs
Professionnels, roulez en «*modèle de voiture*» électrique
Découvrez notre Executive Mastère Spécialisé® Direction Marketing et Digital
Les voitures électriques «*marque de voiture*»

Toutes les informations sur **www.signal-spam.fr** ou sur nos réseaux sociaux

LE PHISHING : UNE MENACE RÉELLE À NE PAS SOUS-ESTIMER

Aujourd'hui, nous vivons dans un monde de plus en plus connecté. Malheureusement, cette connectivité accrue comporte également son lot de dangers, notamment le phishing. Dans cet article, nous allons nous pencher sur cette menace grandissante qui vise à tromper les utilisateurs et à leur dérober des informations confidentielles.

Le phishing : une menace en pleine expansion

Le phishing, ou hameçonnage en français, est une technique frauduleuse utilisée par des cybercriminels pour obtenir des informations confidentielles, telles que des identifiants de connexion, des données bancaires ou des informations personnelles. L'email reste un principal vecteur d'attaque de phishing et de distribution de malwares, et notamment des ransomwares.

L'article de Vade Secure met en évidence une attaque de phishing sophistiquée contre les utilisateurs de Microsoft 365. Les cybercriminels derrière cette attaque ont utilisé une combinaison de techniques d'ingénierie sociale et de faux sites web pour tromper les utilisateurs et leur voler leurs identifiants de connexion. Ces informations étaient ensuite utilisées pour accéder aux comptes des victimes et mener des activités frauduleuses.

Top 5 des noms d'hôte des pages de phishing dont l'ouverture est bloquée grâce aux modules Signal Spam :

1/ storage.googleapis.com
2/ d15k2d11r6t6rl.cloudfront.net
3/ testez-echantillon.world
4/ ipolos-work.com
5/ 21-domain.biz

Avertissement aux internautes :

Derrière storage.googleapis.com peuvent se cacher des faux liens de désinscription.

Ces méthodes d'attaque soulignent à quel point les cybercriminels sont devenus ingénieux dans leurs méthodes, en créant des e-mails et des sites web qui ressemblent presque parfaitement à ceux légitimes. Cela rend difficile pour les utilisateurs de faire la différence entre une communication légitime et une tentative de phishing. Les conséquences de telles attaques peuvent être dévastatrices, allant de la compromission des comptes professionnels à la fuite d'informations sensibles.

Comment se protéger contre le phishing ?

1. **Méfiez-vous des e-mails et des messages suspects :** Soyez attentif aux emails non sollicités ou aux messages provenant d'expéditeurs inconnus. Vérifiez attentivement les adresses d'email et les liens avant de cliquer dessus.

2. **Évitez de divulguer des informations confidentielles :** Les institutions légitimes ne vous demanderont jamais de leur fournir des informations sensibles par e-mail. Soyez vigilant et ne partagez pas vos mots de passe ou vos informations financières par ce biais.

3. **Utilisez une solution de sécurité fiable :** Assurez-vous de disposer d'un logiciel de sécurité à jour sur tous vos appareils. Les solutions de sécurité modernes peuvent détecter et bloquer les tentatives de phishing.

4. **Sensibilisez-vous et sensibilisez les autres :** Restez informé.e.s sur les dernières techniques de phishing et partagez vos connaissances avec vos entourages. Plus nous sommes informés, plus nous sommes en mesure de détecter et d'éviter les attaques.