Baromètre du Spam

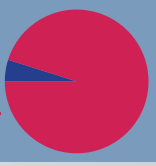
JANVIER/FÉVRIER/MARS 2019

signal spam

SIGNALER, **C'EST AGIR !**

Signal Spam effectue ses statistiques à partir des e-mails signalés comme spam qui sont parvenus jusqu'à l'internaute (c'est-à-dire qui sont délivrés dans sa boîte de réception). La majeure partie du spam (près de 90%) est filtrée en amont par les outils anti-spam des fournisseurs d'accès internet et de messagerie, et ne touche jamais l'internaute. Les signalements effectués auprès de Signal Spam portent sur cette fraction du spam qui parvient jusqu'aux internautes (environ 10%), ce qui les rend d'autant plus important pour l'analyse du phénomène et la protection collective.

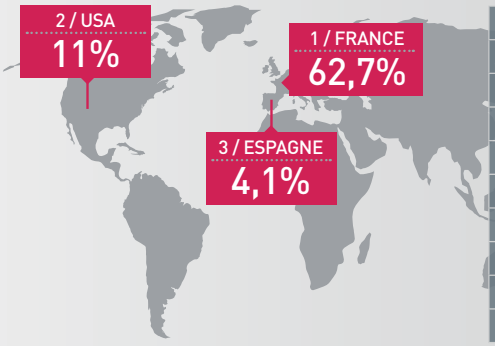
Répartition Marketing / Cybercriminalité



SIGNALEMENTS TRIMESTRIEL
DE JANVIER À MARS 2019

7 157 635 SIGNALEMENTS

PROVENANCE GÉOGRAPHIQUE DES SIGNALEMENTS

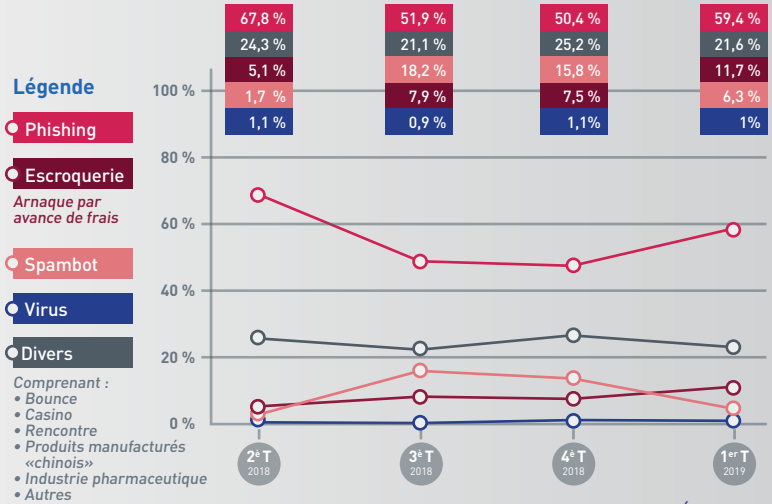


1	FRANCE	62,7%
2	USA	11%
3	ESPAGNE	4,1%
4	ANGLETERRE	3,3%
5	POLOGNE	2,1%
6	RUSSIE	1,8%
7	CANADA	1,8%
8	ALLEMAGNE	1,8%
9	ITALIE	1,3%
10	BRÉSIL	0.9 %

LE TOP 10 DES OBJETS

n°	Objet
1	Votre mutuelle à partir de 8 euros par mois
2	La Clé USB Nouvelle Génération pour votre Smartphone -40% De Remise Immediate+Livraison Offerte
3	Remplacez votre baignoire par une douche à l'italienne
4	Rendons nos routes plus sures !
5	Découvrez vos 3 devis
6	Isolez votre logement pour 1 euro
7	Isolez votre maison pour 1 EUR
8	Comparez les assurances auto
9	Assurance complémentaire santé : Votre devis en ligne dès maintenant !
10	Demandez votre guide découverte des tapisseries *(société)*

ÉVOLUTION DU SPAM D'ORIGINE CYBERCRIMINELLE



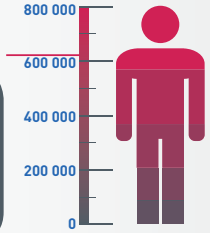
LE TOP DES OBJETS PAR CATÉGORIE

n°	Objet par Catégorie / PHISHING	Objet par Catégorie / SCAMY	Objet par Catégorie / SPAMBOT
1	Sécurité : Activation du service Clé Digitale	Offre de prêts	message
2	***SPAM*** Essayez Notre CBD Cliniquement Valide Et 100% Biologique!	Bonjour	*(société d'expédition)* Order Confirmation
3	Dernier Rappel: Notre système a détecté que vous n'avez pas encore activé la CLÉ DIGITALE !	Hello	*(prénom)* vous a envoyé un message
4	Rappel : Suivi Votre Colis	NEW MESSAGE FROM *(banque)* NEW YORK	Notre offre d'emploi 2865 euros/mois
5	Rappel : Suivez vos expéditions *(société d'expédition)*	Offre de prêts	Regarde moi seulement

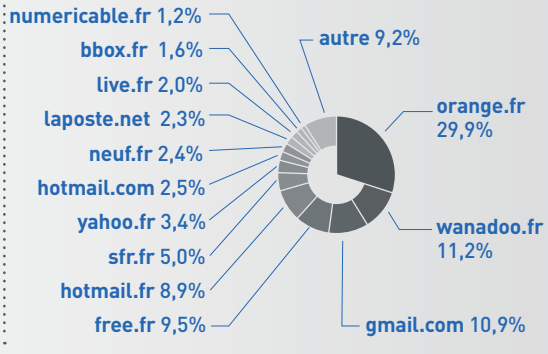
NOMBRE D'UTILISATEURS TOTAL DE SIGNAL SPAM

612 570

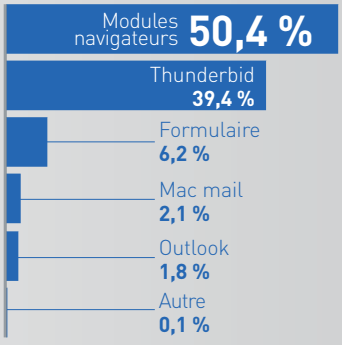
DONT **45,552** NOUVEAUX UTILISATEURS SUR LES TROIS DERNIERS MOIS



MESSAGERIES DES INTERNAUTES INSCRITS À SIGNAL SPAM



MOYEN DE SIGNALEMENTS



FOCUS // KIT DE SENSIBILISATION

L'ARNAQUE AU FAUX SUPPORT TECHNIQUE

La plateforme cybermalveillance.gouv.fr à laquelle appartient Signal Spam a produit des fiches réflexe de sensibilisation aux menaces cybercriminelles. Nous proposons en focus de ce baromètre une fiche thématique pour vous aider à mieux vous prémunir contre les risques inhérents aux communications électroniques et à la navigation sur internet.

FICHE RÉFLEXE 5

CYBERMALVEILLANCE.GOUV.FR
Assistance et prévention du risque numérique

L'ARNAQUE AU FAUX SUPPORT TECHNIQUE

L'arnaque au faux support technique (**Tech support scam** en anglais) consiste à effrayer la victime, par SMS, téléphone, chat, courriel, ou par l'apparition d'un message qui bloque son écran, lui indiquant un problème technique grave et un risque de perte de ses données ou de l'usage de son équipement, afin de la pousser à contacter un prétendu support technique officiel (Microsoft, Apple, Google…), pour ensuite la convaincre de payer un pseudo-dépannage informatique et/ou à acheter des logiciels inutiles, voire nuisibles. Si la victime refuse de payer, les criminels peuvent la menacer de détruire ses fichiers ou de divulguer ses informations personnelles.

BUT RECHERCHÉ

EXTORQUER DE L'ARGENT
à la victime en la poussant à laisser prendre le contrôle de sa machine pour faire semblant de la lui dépanner et lui installer des logiciels et/ou faire souscrire des abonnements qui lui seront facturés.

SI VOUS ÊTES **VICTIME**

NE RÉPONDEZ PAS AUX SOLLICITATIONS et n'appelez jamais le numéro indiqué.

CONSERVEZ TOUTES LES PREUVES. Photographiez votre écran au besoin.

S'il semble « bloqué », **REDÉMARREZ VOTRE APPAREIL**. Cela peut suffire à régler le problème.

Si votre navigateur reste incontrôlable, **PURGEZ LE CACHE, SUPPRIMEZ LES COOKIES, RÉINITIALISEZ LES PARAMÈTRES PAR DÉFAUT** et si cela ne suffit pas, supprimez et recréez votre profil.

DÉSINSTALLEZ TOUTE NOUVELLE APPLICATION SUSPECTE présente sur votre appareil.

FAITES UNE ANALYSE ANTIVIRUS approfondie de votre machine.

Si un faux technicien a pris le contrôle de votre machine, **DÉSINSTALLEZ LE PROTOCOLE ET/OU LE PROGRAMME DE GESTION À DISTANCE, ET CHANGEZ TOUS VOS MOTS DE PASSE**. En cas de doute ou si vous n'arrivez pas à reprendre le contrôle de votre équipement par vous-même, vous pouvez faire appel à un prestataire référencé sur www.cybermalveillance.gouv.fr.

Si vous avez fourni vos coordonnées bancaires ou de carte de crédit, **FAITES OPPOSITION** sans délai. Si un paiement est débité sur votre compte, **EXIGEZ LE REMBOURSEMENT** en indiquant que vous déposez plainte.

Si vous avez été contacté par un faux support technique, **SIGNALEZ-LE AU SUPPORT OFFICIEL** (Microsoft, Apple, Google…). **SIGNALEZ LES FAITS AU MINISTÈRE DE L'INTÉRIEUR** sur sa plateforme Internet-signalement.gouv.fr.

DÉPOSEZ PLAINTE au commissariat de police ou à la brigade de gendarmerie, ou en écrivant au procureur de la République dont vous dépendez. Faites vous au besoin assister par un avocat spécialisé.

MESURES **PRÉVENTIVES**

Appliquez de manière régulière et systématique les mises à jour de sécurité du système et des logiciels installés sur votre machine, en particulier vos navigateurs.

Tenez à jour votre antivirus et **activez votre pare-feu**. Vérifiez qu'il ne laisse passer que des applications et services légitimes.

Évitez les sites non sûrs ou illicites, tels ceux qui hébergent des contrefaçons (musique, films, logiciels…) ou certains sites pornographiques qui peuvent infecter votre machine ou héberger des régies publicitaires douteuses.

N'installez pas d'application ou de programme « piratés », ou dont l'origine ou la réputation sont douteuses.

N'utilisez pas un compte avec des droits « administrateur » pour consulter vos messages ou naviguer sur Internet.

N'ouvrez pas les courriels, leurs pièces jointes et ne cliquez pas sur les liens provenant de chaînes de messages, d'expéditeurs inconnus, ou d'un expéditeur connu, mais dont la structure du message est inhabituelle ou vide.

Faites des sauvegardes régulières de vos données et de votre système pour pouvoir le réinstaller dans son état d'origine.

Aucun support technique officiel ne vous contactera jamais pour vous réclamer de l'argent.

CYBERMALVEILLANCE.GOUV.FR
Assistance et prévention du risque numérique

LES **INFRACTIONS**

En fonction du cas d'espèce, les infractions suivantes peuvent être retenues :

• L'incrimination principale qui peut être retenue est l'**escroquerie**. L'**article 313-1 du code pénal** dispose que : « *l'escroquerie est le fait, soit par l'usage d'un faux nom ou d'une fausse qualité, soit par l'abus d'une qualité vraie, soit par l'emploi de manœuvres frauduleuses, de tromper une personne physique ou morale et de la déterminer ainsi, à son préjudice ou au préjudice d'un tiers, à remettre des fonds, des valeurs ou un bien quelconque, à fournir un service ou à consentir un acte opérant obligation ou décharge* ». L'escroquerie est passible de cinq ans d'emprisonnement et de 375 000 euros d'amende.

• Si la victime est menacée de suppression de ses fichiers ou en est victime, de tels procédés relèvent de l'**extorsion de fonds**. En effet, ils se caractérisent par une contrainte physique – le blocage de l'ordinateur ou la destruction de fichiers – obligeant à une remise de fonds non volontaire. L'**article 312-1 du code pénal** dispose que : « *l'extorsion est le fait d'obtenir par violence, menace de violences ou contrainte soit une signature, un engagement ou une renonciation, soit la révélation d'un secret, soit la remise de fonds, de valeurs ou d'un bien quelconque* ». L'extorsion est passible de sept ans d'emprisonnement et de 100 000 euros d'amende.

• L'infraction d'**atteinte à un système de traitement automatisé de données (STAD)** pourra également être retenue. Les **articles 323-1 à 323-7 du code pénal** disposent que : « *le fait d'accéder ou de se maintenir frauduleusement* » dans un STAD, « *la suppression ou la modification de données contenues dans le système* », ou l'« *altération du fonctionnement de ce système* » sont passibles de deux ans à sept ans d'emprisonnement et de 60 000 euros à 300 000 euros d'amende.

RETROUVEZ TOUTES NOS PUBLICATIONS SUR :
www.cybermalveillance.gouv.fr

Version 2.0

A PROPOS DE SIGNAL SPAM

Signal Spam œuvre pour la sécurité des réseaux et la restauration de la confiance envers les communications électroniques.
Issue d'un partenariat public/privé, Signal Spam est une association à but non lucratif qui mobilise depuis 2005 les internautes. Après s'être enregistré sur le site www.signal-spam.fr, l'internaute signale tout e-mail qu'il juge indésirable à partir de son logiciel de messagerie ou sur le site www.signal-spam.fr.
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.