Baromètre du Spam

OCTOBRE/NOVEMBRE/DÉCEMBRE 2017

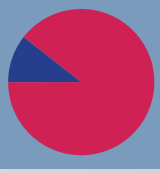
signal spam
SIGNALER, **C'EST AGIR !**

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

Cybercriminalité

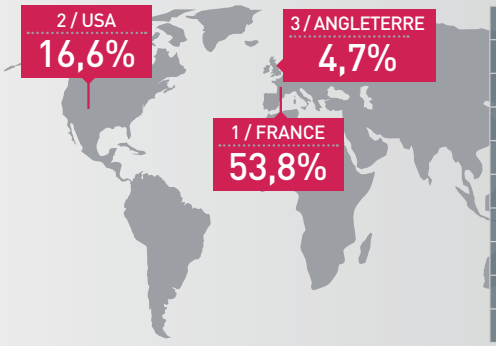
Marketing
89,4 %



SIGNALEMENTS TRIMESTRIEL
DE OCTOBRE À DÉCEMBRE 2017

3 211 883
SIGNALEMENTS

PROVENANCE GÉOGRAPHIQUE DES SIGNALEMENTS



1	FRANCE	53,8%
2	USA	16,6%
3	ANGLETERRE	4,7%
4	ESPAGNE	4,2%
5	ALLEMAGNE	2,4%
6	ITALIE	2,4%
7	POLOGNE	1,6%
8	PAYS-BAS	1,4%
9	CHINE	1,3%
10	RUSSIE	1,1 %

LE TOP 10 DES OBJETS

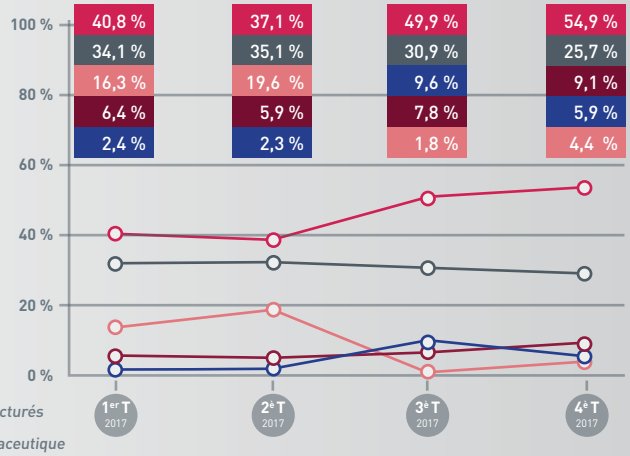
n°	Objet
1	hi
2	site : (*webmail*)
3	Ecoutez votre Ange Gardien !
4	Découvrez vite le radiateur Ultra Basse Conso
5	Votre mutuelle vous côute trop cher
6	Economisez jusqu'a 80% sur tout le site
7	Radiateurs : Prix exceptionnels
8	(*Nom d'un Assureur*) vous fait decouvrir la Convention Obseques
9	Undelivered Mail Returned to Sender
10	Votre invitation à venir essayer le (*modèle de voiture*) suréquipé

ÉVOLUTION DU SPAM D'ORIGINE CYBERCRIMINELLE

Légende

- Phishing
- Escroquerie
  Arnaque par avance de frais
- Spambot
- Virus
- Divers

Comprenant :
- *Bounce*
- *Casino*
- *Rencontre*
- *Produits manufacturés «chinois»*
- *Industrie pharmaceutique*
- *Autres*



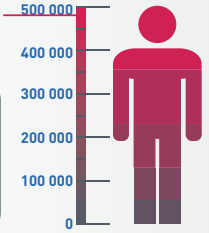
LE TOP DES OBJETS PAR CATÉGORIE

n°	Objet par Catégorie / PHISHING	Objet par Catégorie / SCAMY	Objet par Catégorie / SPAMBOT
1	Service Paiement securise par Internet - [78450120-65402225]	Conclure une Affaiire.	*** SPAM *** Purchase verified
2	URGENT : Service securise par Internet [009450120-65402225]	Bonjour	File has been damaged
3	Rappel : Vous devez avoir activer le service Cyber II Plus	GAiN 250.00 euros	File has been uploaded
4	Suivre votre colis	Hello	Image has been sent
5	Rappel : Vous devez avoir validez votre I PASS I	Offre de prêts	*** SPAM *** New message

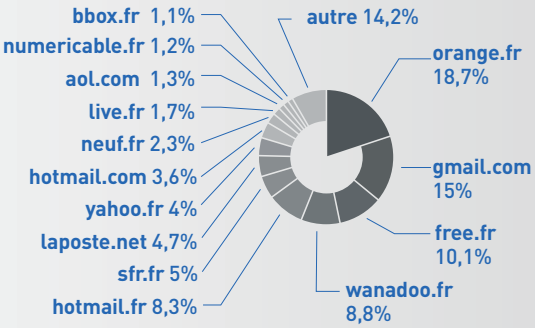
NOMBRE D'UTILISATEURS TOTAL DE SIGNAL SPAM

483 894

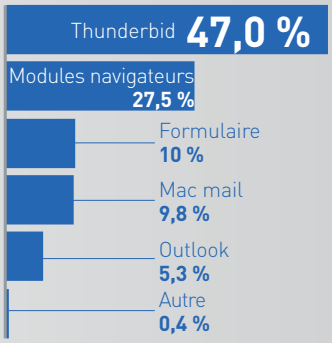
DONT
16 261
NOUVEAUX UTILISATEURS
SUR LES TROIS DERNIERS MOIS



MESSAGERIES DES INTERNAUTES INSCRITS À SIGNAL SPAM



MOYEN DE SIGNALEMENTS



signal spam
SIGNALER, C'EST AGIR !

FOCUS // L'ARNAQUE AU FAUX SUPPORT TECHNIQUE
14 DÉCEMBRE 2017 SUR CYBERMALVEILLANCE.GOUV.FR

Cette forme particulière d'escroquerie (appelée tech support scam en anglais) consiste à effrayer la victime afin de la pousser à contacter un prétendu support technique officiel ou son soit-disant sous-traitant (Microsoft, Apple, Google...) pour ensuite la convaincre de payer un pseudo dépannage informatique et/ou à acheter des logiciels inutiles voire nuisibles.
La victime peut être contactée par SMS, téléphone, courriel (email en anglais), messagerie instantanée (chat en anglais), ou voir apparaître un message sur l'écran de son équipement (ordinateur, tablette, smartphone) qui lui signale un problème grave (panne, virus, licence logiciel expirée...) et qui lui demande de rappeler un numéro de support technique d'apparence officielle, sous peine de perdre toutes ses données ou de ne plus pouvoir utiliser son matériel. Parfois, l'équipement de la victime peut sembler complètement bloqué et même l'être réellement dans des cas plus rares.

BUT RECHERCHÉ

L'objectif de ce type d'attaque commise par des organisations criminelles est d'extorquer de l'argent à la victime.
Par un discours bien rodé et en se faisant passer pour un support technique officiel ou son sous-traitant, les cybercriminels vont alors faire semblant de réparer la machine de la victime et lui facturer cette prestation de dépannage factice souvent plusieurs centaines d'euros. Les cybercriminels peuvent aller jusqu'à lui demander d'installer un logiciel sur sa machine qui va leur permettre d'en prendre le contrôle complet à distance.
Dans certains cas, lorsque la victime refuse de payer, les criminels n'hésitent pas à la menacer de détruire ses fichiers ou de divulguer les informations personnelles présentes sur sa machine.

MESURES PRÉVENTIVES

- Appliquez de manière régulière et systématique les correctifs de sécurité du système d'exploitation et des logiciels installés sur votre machine: en particulier vos navigateurs - Chrome, Edge, Firefox, Safari...
- Tenez à jour votre antivirus.
- Activez votre parefeu et vérifiez qu'il ne laisse passer que des applications et services légitimes.
- Évitez les sites non sûrs ou illicites, tels ceux hébergeant des contrefaçons (musique, films, logiciels...) ou certains sites pornographiques qui peuvent injecter du code en cours de navigation et infecter votre machine ou héberger des régies publicitaires douteuses.
- Lors de l'installation d'un nouveau logiciel, a fortiori s'il est présenté comme « gratuit », vérifiez si vous n'acceptez pas en même temps l'installation d'un autre programme ou d'un module qui pourraient modifier votre navigateur ou votre ordinateur.
- N'ouvrez pas vos courriels, et ne naviguez pas sur Internet depuis un compte ayant des droits « Administrateur ». Utilisez un compte ayant des droits « Utilisateur ».
- 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 au besoin.
- Retenez qu'aucun support technique officiel ne vous contactera jamais directement pour vous réclamer de l'argent.

signal spam
SIGNALER, C'EST AGIR !

SI VOUS ÊTES VICTIME

- Si vous êtes confronté à ce type d'arnaque quelle qu'en soit l'origine, surtout ne répondez pas aux sollicitations et n'appelez jamais le numéro indiqué.
- Conservez toutes les preuves pour le signalement ou le dépôt de plainte aux autorités (voir plus loin) : photographiez votre écran au besoin.
- Si votre appareil est bloqué, redémarrez-le, cela peut suffire à régler le problème.
- Si notre navigateur devient incontrôlable (affichage intempestif de fenêtres, navigation impossible...), purgez son cache, supprimez les cookies, réinitialisez ses paramètres par défaut et si cela ne suffit pas, supprimez et recréez votre profil.
- Vérifiez qu'aucune nouvelle application suspecte n'est présente sur votre appareil et si c'est le cas désinstallez-la.
- Réalisez une analyse approfondie de votre machine avec votre antivirus.
- Si un faux technicien a pris le contrôle de votre machine, il faut désactiver ou désinstaller le protocole et/ou le programme de gestion à distance qu'il a pu utiliser sur votre machine et changer tous vos mots de passe. Dans certains cas, une réinstallation complète de votre machine peut s'avérer nécessaire.
- 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 à un faux support technique, faites opposition sans délai auprès de votre banque
- Si un paiement est débité sur votre compte suite à cette arnaque, rappelez le faux support technique pour exiger le remboursement en indiquant que vous déposez plainte.
- Si vous avez été contacté par un faux support technique, que vous ayez donné suite ou non, signalez-le au support officiel dont il se revendique tels **Microsoft**, **Apple** ou **Google** qui, fréquemment concernés, recueillent les plaintes de leurs clients.
- Signalez également les faits sur la plateforme Pharos (**Internet-signalement.gouv.fr**) du ministère de l'Intérieur.
- Déposez plainte auprès de la police ou de la gendarmerie de votre domicile ou en écrivant au procureur de la République dont vous dépendez. Faites vous au besoin assister par un avocat.
- Contactez le service du ministère de l'Intérieur INFO ESCROQUERIES au 0 805 805 817 (numéro gratuit), pour être conseillé dans vos démarches.

LES INFRACTIONS

L'incrimination principale qui peut être ici retenue est l'escroquerie :
L'**article 313-1 du code pénal** dispose : 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 manoeuvres 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 : 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 € à 300 000 € d'amende.

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.