Baromètre du Spam

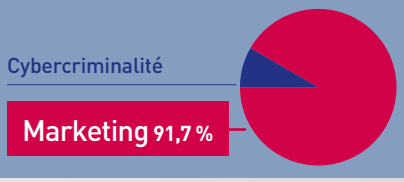
JUILLET/AOUT/SEPTEMBRE

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.

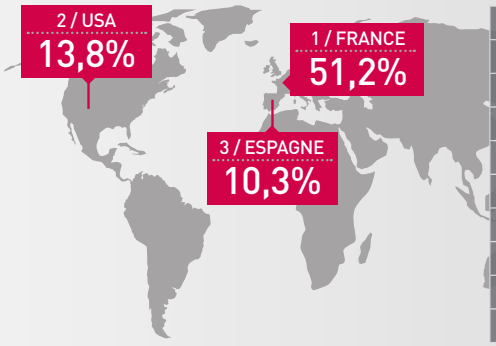
Répartition Marketing / Cybercriminalité



SIGNALEMENTS TRIMESTRIEL
DE JUILLET À SEPTEMBRE 2019

5 591 717 SIGNALEMENTS

PROVENANCE GÉOGRAPHIQUE DU SPAM SIGNALÉ

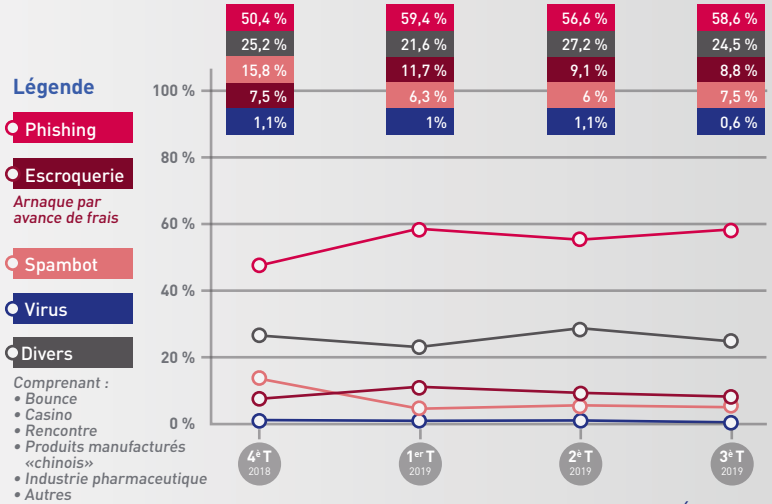


1	FRANCE	51,2%
2	USA	13,8%
3	ESPAGNE	10,3%
4	ANGLETERRE	3,5%
5	ALLEMAGNE	2,8%
6	POLOGNE	2,6%
7	RUSSIE	1,7%
8	TURQUIE	1,5%
9	ITALIE	1,3%
10	BRESIL	1,1 %

LE TOP 10 DES OBJETS

n°	Objet
1	Un outil de sport primordial à moins 57 pourcent
2	Consultez nos tarifs en ligne
3	Profitez de nos offres folles
4	Investissez en résidences services avec (nom)
5	Inscrivez vous pour l'isolation a 1 euro
6	Votre mutuelle à partir de 8 euros par mois
7	C'est la solution pour exporter vos photos
8	Profitez de nos offres extraordinaires sur site
9	Votre douche à l'italienne à la place de votre baignoire en moins de 8h
10	Vous souhaitez rénover votre intérieur ?

ÉVOLUTION DU SPAM D'ORIGINE CYBERCRIMINELLE

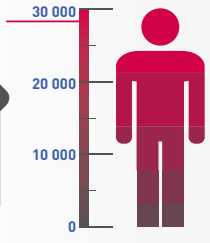


LE TOP DES OBJETS PAR CATÉGORIE

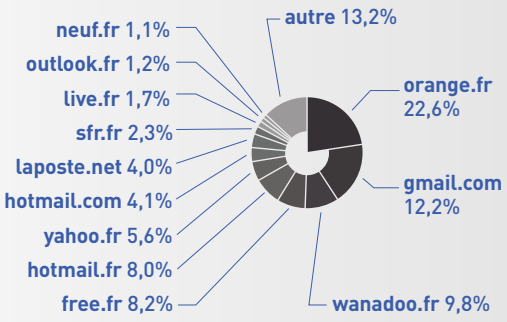
n°	Objet par Catégorie / PHISHING	Objet par Catégorie / SCAMY	Objet par Catégorie / SPAMBOT
1	*(société de livraison)* le remboursement de vos achats précédents est ici	Bonjour	Accusé de lecture
2	Vous devez confirmer votre participation avant de choisir de nouveaux gagnants	Cash loan as soon as tomorrow	Facebook
3	Cher client, toutes nos félicitation!	Hello	Bonjour
4	*(pseudo)* Nous Avons un Message important pour vous	Compensation Fund Department	Commentaire
5	*(magasin de distribution)* a essayé de vous atteindre plus tôt	Your gift is Accepted *(numero)*	hallo

NOMBRE D'UTILISATEURS DE SIGNAL SPAM

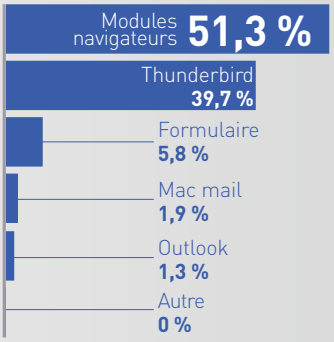
19 112 NOUVEAUX UTILISATEURS SUR LES TROIS DERNIERS MOIS



MESSAGERIES DES INTERNAUTES INSCRITS À SIGNAL SPAM



MOYEN DE SIGNALEMENTS



FOCUS // KIT DE SENSIBILISATION

LES MISES À JOURS

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.

CYBERMALVEILLANCE.GOUV.FR
Assistance et prévention du risque numérique

LES MISES À JOUR

ADOPTER LES **BONNES PRATIQUES**

Les appareils numériques et les logiciels que nous utilisons au quotidien sont exposés à des failles de sécurité. Ces failles peuvent être utilisées par des cybercriminels pour prendre le contrôle d'un ordinateur, d'une montre connectée ou d'un équipement mobile. Face à ces risques, les éditeurs et les fabricants proposent des mises à jour (*patch* en anglais) visant à corriger ces failles. Si l'opération de mise à jour est souvent ressentie comme une contrainte, il s'agit pourtant d'un acte essentiel pour se protéger. **Voici 10 bonnes pratiques à adopter pour vos mises à jour.**

1 PENSEZ À METTRE À JOUR SANS TARDER L'ENSEMBLE DE VOS APPAREILS ET LOGICIELS

Ordinateurs, téléphones, systèmes d'exploitation, logiciels de traitement de texte, objets connectés… nous utilisons un grand nombre d'appareils et de logiciels. Il suffit qu'un seul ne soit pas à jour et soit exposé à une faille de sécurité pour ouvrir une brèche dans votre environnement numérique. Afin d'empêcher les cybercriminels d'utiliser ces failles de sécurité pour vous pirater et vous dérober des informations personnelles sensibles, il est primordial de réaliser les mises à jour de vos équipements dès qu'elles sont disponibles.

DIFFÉRENTS TYPES DE MISES À JOUR

- **Les mises à jour importantes ou critiques** corrigent des failles de sécurité qui peuvent être utilisées pour pirater votre équipement.
- **Les mises à jour de version** apportent en général de nouvelles fonctionnalités et corrigent également des failles de sécurité. Ce type de mise à jour peut être payant.

2 TÉLÉCHARGEZ LES MISES À JOUR UNIQUEMENT DEPUIS LES SITES OFFICIELS

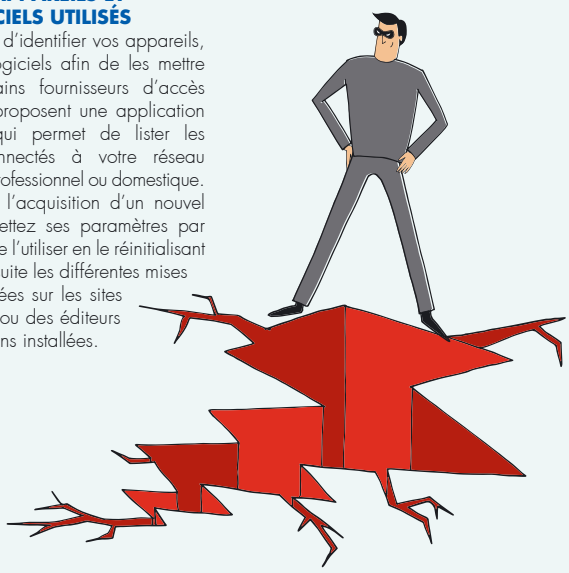
Seuls les sites ou dispositifs officiels des éditeurs et fabricants vous garantissent au mieux que les mises à jours que vous allez installer ne sont pas infectées par un virus. A l'installation de vos mises à jour, soyez attentif aux éventuelles conditions d'utilisation ou cases pré-cochées qui pourraient valoir acceptation de l'installation d'un autre logiciel non désiré (logiciels publicitaires, par exemple).

3 IDENTIFIEZ L'ENSEMBLE DES APPAREILS ET LOGICIELS UTILISÉS

Il est conseillé d'identifier vos appareils, matériels et logiciels afin de les mettre à jour. Certains fournisseurs d'accès Internet (FAI) proposent une application d'inventaire qui permet de lister les appareils connectés à votre réseau informatique professionnel ou domestique. Si vous faites l'acquisition d'un nouvel appareil, remettez ses paramètres par défaut avant de l'utiliser en le réinitialisant et installez ensuite les différentes mises à jour proposées sur les sites du fabriquant ou des éditeurs des applications installées.

4 ACTIVEZ L'OPTION DE TÉLÉCHARGEMENT ET D'INSTALLATION AUTOMATIQUE DES MISES À JOUR

Si le logiciel le permet, configurez-le pour que les mises à jour se téléchargent et s'installent automatiquement. Avec cette fonctionnalité, vous disposerez ainsi de la dernière version à jour de la solution de l'éditeur. Assurez-vous également que la mise à jour fonctionne par une vérification manuelle, au besoin.



QUELQUES EXEMPLES DE FAILLES DE SÉCURITÉ

• **Aux États-Unis,** des cybercriminels ont réussi à dérober des données confidentielles d'un **casino grâce au thermomètre connecté présent dans un aquarium** de l'établissement.

• **En France,** la **trottinette** électrique connaît un succès grandissant. **Une faille de sécurité sur certains modèles** a été découverte. Elle permettait d'exécuter certaines commandes sans avoir besoin du mot de passe comme **les déverrouiller, contrôler l'accélération ou le freinage**. Une mise à jour a été publiée pour corriger cette faille.

5 DÉFINISSEZ LES RÈGLES DE RÉALISATION DES MISES À JOUR

Pro

Pour assurer votre sécurité numérique, la définition de certaines règles peut faciliter l'opération de mise à jour, notamment en entreprise. Il s'agit par exemple de spécifier la façon de réaliser l'inventaire des appareils et logiciels utilisés, de savoir où et comment rechercher les mises à jour, comment et qui procède à la mise à jour ou encore à quel moment réaliser cette opération.

6 PLANIFIEZ LES MISES À JOUR LORS DE PÉRIODES D'INACTIVITÉ

Lorsqu'ils interrompent une activité personnelle ou professionnelle (visionnage d'une vidéo, rédaction d'un courriel…), les messages indiquant la disponibilité d'une mise à jour sont souvent ignorés car le processus de mise à jour peut être ressenti comme une contrainte. En effet, la mise à jour peut prendre du temps, allant de quelques secondes à plusieurs minutes ou heures, selon les cas. Aussi, profitez de périodes d'inactivité pour effectuer vos mises (déjeuner, réunion, de nuit…).

7 MÉFIEZ-VOUS DES FAUSSES MISES À JOUR SUR INTERNET

En navigant sur Internet, il arrive que des messages prenant l'apparence d'alertes de mises à jour apparaissent à l'écran : fausses publicités sur des sites Internet ou fenêtres (*pop-up* en anglais) malveillantes. Restez extrêmement vigilant car il peut s'agir d'une technique pour vous inciter à installer une prétendue mise à jour qui serait en réalité un virus.

8 INFORMEZ-VOUS SUR LA PUBLICATION RÉGULIÈRE DES MISES À JOUR DE L'ÉDITEUR

Pro

L'utilisation d'un appareil ou d'un logiciel pas à jour augmente les risques d'attaques informatiques. Si les mises à jour ne sont plus proposées, ils sont plus vulnérables. Aussi, avant l'acquisition d'un nouveau matériel ou logiciel, vérifiez la publication régulière des mises à jour de l'éditeur ou du fabricant, ainsi que la date de fin de leur mise à disposition. Lorsqu'une solution arrive en fin de vie et que des mises à jour ne sont plus proposées, identifiez les délais et les ressources nécessaires pour migrer vers de nouveaux outils afin de rester protégé.

9 TESTEZ LES MISES À JOUR LORSQUE CELA EST POSSIBLE ET FAITES DES SAUVEGARDES

Pro

Il arrive que la mise à jour d'un équipement ou d'un logiciel entraîne des conséquences inattendues, comme de rendre incompatible la solution qui vient d'être mise à jour avec un autre équipement ou logiciel. Il convient donc de tester les mises à jour lorsque cela est possible. Par ailleurs, n'hésitez pas à réaliser une sauvegarde de vos données et de vos logiciels avant une opération de mise à jour pour pouvoir revenir en arrière si nécessaire.

10 PROTÉGEZ AUTREMENT LES APPAREILS QUI NE PEUVENT PAS ÊTRE MIS À JOUR

Pro

Dans certains cas, des appareils peuvent ne pas être mis à jour pour diverses raisons, comme leur ancienneté, la perte d'une garantie ou d'un agrément. Il est, par conséquent, nécessaire de protéger ce dispositif autrement, par exemple en ne le connectant pas à Internet, en le séparant du reste du réseau informatique ou encore, en désactivant les services vulnérables.

BON À SAVOIR

Pro

En entreprise, s'il existe un service informatique, il est généralement chargé de la mise à jour des appareils et des logiciels. **Dans le cas contraire, ce sont les collaborateurs qui effectuent cette opération, sous l'autorité du chef d'entreprise.**

DOCUMENT RÉALISÉ AVEC NOS MEMBRES :

CESIN · CLUSIF · CROWDSTRIKE · Fédération Française de l'Assurance · paloalto · STORMSHIELD

Pro = destiné principalement aux professionnels

En partenariat avec l'Agence nationale de la sécurité des systèmes d'information

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

Version 1.0

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.