Baromètre du Spam

OCTOBRE / NOVEMBRE / DÉCEMBRE 2014

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

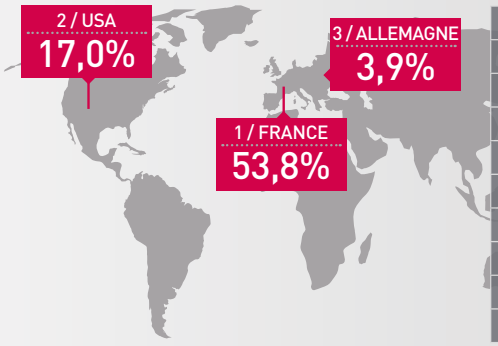
Marketing
76,9 %

SIGNALEMENTS TRIMESTRIEL

OCTOBRE À DÉCEMBRE 2014

1 116 889 SIGNALEMENTS

PROVENANCE GÉOGRAPHIQUE DES SIGNALEMENTS



1	FRANCE	53,8%
2	USA	17,0%
3	ALLEMAGNE	3,9%
4	ANGLETERRE	2,8%
5	ITALIE	2,3%
6	CHINE	1,8%
7	PAYS-BAS	1,3%
8	AUTRICHE	1,1%
9	RUSSIE	1,1%
10	BELGIQUE	1,0%

LE TOP 10 DES OBJETS

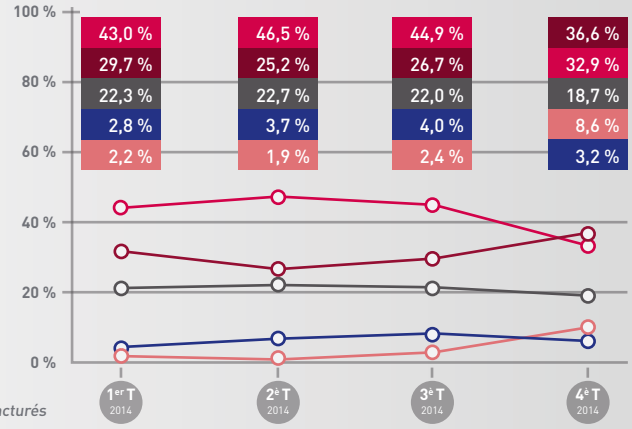
n°	Objet
1	Le guide de la nouvelle Loi Pinel
2	Apprenez l'anglais en 6 mois-test offert
3	Devenez propriétaire-investisseur
4	ventes privées dédiées au bricolage, jardin, maison
5	Votre mutuelle au meilleur prix
6	numero 1 des ventes privees de bricolage, jardinage maison
7	Pour vous, une superbe tablette tactile avec votre abonnement
8	Jusqu'à 75000 euros sans apport et sans aucun frais de dossier
9	Comparez et choisissez la Mutuelle adaptée a vos besoins
10	Feedback de 1001 cocktails

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*



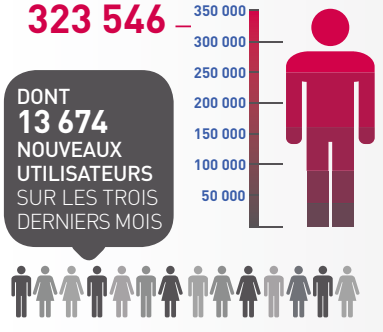
LE TOP DES OBJETS PAR CATÉGORIE

n°	Objet par Catégorie / PHISHING	Objet par Catégorie / SCAMY	Objet par Catégorie / SPAMBOT
1	Bonsoir	Deux Cent Cinquante Milles Euros	Message you sent blocked by our bulk email filter
2	RE: En Retour	fw: Réclamation 250.000 Euro	*** SPAM *** New voicemail(s) at Nov 1 2014, 09 seconds
3	Ca va?	RECLAMATION	Important notification
4	Bonjour	fw: Réclamation 250.000 Euro	*** SPAM *** Incoming voice mail
5	Tr: Bonjour, je m'appelle Mathilde	TR :tr: fw:Rania HASSAN	***SPAM*** nombreux produits high-tech a -80%

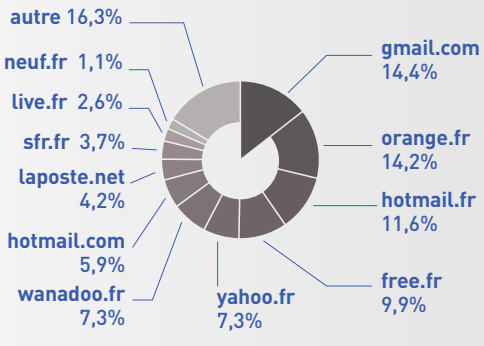
NOMBRE D'UTILISATEURS TOTAL DE SIGNAL SPAM

323 546

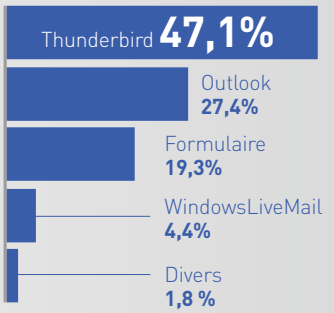
DONT **13 674** NOUVEAUX UTILISATEURS SUR LES TROIS DERNIERS MOIS



MESSAGERIES DES INTERNAUTES INSCRITS À SIGNAL SPAM



MOYEN DE SIGNALEMENTS



ANALYSE D'UN SPAM DE DIFFUSION DE VIRUS

Présentation du cas étudié

L'internaute reçoit un e-mail d'une boutique victime d'une usurpation de son nom et de son image, l'informant qu'une commande - qu'il n'a en réalité jamais passée - a bien été enregistrée, et le paiement associé correctement débité.

BOUTIQUE <commande@.com> Jan 19 (2 days ago)
to eric

Si vous ne parvenez pas à lire cet e-mail, cliquez ici

BOUTIQUE : .DE
Adresse URL : http://.DE

Bonjour ,

Cet e-mail confirme que nous venons d'enregistrer votre demande de paiement de 1845,89 EUR pour votre commande référencée FT0100X89 sur la boutique de .DE.

Détails du paiement

Identifiant du commerçant	: 009308598
Numéro de transaction	: 707501
Numéro de commande	: FT0100X89
Date / Heure	: 19-01-2015 / 03:58:31 (GMT+1)
Moyen de paiement	: e-Carte Bleue
Numéro de carte	: 4XXXXXXXXXXXXXX 04/15
Montant	: 1845,89 EUR
Type	: Débit
Numéro d'autorisation	: 11274546
Certificat	: 5WX5rff82779c75fc541trff80c4

Vous avez choisi le paiement par e-cartebleue donc votre carte a été débité de la totalité des frais pour plus d'informations concernant cette transaction veuillez accéder à votre compte e-cartebleue émis par votre banque ou bien vous avez accès à votre facture détaillée "Ma Facture -FT0100X89" Etant donné qu'aucune facture ne sera jointe à votre colis, je vous invite à bien conserver votre facture télécharger. En effet, celui-ci fait office de facture et de bon de garantie vous pouvez consulter l'historique de votre e-cartebleue le prélèvement sera visible d'ici 2 heurs.

La Boutique vous remercie de votre confiance.

exemple de personnalisation d'e-mail

La personnalisation de l'e-mail, même minimaliste (ici le prénom réel du destinataire, sans doute récupéré à moindre effort en analysant son adresse), est un facteur crédibilisant le message.

Autre facteur de persuasion : il n'est à aucun moment demandé de renseigner des données personnelles ou bancaires, comme le ferait un spam de hameçonnage (phishing). Ici le paiement aurait déjà eu lieu. Il est seulement proposé de visiter une page sur laquelle pointe un lien permettant soi-disant de consulter la facture, qui n'existe évidemment pas.

À la place, la page invite à télécharger un fichier en .zip. Une fois décompressé, le fichier apparait bien sur le bureau d'un ordinateur standard avec l'icône d'un PDF et le nom **Facture_client_dZZ8NEJBxg6yBDS.PDF** crédibilisant encore le fait qu'il puisse s'agir de la facture liée au paiement qu'aurait effectué l'internaute.

Mais il s'agit en réalité d'un exécutable : en paramétrant correctement son terminal pour qu'il affiche les extensions, le .exe apparait : **Facture_client_dZZ8NEJBxg6yBDS.PDF.exe.**

L'analyse d'un anti-virus confirme la dangerosité du fichier.

virustotal

SHA256:	65d347f62b7010e183ce0cdfba9b3695c0e9e2ff47ce716ebbd1085667983993
Nom du fichier :	Facture_client_dZZ8NEJBxg6yBDS.PDF.exe
Ratio de détection :	33 / 57
Date d'analyse :	2015-01-26 12:35:44 UTC (il y a 1 semaine)

0 0

analyse d'un anti-virus

De même que le test du comportement du fichier dans un bac à sable (sandbox en Anglais : un environnement de test pour les codes ou fichiers inconnus) :

File Details

FILE NAME	Facture_client_dZZ8NEJBxg6yBDS.PDF.exe
FILE SIZE	483936 bytes
FILE TYPE	PE32 executable (GUI) Intel 80386, for MS Windows
MD5	faf8846a4d4b1f8d4276b51be216c57c
SHA1	b71173951024cd5206e69c11a0e72abf0ceca5f0
SHA256	65d347f62b7010e183ce0cdfba9b3695c0e9e2ff47ce716ebbd1085667983993
SHA512	39f19f3e5369e91a941d43fcadcc5770e36c98dc8970679dcb189af16710e688d5c279833f1c91a45efa628be09a492a23eee5b952b4444ab17947e4121d6719
CRC32	4F8A0FB8
SSDEEP	6144:5LPe6wtlrY2JSleJcX9GEYZTjde0511sFZU0sJDnOlD+loFICw1kRfK9v:5be6w02JOJO0BjdWBqsCloGCEkY9v
YARA	None matched
	Download You need to login

Signatures

- Starts servers listening on 0.0.0.0:38071, 127.0.0.1:13719
- File has been identified by at least one AntiVirus on VirusTotal as malicious
- Performs some HTTP requests
- Queries information on disks, possibly for anti-virtualization
- Executed a process and injected code into it, probably while unpacking
- Tries to unhook Windows functions monitored by Cuckoo
- Collects information to fingerprint the system (MachineGuid, DigitalProductId, SystemBiosDate)
- Creates Zeus (Banking Trojan) mutexes
- Creates a slightly modified copy of itself
- Installs itself for autorun at Windows startup

test de comportement du fichier

Le spam quant à lui provient d'un expéditeur légitime dont l'infrastructure est abusée.

Entête technique :

```
Delivered-To: ――――@gmail.com
Received: by 10.25.125.198 with SMTP id y189csp146330lfc;
        Mon, 19 Jan 2015 03:09:55 -0800 (PST)
X-Received: by xx.xxx.x.xxx with SMTP id db4mr29824340lad.79.1421665792962;
        Mon, 19 Jan 2015 03:09:52 -0800 (PST)
Authentication-Results: mx.google.com;
       spf=softfail (google.com: domain of transitioning noreply@[redacted].com does not designate xxx.xxx.xx.xx as permitted sender)
smtp.mail=noreply@[redacted].com;
       dkim=pass header.i=@[redacted].com
Received-SPF: softfail (google.com: domain of transitioning noreply@[redacted].com does not designate xxx.xxx.xx.xx as permitted sender) client-ip=
xxx.xxx.xx.xx;
Received: by xx.xxx.xxx.xxx with POP3 id gf13mf3676996lab.16;
        Mon, 19 Jan 2015 03:09:52 -0800 (PST)
X-Gmail-Fetch-Info: ――――@f――――.com 6 ssl0.ovh.net 995 postmaster%―――.com
Return-Path: <noreply@[redacted].com>
Delivered-To: postmaster@―――.com
Received: from b0.ovh.net (HELO queue) (213.186.33.50)
                by b0.ovh.net with SMTP; 19 Jan 2015 12:29:00 +0200
Received: from localhost (HELO mail109.ha.ovh.net) (127.0.0.1)
  by localhost with SMTP; 19 Jan 2015 12:29:00 +0200
Received: from b0.ovh.net (HELO queueout) (xxx.xxx.xx.xx)
                by b0.ovh.net with SMTP; 19 Jan 2015 12:29:00 +0200
Delivered-To: ――――@――――.com
Received: from b0.ovh.net (HELO queue) (xxx.xxx.xx.xx)
                by b0.ovh.net with SMTP; 19 Jan 2015 12:29:00 +0200
Received: from fotothun.com (94.143.19.209)
  by mx1.ovh.net with SMTP; 19 Jan 2015 12:28:58 +0200
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed; d=[redacted].com;
 q=dns/txt; s=mail; bh=XJ/XN68qDfOLw26SkEbvGpop8MNE4VqOEowFUIBg1/8=;
 h=from:reply-to:subject:date:mime-version:content-type:list-id:list-unsubscribe;
       b=qPeTCe3FsQ6RSG2WXSo5yeEpfupBlz18S6DdRdWuRQxoHtVN9gJvWmC2Gfc7zmg/8Tinm0gIO2OL
       zswjJRFs2DQV/p7A0G3fY61rl4jjxKvXW3Keq3Elfb7DPbOqLfQHpm878Mv7XdcMwfkPYJKlnge7
       2g/s0RNwQ8bp+MwpqUg=
To: <――――@――――.com>
Subject: =?UTF-8?Q?Facture_de_votre_commande_-_Pensez_=C3=A0_l'imprimer_ou_=C3=A0_la_sauvegarder.?=
From: =?UTF-8?Q?BOUTIQUE=20[redacted]=20?= <commande@fotothun.com>
List-Id: MTA2MzkxMC0xMTY2NDctMTE= <MTA2MzkxMC0xMTY2NDctMTE=.list-id.[redacted].com>
List-Unsubscribe: <mailto:unsubscribe@[redacted].com?subject=unsub-3o6506scr81fj&body=3o6506scr81fj>,<http://r.[redacted].com/j0wrascr81fg.html>
Content-Type: multipart/alternative; boundary="------?=_53369-4625980286962"
MIME-Version: 1.0
Precedence: bulk
Feedback-ID: ded_xx.xxx.xx.xxx:1063910:1063910_7:espname
X-Mailer: espname
X-Mailin-Client: xxxxxx
X-Mailin-Campaign: 7
Reply-To: commande@[redacted].com
Message-Id: <201501190511.3o6506scr81fj@[redacted].com>
Date: Mon, 19 Jan 2015 05:11:06 +0100
X-Ovh-Tracer-Id: 15882507037257698659
X-Ovh-Remote: xx.xxx.xx.xxx([redacted].com)
X-Ovh-Local: xxx.xxx.xx.xx (mx1.ovh.net)
X-OVH-SPAMSTATE: OK
X-OVH-SPAMSCORE: 0
X-OVH-SPAMCAUSE: gggruggvucftvghtrhhoucdtuddrfeejjedrjeeiucetufdoteggodetrfcurfhrohhfihhlvgemucfqggfjnecuuegrihhlohhuthemuceftddtnecu
```

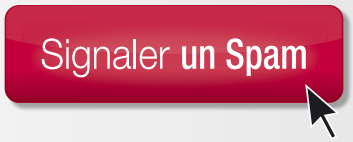
analyse de l'email expéditeur

Le malware infectant l'ordinateur peut avoir plusieurs fonctions :

- Infecter la machine et la relier à un botnet (un tiers peut donner des ordres à votre machine)
- Analyser les combinaisons de touches sur le clavier et les transmettre à tiers, notamment dans le but de récupérer des identifiants bancaires
- Identifier et transmettre des données personnelles sur la machine infectée

COMMENT SIGNALER UN MALWARE ?

1. **Signaler le spam « malware » à Signal Spam comme n'importe quel autre spam.** Celui-ci sera identifié comme diffusant un malware, et les informations autorisant une action seront transmises aux membres et partenaires (sociétés victimes, routeurs, hébergeurs, CERTs et autorités) de l'association qui pourront empêcher sa diffusion et protéger l'internaute.



2. **L'hébergeur du site doit être notifié du contenu malfaisant qu'il héberge sur sa plateforme.**
3. **La société victime doit être notifiée de l'usurpation de son nom pour piéger ses clients :** elle pourra mettre en place des contre-mesures auprès des hébergeurs / registrar / listes noires.
4. **Enfin, les forces de l'ordre ont la capacité de récupérer les données en ligne et chez l'hébergeur pour investigation.** Ils pourront identifier les victimes potentielles et prévenir les tiers si cela n'est pas déjà fait.

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.