

Defend what you create

Mini-guide sur la sécurité à destination des petites entreprises

**Pourquoi et comment
se protéger des menaces
informatiques ?**

Dans un monde où les outils de communication se multiplient et se perfectionnent de jour en jour, et où Internet est devenu un véritable outil de travail, la question de la sécurité informatique se pose à tous. Sortie des laboratoires d'experts, la problématique de la protection contre la cybercriminalité est devenue une préoccupation publique et les médias s'en font régulièrement l'écho.

Néanmoins, les attaques qui font le plus parler d'elles sont souvent celles qui affectent de grandes entreprises ou institutions et la presse spécialisée, c'est son rôle, traite de la sécurité informatique en des termes parfois très techniques.

Dans ce contexte, nous nous sommes interrogés : les TPE se sentent-elles concernées par ce sujet ? L'enjeu de la sécurité informatique est crucial aussi bien pour les petites que pour les grandes entreprises. La frontière entre vie privée et vie professionnelle est souvent mince dans une petite entreprise (artisans, commerçants, services etc.), et c'est, entre autres, pour cette raison que la protection des données et leur intégrité doit être garantie. Mais dans la réalité, les acteurs de ces petites structures se trouvent souvent démunis face à cet enjeu pour au moins trois raisons : manque de temps, manque de formation, manque de ressources humaines.

Notre ambition, à travers ce Mini-guide, est de faire comprendre cet enjeu majeur en expliquant de manière très simple et la plus concrète possible de quoi il s'agit lorsqu'on parle de « menaces informatiques », « malwares, trojan, virus, botnet » et autres termes qui ne recouvrent pas de réalité concrète pour les novices en la matière. Ce Mini-guide s'adresse donc à toutes les petites structures, aux entrepreneurs qui souhaitent acquérir une vision synthétique du sujet et quelques bonnes pratiques à mettre en place dans leur façon de travailler.

Nous avons souhaité dresser un panorama le plus clair et le plus accessible possible. Pour ceux qui souhaitent approfondir, nos chercheurs et analystes sont disponibles !

Doctor Web a plus de vingt ans d'expérience en recherche antivirus et en développement de logiciels antivirus.



Pierre Curien

Gérant
Doctor Web France



Cécile Chastanet

Responsable Communication
Doctor Web France

QUI S'ATTAQUE AUX DONNEES DES ENTREPRISES ET DES UTILISATEURS ?

Les pirates informatiques ou cybercriminels

Initialement, l'objectif de ces pirates du net est de **NUIRE** aux utilisateurs : particuliers, entreprises, administrations, voire Etats. Aujourd'hui, le piratage s'est organisé en véritable « industrie » et son objectif principal est, en plus de nuire, de **GAGNER DE L'ARGENT** grâce à ses méfaits.

Dans ce contexte, les utilisateurs sont d'autant plus menacés, car ils peuvent perdre plus que des données : abonnement à des services payants, envoi de SMS surtaxés, vol de données bancaires, usurpation d'instances officielles pour obliger les utilisateurs à payer en ligne une soi-disant « amende » pour un méfait qu'ils n'ont pas commis etc. Telles sont les principales activités des pirates actuels.

Les pirates ont suivi les évolutions technologiques qui ont révolutionné nos modes de communication et d'échanges d'information (Internet, messageries électroniques, réseaux sociaux etc...), et ils **ont perfectionné leurs techniques d'attaque, les moyens de diffuser des virus et le niveau technique de ces virus.**

Qui sont les **CIBLES** de ces pirates ?

Il existe plusieurs niveaux de criminalité informatique : certains réseaux organisés auront comme seul objectif de cibler une entreprise en particulier, ou même un Etat.

Mais, en général, le but des pirates est de toucher **LE PLUS GRAND NOMBRE D'UTILISATEURS POSSIBLE**, et de les atteindre **AU HASARD**, sans cibler un profil particulier. Le pirate cherche moins à cibler des personnes que des ordinateurs !

C'est pourquoi tout le monde est concerné par la sécurité informatique.

Un exemple : le BOTNET

Il existe un type de menace informatique appelée : BOTNET ou « réseau zombies ». Le but d'un Botnet est d'enrôler le plus grand nombre possible d'ordinateurs et de les pirater afin qu'ils envoient massivement des spams ou qu'ils réalisent d'autres actions malveillantes. Un Botnet est contrôlé par une personne ou un groupe de personnes qui effectue des opérations à distance sur les ordinateurs contaminés.

Les cybercriminels sont souvent désignés sous le terme de Hackers. Pour être précis, il convient de noter que les hackers sont, à l'origine, des experts en sécurité informatique qui contribuent à trouver les failles de sécurité et vulnérabilités des systèmes et des logiciels. Cependant, certains hackers ont choisi de devenir des cybercriminels.

QUE PEUT FAIRE UN VIRUS UNE FOIS INSTALLE SUR UNE MACHINE ?

Différents types de virus existent et chaque « famille » de virus à un but précis (cf glossaire à la fin de ce guide), mais nous pouvons essayer de résumer les actions les plus nuisibles qu'un virus peut exécuter sur un ordinateur ou sur un réseau d'ordinateurs en entreprise :

- Crypter les données de l'ordinateur (et parfois demander une rançon pour les récupérer)
- Voler des mots de passe et autres identifiants
- Voler des contacts (par exemple dans Outlook)
- Envoyer des spams à l'insu de l'utilisateur (que se passe-t-il si les destinataires de ces spams sont vos clients ?)
- Rendre inaccessible l'accès à certains fichiers, dossiers et/ou applications
- Modifier les paramètres système (de Windows)
- Nuire voire désactiver ou supprimer les logiciels de protection installés sur l'ordinateur

Les conséquences de cette liste non exhaustive de nuisances sont multiples et plus ou moins graves :

- Diffusion de données confidentielles sur Internet
- Dysfonctionnement des machines et des serveurs, voir arrêt complet du réseau de l'entreprise
- Pertes de données vitales et/ou confidentielles : certaines données ne pourront jamais être restaurées
- Impossibilité d'accéder à certains sites Internet (notamment des sites de mises à jour des logiciels de sécurité)
- Ralentissement des machines

Autant de nuisances qui peuvent tout simplement conduire à la **PARALYSIE TOTALE OU PARTIELLE DE L'ACTIVITE DE L'ENTREPRISE** ; Or, **les petites entreprises sont vulnérables car elles n'ont pas forcément les ressources humaines et matérielles pour faire face à un arrêt, même momentané, de leur activité.**

COMMENT LES VIRUS ARRIVENT-ILS SUR LES MACHINES ET LES APPAREILS PORTABLES ?

Les virus ou programmes malveillants existent et agissent, c'est une réalité. Mais pourquoi la menace est-elle si préoccupante ? Parce qu'ils peuvent pénétrer très facilement sur un ordinateur, sur un serveur, une tablette, un Smartphone, en utilisant notamment des techniques d'ingénierie sociale, fondées sur la crédulité de l'utilisateur, qui consistent à le pousser à installer lui-même un programme malveillant en cliquant sur un lien, en ouvrant une pièce jointe ou même un document PDF.

Alors, comment les virus arrivent-ils sur une machine ou un Smartphone ?

- **PAR EMAIL** : le courrier électronique est le moyen le plus facile de diffusion des virus. Un virus peut se dissimuler :

- **Dans une pièce jointe** : un fichier image (type JPG, PNG), un fichier compressé (type ZIP ou RAR), un fichier PDF, Power Point etc...
- **Dans un message spam** : le message contient en général un lien sur lequel l'utilisateur est invité à cliquer. C'est la page vers laquelle mène ce lien qui contiendra le virus.
- **Dans le corps du message** : indirectement, comme dans le spam, s'il contient un lien et invite l'utilisateur à le suivre.

Pour se protéger, la première arme est la vigilance. Avant de cliquer sur un lien ou d'ouvrir une pièce jointe, vérifiez la provenance du mail et lisez attentivement le message transmis. Bien souvent, le texte contenu dans le spam ou d'autres types de mails malveillants a été traduit par un outil en ligne et n'est pas correct stylistiquement.

PAR INTERNET :

- **certains sites web contiennent des pages piratées** qui, si elles sont cliquées, installeront un malware sur le PC ou la tablette de la victime, la plupart du temps sans qu'il s'en aperçoive. Les cybercriminels créent de « fausses » page web, imitant (parfois très bien) les pages de sites de banques ou de services (livraison, messageries, etc.).
- Certaines techniques virales consistent à **modifier une page web ouverte qui n'a pas été consultée depuis un moment** : l'internaute croyant être sur un site qu'il connaît est en réalité sur une fausse page imitant parfaitement la page officielle.
- Certaines **fenêtres publicitaires** (les « pop-up ») peuvent rediriger l'utilisateur vers des sites contenant des virus.

Là encore, la vigilance est la première protection. Vérifiez bien l'URL (l'adresse) de la page web que vous consultez, les « fausses » pages contiennent souvent un mot en plus ou en moins. *Par exemple : au lieu de <http://monservice.fr>, l'adresse URL sera <http://monservicebad.fr> . Ne pas cliquer sur les pop-up publicitaires est également conseillé.*

- **VIA UNE CLE USB** : les supports amovibles sont parfois porteurs de virus car ils passent d'un ordinateur à un autre. Si une machine est infectée et que le virus s'installe sur la clé, le prochain ordinateur à la recevoir sera à son tour infecté, notamment parce que beaucoup d'ordinateurs sont paramétrés pour ouvrir automatiquement les supports amovibles (autorun).

Il est particulièrement recommandé de ne pas connecter une clé USB à l'ordinateur de l'entreprise si elle a été utilisée auparavant dans un lieu public (cybercafé, hôtel, aéroports, gares etc...) ou sur un ordinateur sur lequel on ne sait pas comment le propriétaire utilise Internet.

- **VIA UN TELEPHONE MOBILE** : aujourd'hui, les virus ciblant les téléphones mobiles se développent, touchant notamment, et beaucoup, le système Android. Les virus arrivent le plus souvent sur les téléphones via des applications téléchargées sur les différents « market » disponibles.

Avant de télécharger une application, vérifiez sa source (est-ce un « market » officiel comme Google Play ou un site de téléchargements non officiel ?) et les droits qu'elle demande sur votre téléphone. *Par exemple : une application de bloc-notes n'a pas lieu de demander un accès à vos contacts ou à vos SMS.*

WINDOWS, MAC, LINUX : QUELLE REALITE DES MENACES SUR CES SYSTEMES D'EXPLOITATION (OS) ?

Pendant très longtemps, il a été dit que les Mac n'étaient pas susceptibles d'être touchés par des virus, car le système d'Apple était en quelque sorte « sécurisé de l'intérieur ». De plus, le nombre d'utilisateurs Mac dans le monde n'a pas, pendant longtemps, été « suffisant » pour mobiliser les cybercriminels, préférant s'attaquer au système Windows, adopté par des milliards d'utilisateurs. Cette affirmation était vraie, dans le passé.

Aujourd'hui, les menaces ciblant les Mac sont une réalité. Doctor Web a révélé, en avril 2012, la découverte d'un botnet enrôlant plus de 600 000 machines tournant sous Mac OS X. D'autres éditeurs d'antivirus ont également mis en lumière des malwares « dédiés » Mac.

De plus, et c'est souvent le cas dans les petites entreprises qui utilisent à la fois des PC et des Mac (les Mac pour leur activité principale et un PC pour la comptabilité, par exemple), les supports amovibles qui circulent d'un système d'exploitation à un autre véhiculent des malwares « compatibles » sur différents OS.

S'il est clair que Windows demeure le système d'exploitation le plus ciblé, et pour lequel les menaces sont de plus en plus sophistiquées, on ne peut plus faire l'impasse de la sécurité sous Mac.

Concernant Linux, système open source qui a également longtemps bénéficié d'une certaine immunité, la situation est également en train de changer progressivement avec pour preuve la découverte de malwares ciblant cet OS.

Conclusion ? Que l'on travaille sous Windows, sous Mac, ou sous Linux, mieux vaut prévenir que guérir. De nos jours, les malwares sont capables de s'adapter aux différents OS et de se lancer indifféremment sur l'un des trois systèmes. Même si les dommages ne seront peut-être pas équivalents selon l'OS touché, il est primordial de protéger ses données, notamment parce que de nombreuses entreprises peuvent travailler sous ces trois OS en même temps.

A QUOI SERT UN ANTIVIRUS ?

Les menaces informatiques sont une réalité, et dans un contexte de multiplication des outils de communication et d'omniprésence d'Internet, travailler sans protéger ses données comporte un risque. Néanmoins, certaines voix s'élèvent pour dire que les éditeurs d'antivirus exagèrent les menaces pour inciter les utilisateurs à acheter leurs produits. D'autres encore affirment qu'un antivirus « ne sert à rien » et qu'il ne protège pas.

C'est faux.

Ce qui est vrai, en revanche, c'est **qu'un logiciel antivirus ne peut pas protéger les ordinateurs à 100%**. Pour trois raisons majeures :

- **L'antivirus est un outil créé par l'homme** : même s'ils sont de plus en plus performants et qu'ils évoluent en permanence, les logiciels antivirus ne peuvent pas être infaillibles. De plus, chaque outil a des atouts différents. Les logiciels antivirus dépistent et éradiquent la plupart des menaces répertoriées et connues, même dans leur diversité de forme ou de propagation. Ils peuvent aussi manquer une menace.

- **Les pirates ont toujours une longueur d'avance** : ils peuvent étudier les mécanismes des anti-virus pour les contourner, ainsi que les failles d'autres logiciels pour fabriquer des virus « adaptés » à ces failles. Si le pirate peut étudier avec précision le fonctionnement des antivirus, les éditeurs de ces outils, eux, ne peuvent pas étudier en amont des virus qui n'existent pas encore ! Enfin, sans savoir d'où vient la menace ni où elle va frapper, difficile d'anticiper. Heureusement, les laboratoires antivirus étudient de très nombreux spécimens et anticipent au maximum les menaces à venir.
- **Le facteur humain** : l'infection d'un ordinateur est aussi liée à l'utilisation qui est faite d'Internet, à la vigilance de l'utilisateur et à son incrédulité. L'antivirus n'est pas dans la tête de l'internaute qui clique sur un lien suspect. Même s'il lui adresse un message d'alerte, c'est, là encore, l'humain qui prime.

Alors, à quoi sert un antivirus ?

Un logiciel antivirus représente un « **paravent** » ainsi qu'un « **remède** » face aux menaces informatiques. Ses trois fonctions majeures sont les suivantes :

- **DETECTER** les virus : grâce à des mécanismes techniques complexes, les logiciels antivirus ont la capacité d'analyser tout fichier qui semble suspect, par sa forme, son comportement, ses actions. De même, un lien Internet, un message email ou une pièce jointe sont scannés à la recherche d'objets suspects.
- **STOPPER** les virus : lorsque l'antivirus détecte un fichier suspect, il est capable de l'isoler du système, de le mettre en quarantaine afin de l'empêcher de contaminer tout l'ordinateur ou le réseau
- **DESINFECTER** : après avoir détecté un virus, les logiciels antivirus sont conçus pour « réparer », lorsque c'est possible techniquement, les fichiers endommagés ou piratés, pour restaurer les données.

Les laboratoires des éditeurs d'antivirus analysent des millions de virus chaque jour, et en extraient leur « empreinte », c'est ce que l'on appelle une **signature virale**. Ensuite, ces signatures sont regroupées dans des **bases de données**. Ainsi, à chaque fois que l'antivirus rencontrera de nouveau un fichier portant cette signature, il saura que c'est un virus et pourra l'arrêter. Les bases de données sont mises à jour plusieurs fois par jour, voire par heure.

C'est pourquoi il est primordial de mettre à jour l'antivirus installé sur un poste.

D'autres méthodes dites « comportementales » permettent aux logiciels antivirus d'analyser le « comportement » d'un fichier, d'une application ou d'un système afin de déceler une activité suspecte.

En conclusion, les antivirus ne sont pas des outils parfaits, mais ils peuvent éviter de très nombreuses contaminations virales et préserver les données vitales des ordinateurs. Le développement des virus croît à une vitesse considérable. **Il est clair qu'installer un antivirus est la meilleure façon de prévenir, car une fois l'infection installée, guérir n'est pas toujours possible !**

QUELQUES BONNES PRATIQUES A METTRE EN PLACE POUR EVITER LES INFECTIONS VIRALES

Si les antivirus sont des outils informatiques indispensables, il est clair que de nombreuses infections surviennent en raison de la crédulité de l'utilisateur, d'un manque de connaissances de sa part mais également parce que certaines règles de base ne sont pas mises en place et représentent ce que l'on appelle **des failles de sécurité**. Ces failles ou vulnérabilités peuvent être évitées en appliquant certaines pratiques simples. N'oublions pas que les pirates exploitent avant tout ces failles pour pénétrer dans un ordinateur ou un réseau : **ils comptent sur le manque de vigilance ou la crédulité des utilisateurs.**

Les mises à jour

Tous les logiciels qui sont utilisés sur un ordinateur doivent être régulièrement mis à jour. En général, l'éditeur de ces outils alerte l'utilisateur lorsque la mise à jour n'a pas été effectuée depuis longtemps ou si elle est nécessaire à un moment donné.

Ces mises à jour servent à renforcer la sécurité. Il est donc primordial :

- D'effectuer les mises à jour demandées par le système d'exploitation. Windows et Mac affichent des alertes concernant les mises à jour sur le poste. Les installer n'est pas une perte de temps, c'est un gain en sécurité.
- Mettre à jour l'antivirus sur les postes de travail

Les bonnes pratiques avec un antivirus

Pour que le logiciel antivirus soit le plus efficace possible dans l'entreprise, quelques règles à respecter :

- Installer un logiciel antivirus sur TOUS les postes de l'entreprise : un seul poste non protégé qui serait infecté peut contaminer tout le réseau
- S'assurer que les postes dits « nomades », les portables utilisés par les collaborateurs à la fois dans l'entreprise et à la maison, sont protégés par le même antivirus
- Toujours migrer vers les dernières versions de l'antivirus utilisé
- Effectuer les mises à jour demandées par l'antivirus
- Ne pas désactiver certaines fonctionnalités de l'antivirus
- Ne pas installer plusieurs antivirus sur une même machine ! Il convient de supprimer l'antivirus courant lorsque vous souhaitez changer de produit
- Effectuer un scan régulier des machines, en plus du fonctionnement quotidien de l'antivirus. Il est recommandé de le faire la nuit, car un scan complet peut être long.
- Sécuriser les appareils mobiles avec un antivirus

Les courriers électroniques

Comme nous l'avons vu, de nombreuses menaces peuvent se dissimuler dans un email. Pour éviter certaines déconvenues, la vigilance est la meilleure protection :

- **Ne répondez pas à un email non sollicité**, même s'il vient de votre banque, ou lisez-le attentivement. Même pour une opération de maintenance, votre banque ne vous demande généralement pas vos codes d'accès à son site, ni vos coordonnées bancaires (N° de compte, numéro de carte bleue, cryptogramme de votre carte etc...)

- **N'ouvrez pas une pièce jointe** si vous ne connaissez pas l'expéditeur ou si le message de l'email semble bizarre. Souvent dans le spam ou dans les messages vérolés, le texte n'est pas correct car il a été traduit de façon littérale par un outil en ligne.
- **Ne cliquez pas sur un lien Internet** sans avoir au préalable bien regardé l'expéditeur et lu le message l'accompagnant.

En cas de doute, mieux vaut faire analyser une pièce jointe ou un lien par un outil spécifique (des outils antivirus gratuits sont disponibles sur le marché).

Faire analyser un lien prend trois minutes = réparer un ordinateur après une infection peut prendre des jours, voire être impossible.

Les mots de passe

Certains outils viraux sont créés spécialement pour récupérer les mots de passe, et d'autres, en pénétrant sur un ordinateur, volent tous les mots de passe qu'ils trouvent. Quelques règles permettent de renforcer la sécurité autour des mots de passe :

- Changer régulièrement ses mots de passe
- Ne pas utiliser un mot de passe unique pour accéder à différentes applications ou différents services en ligne (exemple : le même mot de passe pour la messagerie personnelle, le site de la banque, la messagerie professionnelle, un site de loisir).
- Un mot de passe est personnel. Mieux vaut le mémoriser que le noter
- Créer un mot de passe dit « fort » : au moins 8 caractères, des lettres, des chiffres, des symboles.

Faire appel à des spécialistes

De nombreuses sociétés de dépannage et de maintenance informatique proposent des outils antivirus. Ce sont des spécialistes en sécurité qui peuvent intervenir rapidement auprès d'une petite structure pour des conseils, de la formation ou un dépannage. Consulter ces experts aidera les petites entreprises à choisir un outil mais également à l'installer et à en assurer la maintenance. En cas de problème, mieux vaut confier son ordinateur directement à un expert que d'essayer de « réparer » son ordinateur soi-même ou à l'aide de proches.

EN RESUME

- *Un virus informatique peut pénétrer sur un ordinateur EN UNE SECONDE*
- *Une infection virale peut entraîner une GRANDE PERTE DE TEMPS, mais également une PERTE DE DONNEES VITALES, voire, dans le pire des cas, un ARRET MOMENTANE DE L'ACTIVITE DE L'ENTREPRISE*

GLOSSAIRE

L'ingénierie sociale.

C'est un procédé qui consiste à tromper l'utilisateur pour l'inciter à effectuer une action dans le but de récupérer ses données personnelles : télécharger un fichier, cliquer sur un lien, répondre à un email etc... Les arguments avancés pour induire l'utilisateur en erreur sont variables, il peut s'agir d'une soi-disant menace pour la sécurité de son ordinateur ou d'une demande pour aider un tiers ou encore d'une invitation à regarder une vidéo. L'ingénierie sociale repose sur la crédulité de l'utilisateur et sa caractéristique est de le pousser à donner volontairement ses données.

- **Le phishing : ou hameçonnage**, est une technique visant à obtenir de l'internaute ses données personnelles (mots de passe, numéros de carte de crédit etc...). Le phishing utilise le spam et les vers de courrier afin d'entraîner l'internaute sur une fausse page web imitant celle d'un organisme officiel.
- **Trojan : ou Cheval de Troie**, est un programme qui s'exécute ou exécute des actions sur un ordinateur sans l'autorisation préalable de l'utilisateur. Cette action peut être non destructrice mais également causer des dommages significatifs à un système, si le Trojan télécharge un programme malveillant sur le poste, par exemple. Les Chevaux de Troie s'introduisent dans le système de façon erronée en se substituant à l'une des applications actives, teste ses fonctions ou en imite les performances et génère différentes actions malveillantes.
- **Spyware (logiciel espion)** : ce sont des Chevaux de Troie dangereux pour les utilisateurs. Ils sont destinés à suivre le système et à envoyer des informations à des tiers, créateur ou bénéficiaire du virus. Le logiciel espion s'intéresse aux pré-requis système, au type de navigateur, aux sites Internet visités et parfois au contenu des fichiers présents sur le disque dur de l'ordinateur. Ces logiciels sont chargés en secret sur l'ordinateur via un «freeware» ou bien lors du visionnage de pages HTML et de popup publicitaires. Ils s'installent sans informer l'utilisateur. Parmi les effets secondaires, témoins de la présence d'un logiciel espion sur l'ordinateur, on retiendra un fonctionnement instable du navigateur et le ralentissement du système.
- **Hoax ou « canular »** : est un message email qui véhicule une fausse information destinée à susciter une réaction chez son destinataire. En général, il est demandé à l'utilisateur de faire circuler massivement le message, ce qui accroît le trafic email et fait perdre du temps aux utilisateurs. Les hoax ne contiennent pas (forcément) de virus.
- **Backdoor** : ou « porte dérobée » est un programme permettant à un système autorisé d'accéder ou de recevoir des fonctionnalités spécifiques. Les backdoors sont souvent utilisées pour compromettre les paramètres de sécurité système. Les backdoors s'installent à l'insu de l'utilisateur et permettent aux pirates soit de prendre le contrôle de la machine à distance, soit de supprimer, copier, modifier des données.
- **Rootkit** : programme malveillant dissimulé dans le système.
- **Ver : worm** en anglais, est un programme parasite capable de s'auto propager. Il peut déployer des copies de lui-même mais n'affecte pas les autres programmes. Il est propagé par email (souvent sous la forme d'une pièce jointe) et envoie massivement ses propres copies à d'autres ordinateurs.
- **Keylogger** (littéralement : enregistreur de frappe) : est un type de logiciel de Troie qui a la particularité d'enregistrer les touches frappées sur le clavier afin de voler les mots de passe personnels et mots de passe réseau, les données des cartes de crédit et d'autres informations personnelles.
- **Attaques DOS**, ou attaques par déni de service : type d'attaque réseau assez courant qui consiste à envoyer un très grand nombre de requêtes à un serveur avec l'objectif de le faire tomber. Face à la quantité de requêtes, le serveur atteint ses limites et tombe en panne.
- **Dialers** : petites applications installées sur les ordinateurs, élaborées pour scanner un certain type de numéros de téléphone. Par la suite, les malfaiteurs utiliseront les numéros trouvés pour prélever des frais de leurs victime ou bien pour connecter l'utilisateur, via son accès, à des services téléphoniques surtaxés et coûteux.

Russie	Doctor Web, Ltd 12A/2, 3-ème rue Yamskogo polya, 125124, Moscou, Russie Téléphone : +7 (495) 789-45-87 Fax : +7 (495) 789-45-97 www.drweb.com www.av-desk.com www.freedrweb.com mobi.drweb.com
France	Doctor Web France Sarl 333b, Avenue de Colmar, 67100, Strasbourg Téléphone : +33 (0) 3 90 40 40 20 www.drweb.fr
Allemagne	Doctor Web Deutschland GmbH Allemagne, 63457, Hanau-Wolfgang, Rodenbacher Chaussee 6 Téléphone : +49 (6181) 9060-1210 Fax : +49 (6181) 9060-1212 www.drweb-av.de
Kazakhstan	SARL Doctor Web – Asie Centrale 165b/72g, rue Chevtchenko/rue Radostovtsa, office 910, 050009, Ville d'Almaty, Kazakhstan Téléphone : +7 (727) 323-62-30, 323-62-31, 323-62-32 www.drweb.kz
Ukraine	Centre de support technique Doctor Web 01001, Ukraine, Kiev, calle Kostelnaya, 4, oficina 3 Teléfono/Fax: +380 (44) 238-24-35, 279-77-70 www.drweb.ua
Japon	Doctor Web Pacific, Inc. NKF Kawasaki building 2F, 1-2, Higashida-cho, Kawasaki-ku, Kawasaki-shi, Kanagawa-ken 210-0005, Japan Tel: +81 (0) 44-201-7711 www.drweb.co.jp
Chine	Doctor Web Software Company (Tianjin), Ltd. 112, North software tower, N° 80, 4th Avenue, TEDA, Tianjin, China 天津市经济技术开发区第四大街80号软件大厦北楼112 Tel: +86-022-59823480 Fax: +86-022-59823480 E-mail: D.Liu@drweb.com www.drweb.com



© Doctor Web, 2003–2013

Doctor Web France

333b, Avenue de Colmar, 67100, Strasbourg

Téléphone : +33 (0) 3 90 40 40 20

www.drweb.fr | www.drweb.com | www.av-desk.com

www.freedrweb.com | mobi.drweb.com