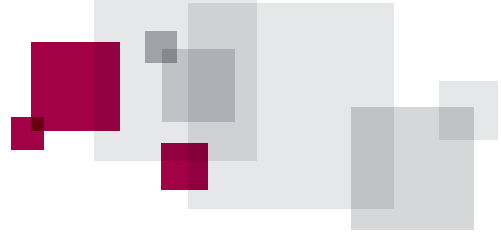




DOCUMENT TECHNIQUE

# RAPPORT DE SÉCURITÉ SUR LES MALWARES : PROTÉGER VOTRE ENTREPRISE, VOS CLIENTS ET VOS RÉSULTATS



## SOMMAIRE

1 LA PROLIFÉRATION GLOBALE DES MALWARES SUR LES SITES INTERNET

1 QU'EST-CE QU'UN MALWARE ?

2 UNE ATTAQUE DE MALWARE À LA LOUPE

3 MALWARE : UN BUSINESS MODEL BIEN FICELÉ

4 CONCLUSION

4 L'ENTREPRISE VERISIGN





# RAPPORT DE SÉCURITÉ SUR LES MALWARES : PROTÉGER VOTRE ENTREPRISE, VOS CLIENTS ET VOS RÉSULTATS

## LA PROLIFÉRATION GLOBALE DES MALWARES SUR LES SITES INTERNET

Ce document technique vous aidera à mieux cerner la menace que représentent les malwares et leur pouvoir de nuisance sur votre e-entreprise. Vous y découvrirez les motivations des spécialistes du malware et leurs méthodes d'infection des serveurs Web pour la propagation de ces programmes malveillants. Également au sommaire de ce document, les techniques permettant aux administrateurs de détecter quand et comment leur serveur Web a été piraté.

De nombreux autres aspects de la lutte anti-malware y sont également abordés :

- La propagation des malwares via les navigateurs plutôt que par des techniques classiques, comme les pièces jointes d'e-mail.
- Les motivations financières incitant les cybercriminels à infecter les systèmes informatiques des internautes.
- La façon dont les malwares se propagent à partir de sites légitimes infectés.
- Les outils développés pour infecter le plus grand nombre possible de pages
- Les techniques d'attaque mises au point par les cybercriminels pour exploiter les failles des sites et contaminer des milliers de sites Web simultanément.
- Les publicités frauduleuses utilisées par les pirates pour infecter les sites Internet les plus populaires, pourtant bien sécurisés.

## QU'EST-CE QU'UN MALWARE ?

« Malware » est un terme générique désignant un logiciel malveillant (contraction de l'anglais « malicious software »). Le fléau des malwares prend une ampleur grandissante sur Internet. Le principe consiste à exploiter les failles de sécurité de votre serveur Web pour y installer ces codes malveillants. Objectif : obtenir l'accès à votre site Internet. La sphère des malwares est vaste et comprend aussi bien les adwares, qui affichent des fenêtres publicitaires non désirées, que les chevaux de Troie (Trojan), grâce auxquels les pirates infiltrent un système pour dérober des informations confidentielles, notamment des coordonnées bancaires.

Les malwares se répandent de plus en plus via les navigateurs Internet. Cette stratégie s'est développée ces dernières années, à mesure que les filtres des messageries électroniques se renforçaient, empêchant les fraudeurs de propager leurs programmes malveillants par le biais des spams. En

outre, grâce à l'essor des pare-feux à domicile comme en entreprise, il est devenu plus difficile pour les malwares de se répandre d'un système à l'autre sur un même réseau. Malgré cela, Internet offre aux pirates de nombreuses possibilités d'infiltrer le site Web de votre entreprise et d'utiliser celui-ci pour contaminer vos clients.

Les codes malveillants ne sont pas faciles à détecter et peuvent infecter les systèmes des internautes lorsque ceux-ci naviguent sur votre site. On parle dans ce cas de malwares « drive by », dans la mesure où l'internaute qui passait par là se retrouve contaminé, sans en avoir conscience dans la plupart des cas. Et c'est bien là tout le problème. Les cybercriminels utilisent ces malwares insidieux pour propager des virus, pirater des ordinateurs ou subtiliser des données sensibles comme les numéros de cartes de crédit ou autres informations personnelles.

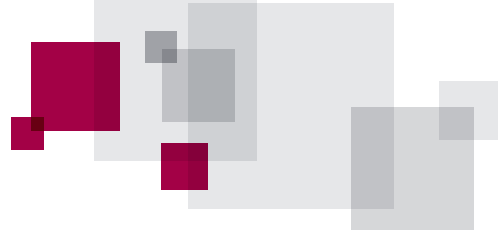
---

## Le modus operandi des malwares « drive by » et le risque pour les sites à faible fréquentation

Les malwares drive-by s'auto-téléchargent sur le système de l'utilisateur sans l'autorisation de ce dernier. Les pirates exploitent les failles du navigateur et/ou des plug-in pour distiller leurs programmes malveillants, en dissimulant ceux-ci comme élément invisible (ex. : balise iframe ou javascript crypté) au sein d'une page Web, ou bien en l'intégrant à une image (ex. : fichier flash ou PDF) pouvant être communiquée par le site à l'ordinateur, ce à l'insu de l'internaute.

N'importe quel site peut être touché. Les sites de plus petite envergure peuvent s'avérer plus vulnérables car ils ne possèdent souvent pas les ressources et l'expertise nécessaires pour détecter et contrer rapidement les attaques. Les malwares peuvent ainsi corrompre les ordinateurs de vos clients alors que ceux-ci se contentent de naviguer sur votre site. En ciblant les sites Web peu fréquentés, les professionnels de l'arnaque en ligne échappent plus longtemps aux détections et causent davantage de dégâts.





## UNE ATTAQUE DE MALWARE À LA LOUPE

Pour infecter un ordinateur par l'intermédiaire d'un navigateur Internet, le pirate procède en deux temps. Il doit d'abord trouver un moyen d'entrer en contact avec sa victime. Ensuite, il lui faut installer le malware sur le système de l'internaute. Selon la stratégie mise en place par le fraudeur, ces deux opérations peuvent être réalisées très rapidement et sans que l'utilisateur ne s'aperçoive de quoi que ce soit.

Pour forcer le navigateur de l'internaute à exécuter un code malveillant, le pirate informatique peut simplement demander à sa victime de visiter un site Web contaminé par un malware. Bien entendu, la plupart des victimes ne le feront pas en connaissance de cause. Le pirate doit donc s'efforcer de dissimuler la nature fallacieuse du site. Les fraudeurs avertis exploitent les toutes dernières techniques de diffusion et envoient souvent des messages infectés via des réseaux sociaux comme Facebook, ou par des systèmes de messagerie instantanée. Si ces méthodes ont obtenu un certain succès, elles reposent toujours sur le même principe : inciter l'internaute à visiter un site Web particulier.

D'autres cybercriminels choisissent de cibler des sites que les victimes visiteront de leur propre chef. Pour ce faire, le pirate corrompt le site en question en introduisant de courtes séquences de code HTML reliées à son serveur. Ce code peut être téléchargé depuis n'importe où, y compris depuis un site Web entièrement distinct. Chaque fois qu'un utilisateur visite un site Web compromis de la sorte, le code malveillant dispose d'une fenêtre de propagation du malware sur le système client.

---

### Techniques courantes de propagation d'un malware :

- **Mises à jour logicielles** : Par le truchement d'un média social, le malware invite l'internaute à visionner une vidéo. Après avoir cliqué sur le lien, l'utilisateur est prié de mettre son logiciel à jour pour pouvoir restituer la vidéo. Naturellement, la mise à jour proposée est un programme malveillant.
- **Bannières publicitaires** : La technique dite du « malvertising » incite des internautes incrédules à cliquer sur une bannière publicitaire qui tente alors d'installer un code malveillant sur le système client. Autre cas de figure : l'annonce redirige l'utilisateur vers un site Web le priant de télécharger un document PDF contenant un code malveillant extrêmement bien dissimulé. Variante : l'internaute est prié de communiquer ses données bancaires afin de télécharger correctement un document PDF.
- **Documents téléchargeables** : L'utilisateur est encouragé à ouvrir un fichier courant, tel que Microsoft Word ou Excel, recelant un cheval de Troie préalablement intégré.
- **Interception de données (Man-in-the-middle)** : Les utilisateurs pensent naviguer sur un site Web digne de confiance. En réalité, un cybercriminel intercepte les données que l'utilisateur transmet au site, comme son identifiant ou son mot de passe. Autre possibilité : un fraudeur détourne la session en cours et continue à utiliser alors que l'internaute pense l'avoir clôturée. Le malfaiteur peut alors se livrer à des transactions frauduleuses. Si l'utilisateur était en train de consulter ses comptes, le fraudeur peut réaliser des virements. Si la victime effectuait des achats en ligne, le pirate peut subtiliser le numéro de carte de crédit utilisé lors de la transaction.
- **Enregistreurs de frappes** : Via l'une des techniques précitées, l'internaute télécharge innocemment un programme d'enregistrement de frappes. Ce programme se concentre alors sur certaines actions spécifiques telles que les mouvements de la souris ou les saisies de clavier, effectuant des captures d'écran afin d'enregistrer les coordonnées bancaires ou les numéros de carte de crédit.



## MALWARE : UN BUSINESS MODÈLE BIEN FICELÉ

Comment les fraudeurs gagnent-ils leur vie grâce aux malwares ? Il existe plus d'une façon de faire de l'argent en exploitant des systèmes contaminés. L'une des plus simples est la publicité. À l'image de nombreux sites qui vivent des bannières publicitaires déployées pour des annonceurs, les malwares peuvent également afficher des publicités qui rémunèrent directement le cybercriminel.

L'autre moyen à disposition est celui de l'extorsion. Un réseau étendu d'ordinateurs corrompus peut représenter une puissance non négligeable. Certains pirates brandissent cette menace pour racketter les propriétaires de sites Internet. En lançant une attaque groupée à partir d'un pool de machines appelé « botnet », un seul et même pirate peut inonder le flux de trafic d'un site Internet jusqu'à saturation, provoquant ce qu'on appelle un déni de service (DoS). Le fraudeur contacte ensuite le propriétaire du site et lui réclame de l'argent pour mettre fin à son offensive.

Par ailleurs, les cybercriminels utilisent souvent des machines infectées pour recueillir des données personnelles précieuses telles que les références bancaires. Ce type de programme malveillant, désigné comme « infostealer » ou cheval de Troie bancaire, constitue l'une des formes de malware les plus sophistiquées et les plus insidieuses. Une fois en possession des données personnelles, les fraudeurs peuvent les utiliser pour leurs propres activités illicites, ou bien les revendre à des tiers aux intentions tout aussi malhonnêtes.

---

## La mise sur liste noire et l'importance d'y échapper

En raison des dégâts pouvant être causés par les malwares, Google, Yahoo, Bing et d'autres moteurs de recherche placent sur liste noire tout site Internet dont la contamination est avérée. Une fois que ces sites sont mis à l'index, les moteurs de recherche avertissent les internautes du risque qu'ils prennent en les visitant. Les sites incriminés peuvent même être purement et simplement radiés des résultats de la recherche.

Quelle que soit votre politique de référencement, la mise au ban de votre site pourrait avoir des conséquences dévastatrices sur votre activité. Le placement sur liste noire s'effectue le plus souvent sans préavis, à votre insu et il est extrêmement compliqué de faire machine arrière. C'est pourquoi la réussite à long terme de tout site Web passe par l'adoption de mesures ad hoc destinées à prévenir un tel désagrément.

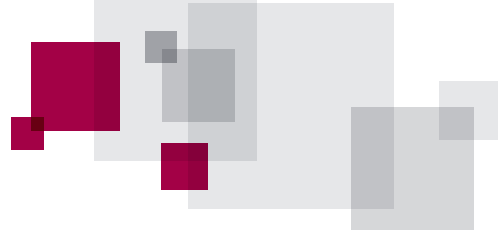
## VERISIGN, PIONNIER ET LEADER DE LA SÉCURITÉ EN LIGNE

Au milieu des années 1990, VeriSign fut la première entreprise à commercialiser une solution SSL. Leader incontesté du marché des certificats SSL, VeriSign incarne aujourd'hui la marque de confiance la plus connue et reconnue du Net. VeriSign doit cette réputation auprès du grand public et des professionnels de l'e-commerce à des années d'efforts incessants et à son engagement sans relâche à incorporer les toutes dernières technologies à ses solutions SSL.



Outre la sérénité que procure le choix d'un certificat SSL réputé, VeriSign continue de répondre aux besoins de ses clients en enrichissant constamment son cœur d'offre SSL de nouveaux standards et de technologies et solutions complémentaires. Fidèle à sa réputation, VeriSign traque désormais jour après jour les malwares sévissant sur les sites de ses clients SSL. L'objectif ? Garantir que votre site Internet, votre image de marque et les données confidentielles de vos clients demeurent à l'abri de cybermenaces en perpétuelle mutation.





## CONCLUSION

Les ventes de produits et de services en ligne ont connu une croissance extraordinaire lors des dix dernières années. Toutefois, l'usage grandissant d'Internet au quotidien entraîne dans son sillage un essor inquiétant de la fraude. Ainsi la propagation des malwares met en péril le développement du Web marchand en attisant les craintes d'usurpation d'identité. Ces appréhensions ont pour effet de tirer vers le bas le chiffre d'affaires des sites marchands. Pour exploiter pleinement son potentiel, le commerce en ligne doit se doter de moyens idoines pour contrer les malwares.

Pour accompagner la croissance de votre e-entreprise, VeriSign vous propose une gamme de solutions complètes associant des certificats SSL haut de gamme à des fonctionnalités anti-malware innovantes. Ainsi vos pages Web publiques font l'objet d'analyses régulières destinées à débusquer la présence d'éventuels malwares. Par le biais du sceau VeriSign, la marque de confiance la plus connue et reconnue au monde, VeriSign vous aide à rassurer vos clients lors de vos interactions et transactions en ligne. Pour une mise en confiance totale des internautes, faites appel aux certificats VeriSign SSL.

## L'ENTREPRISE VERISIGN

VeriSign est le fournisseur de services d'infrastructures Internet de confiance du monde en réseau. Chaque jour, l'infrastructure Internet VeriSign permet aux entreprises et aux particuliers de réaliser des milliards d'échanges et de transactions sécurisés à travers le monde.

**Pour plus d'informations, rendez-vous sur [www.Verisign.fr](http://www.Verisign.fr).**

