Drive-By Download : infecter les ordinateurs par le WEB

Le Drive-By Download désigne une méthode pour infecter les internautes par le WEB.
Cette méthode n'est pas forcément bien connu et pourtant elle fut très utilisée par le passé.
Encore aujourd'hui, elle reste assez présente même si les navigateurs WEB apporte beaucoup de protections.

Cet article vous donne toutes les explications autour du Drive-By Download.

Qu’est-ce que Drive-By Download ?

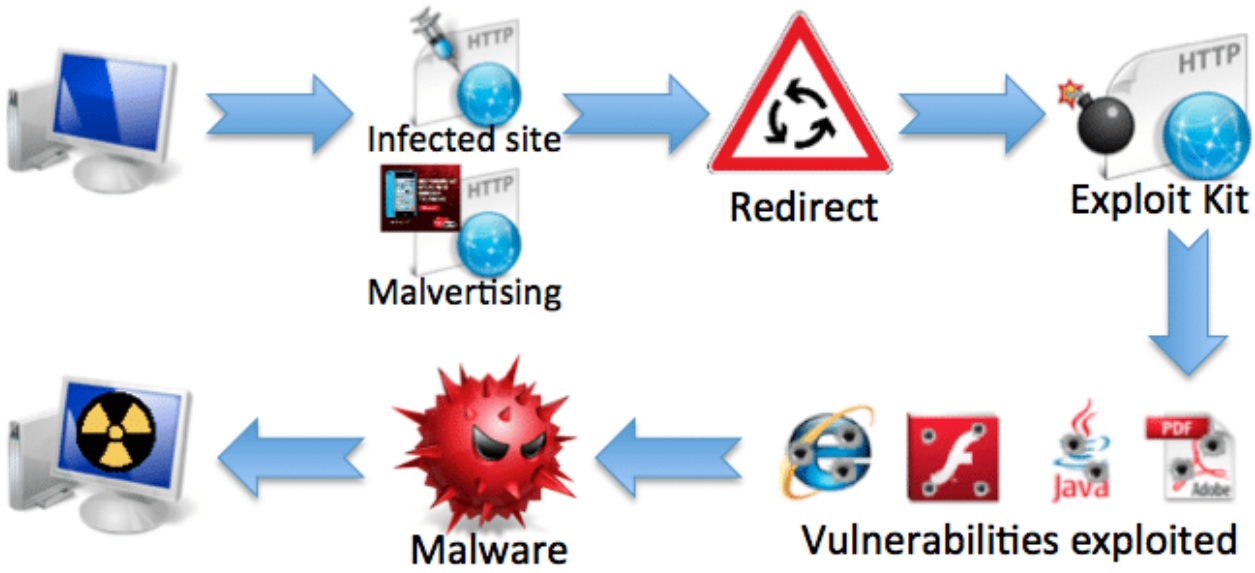
Le principe n’est pas très difficile à comprendre.
Il s’agit d’installer un malware sur un PC par la simple visite d’une page WEB.
L’attaque tire partie de la présence de plugin ou logiciels non à jour et ayant des vulnérabilités.
L’exploit se charge de manière automatique et permet de télécharger et exécuter un malware.

Pour ce faire, les cybercriminels utilise un Exploit Kit.
Il s’agit d’un logiciel capable de regrouper plusieurs exploits.
Les auteurs mettent constamment à jour le Web Exploitkit afin de contourner les défenses antivirus.
Enfin lorsqu’une vulnérabilité est publiée, l’exploit est intégré dans le logiciel.

Le schéma ci-dessous explique le principe.

- L’internaute visite une page WEB.
- Celle-ci contient un code (souvent Javascript) ou une publicité malveillante (malvertising) qui va rediriger et charger le Exploit Kit
- Ce dernier teste des exploits. Si le PC possède des versions de logiciels vulnérables alors le malware se charge.

Tout se ceci se fait sans aucun clic et de manière automatique.



Source : Malwarebytes

Enfin voici une vidéo qui montre un WebExploit Kit en action. Ce dernier charge un malware par la simple visite d'un site WEB.

ou encore :

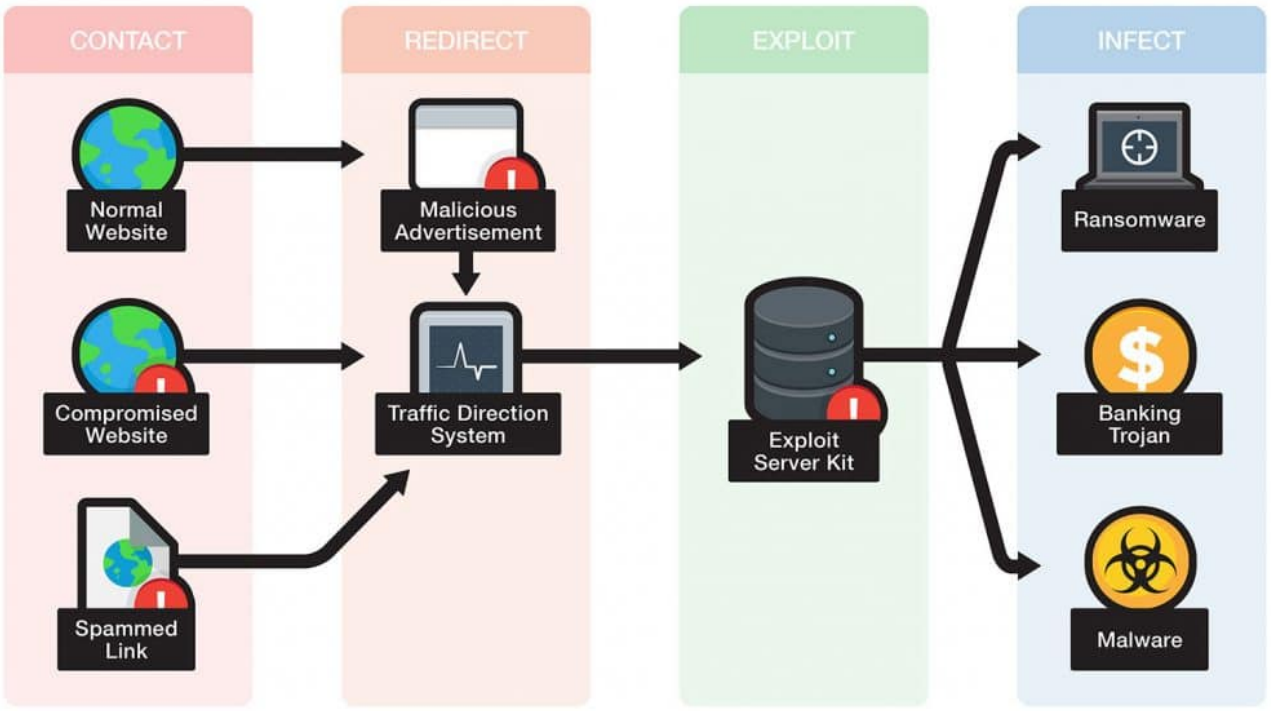
Les attaques par Drive-By Download

Pour infecter un maximum d'internautes, il faut donc charger le WebExploit Kit.
Pour ce faire, les cybercriminels utilisent plusieurs méthodes.

- **Pirater les sites WEB** : Ils tentent d'accéder à un site WEB afin d'en modifier les pages WEB. En général, cela

vise à insérer le code de redirection.

- **Les Malvertising** : Ce sont des publicités malveillantes. Ils proposent des publicités malveillantes à des régies publicitaires. Si la régie ne voit rien, la publicité est mise en ligne et diffusée. Les internautes vont alors être redirigé.
- **Redirections malveillantes lors des recherches Google** : Des sites bidons avec des mots clés sont mis en ligne. Le but est de les retrouver dans les recherche Google. L'internaute clic sur le lien et charge alors l'Exploit Kit Web.



source Trend-Micro

Bien entendu, on peut combiner les méthodes.
Par exemple pirater des sites WEB tout en proposant des malvertising.
En Décembre 2015, la source la plus importante reste les publicités malveillantes.

	From Malvertising	From Other Sources
Angler Exploit Kit	89.32%	10.68%
Magnitude Exploit Kit	100%	0%
Neutrino Exploit Kit	39.80%	60.20%
Rig Exploit Kit	85.93%	14.07%
Nuclear Exploit Kit	33.81%	66.19%
Sundown Exploit Kit	100%	0%
Total	88.07%	11.93%

Table 4. Distribution of exploit kit traffic by source (December 2015)

source
https://blog.trendmicro.com/trendlabs-security-intelligence/exploit-kits-2015-flash-bugs-compromised-sites-malvertising-dominate/

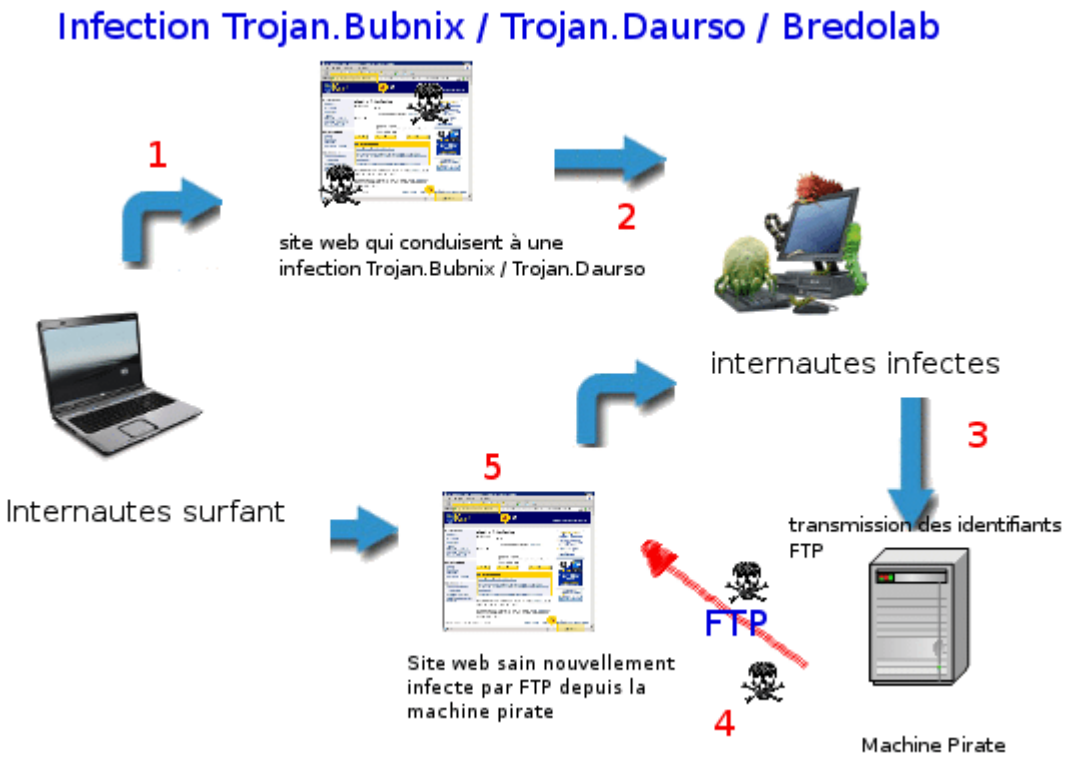
Piratage de sites internet

Afin d'augmenter le trafic de l'attaque, les cybercriminels piratent des sites WEB.
Ainsi les pirates visent les CSM comme WordPress ou Joomla.
En effet, des millions de sites internautes utilisent ces derniers.
Or, lors de la publication de vulnérabilité sur le CSM ou sur un plugin, des attaques automatisées suivent.
Les pages des sites WEB sont alors modifier afin d'injecter du code pour rediriger les internautes.

Autour de 2011, des malwares ont aussi vu le jour pour pirater les sites WEB depuis les PC des webmaster.
Le but était de récupérer les identifiants FTP.
Les articles suivants en parlent :

- Intrusions sur sites internet par vols d’identifiants FTP
- PSW.Win32.Tepfer – vol FTP et injection/hack de sites

Voici un schéma qui récapitule les attaques du Trojan.Bubnix.



Les malvertising

Plus tard, les cybercriminels misent sur les publicités malveillantes.
Il s’agit de mettre en ligne des publicités qui vont permettre de charger l’Exploit Kit.
Les régies publicitaires œuvrant sur les sites pornographiques, cracks, ou de streaming illégaux ont été très visés.
La page suivant évoque quelques campagnes.

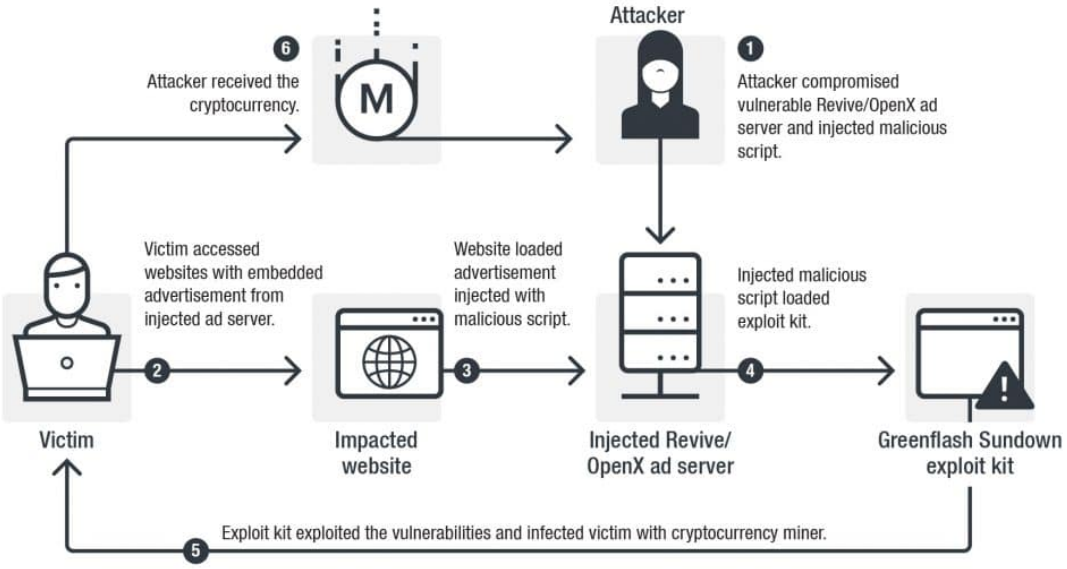
Les publicités malicieuses « Malvertising », source de distribution des virus

Cette méthode a permis d'infecter des milliers d'internautes de part le monde.

A noter qu'on a pu aussi assister à des piratages de régies publicitaires :

- Exemple d'une Malvertising sur OpenX
- [en] OpenX Hacks example (malvertising)

Par exemple les campagnes ShadowGate (WordsJS) piratent des serveurs Revive et OpenX.
Ces derniers permettent de distribuer des publicités.
Ainsi les pirates ciblent les serveurs des régies publicitaires mal sécurisés.



source : Trend-Micro

Les campagnes de Drive-By Download

Les premiers ExploitKit ont vu le jour en 2006.

Mais les attaques par Drive-By-Download massives ont commencé de manière très importantes en 2010.
En effet, c'est à cette époque que les malvertising sur des sites de streaming furent utilisés massivement.
Ces méthodes ont vu la combinaison de plusieurs phénomènes :

La poussée de Web ExploitKit très performant comme BlackHole.
On en parle sur la page : BlackHole Exploit WebKit : Présentation
Beaucoup de groupes ont utilisés ce dernier pour pousser des trojans.
Mais cela a aussi permit l'arrivé de ransomware de type Winlocker : les virus gendarmerie et police.

En 2018 , un cybercriminel très actif pour pousser des malvertising vers 2013 a été condamné.
Notamment pour pousser le ransomware Reveton.

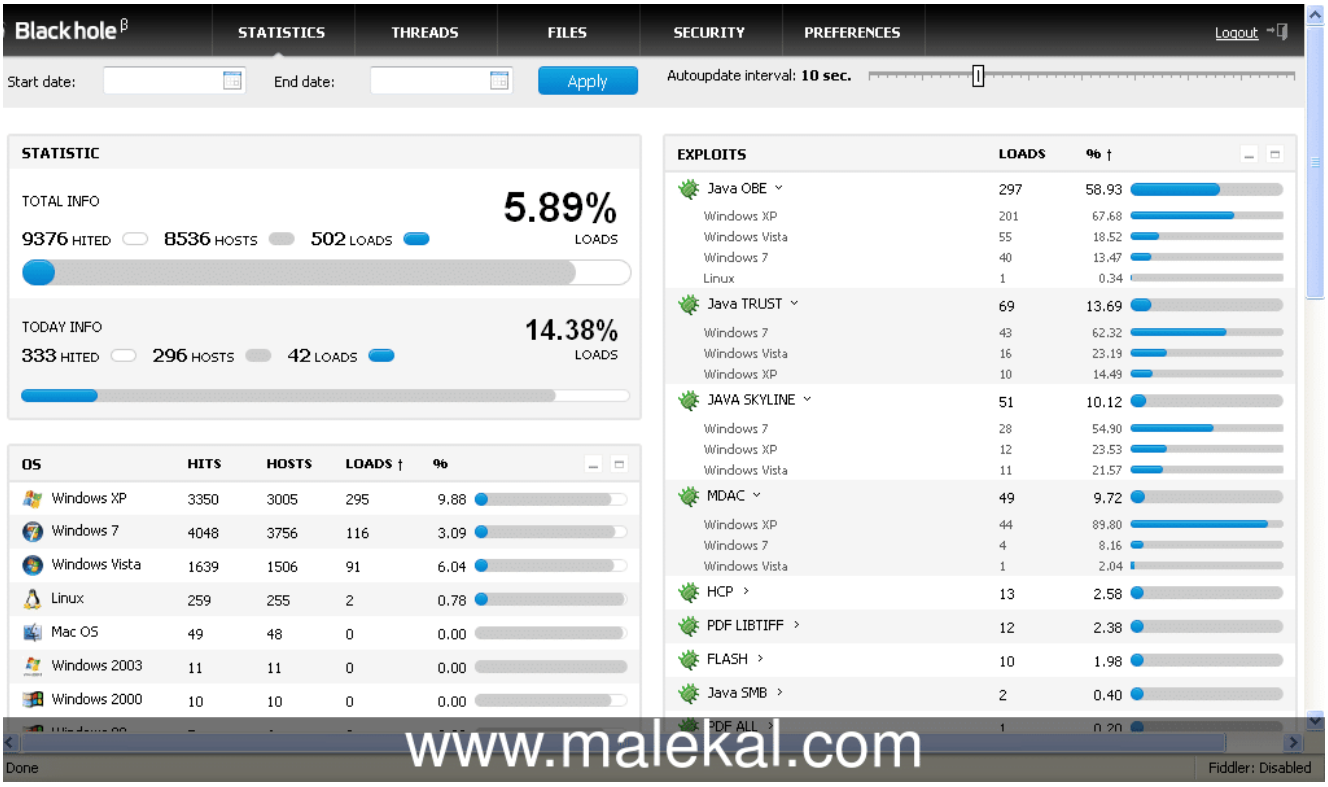
> *Arrestation d'un cybercriminel lié à des malvertising et virus police*

Le phénomène reste encore assez important.

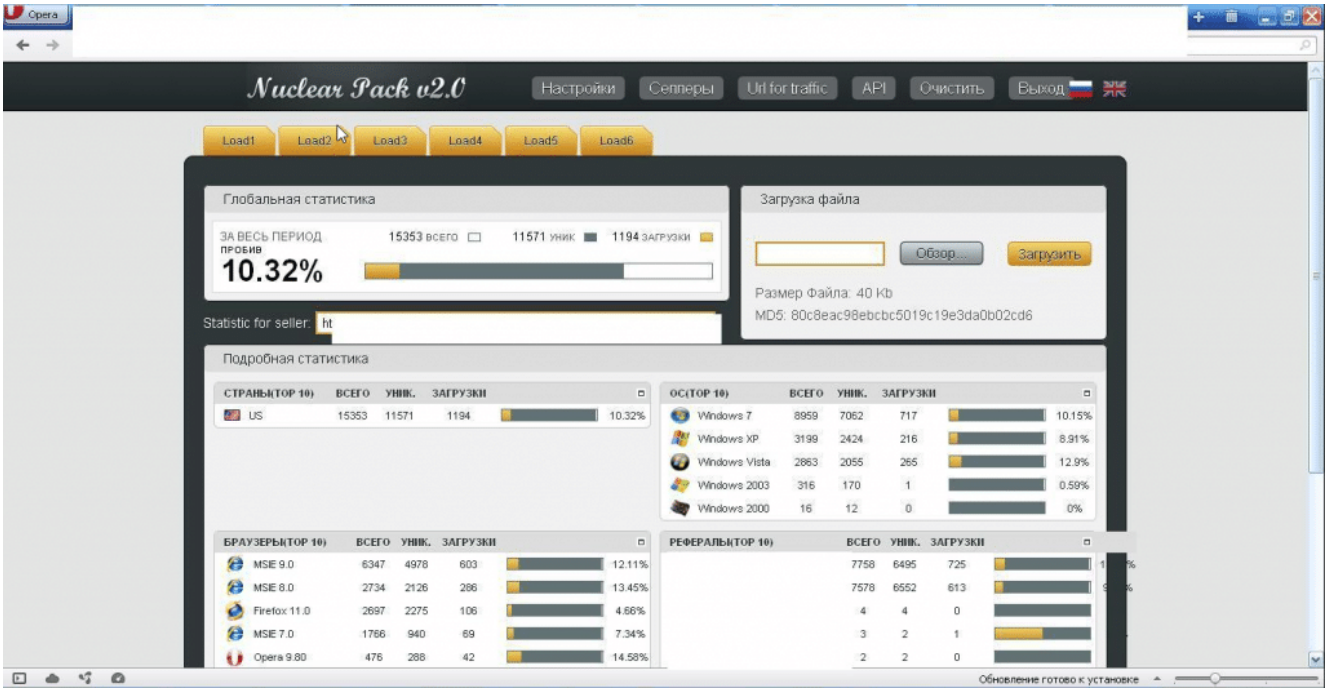
Quelques Web ExploitKit

Il existe tout un business autour des Web ExploitKit.
En effet, des groupes peuvent vendre ces logiciels ou les proposer en SaS.
Ainsi, un groupe peut les utiliser dans des campagnes pour pousser un trojan vendu ou sous-loué par un autre groupe.

Ces derniers possèdent un site de gestion.
Sur ce dernier des statistiques sont donnés.
Par exemple le taux d'infection, la version de Windows la plus touchées, les vulnérabilités qui fonctionne le mieux, etc.



Le panneau de getstion de Nuclear Pack 2.0 :



Comme souvent, il y a eu un âge d'or et divers WebExploitKit se sont concurrencés.
Par la suite certains sont morts et d'autres ont perduré.

Les WebExploit Kit les plus importants :

- BlackHole : A partir de 2010. Un des plus utilisés en 2014 et les plus performants.
- Angler EK apparu après la mort de BlackHole en 2015.
- Magnitude EK (PopAds) actif depuis 2014 et c'est le seul encore actif.
- Neutrino en 2014 et 2015
- Nuclear Exploit Kit (Nuclear EK) très actif à partir de 2016 et utilisé pour pousser le ransomware Cryptowall
- RIG EK actif à partir de 2014 pour pousser des ransomwares comme Locky, CryptoMix, Cryptosheild, Spora et Cerber. Mort en 2016.

Les Web Exploit Kit plus minimum :

- Fiesta (2008 à 2014)
- FlashPack (2014)
- HanJuan (2014)
- Sundown (2014 et 2015)
- Sweet Orange (2014)

Les WebExploit Kit encore actifs en 2019 :

- Lord EK
- Spelevo EK
- Fallout EK
- Magnitude EK
- RIG EK
- Underminer EK
- Router EK

Les défenses contre le Drive-By Download

Les antivirus

Les éditeurs d'antivirus ne pas changé grand chose du point de vue des protections.
En effet, ces derniers possédaient déjà un **module d'analyse WEB**.
Ce dernier permet d'analyser le contenu des pages WEB et jouter sur des listes noires.
Ils peuvent donc bloquer le chargement de la page WEB.

Au quotidien, des détections sur les codes de redirections s'ajoutent.
Comme des détections de type **JS/Redir**.
Mais les cybercriminels utilisent beaucoup de stratagème pour les contourner.

Les navigateurs WEB

Des milliers ont été infectés par ces méthodes avant que les éditeurs de navigateurs WEB (Mozilla, Google et Microsoft) prennent des mesures comme :

- B**loquer les plugins non à jour** et possédant des vulnérabilités.
    - En 2011, j'avais publié la page : Java Exploit en augmentation
    - Vous avez sur cette page les principales bulletins de sécurité d'Adobe Flash : Vulnérabilités sur Player Flash et Shockwave Player
- **Certains éditeurs ont abandonné des logiciels**. Par exemple Adobe Reader utilisait pour lire les PDF a été remplacé par des plugins natifs. De même chose pour Adobe Flash. L'éditeur contrôle ainsi ces plugins (blocage, mise à jour).
- **HTML5** change pas mal la donne rendant certains plugins obsolètes (Flash pour les vidéos en streaming).
- **Plus des arrestations**. Certains WebExploit Kit ayant une certaine notoriété sont morts, comme par exemple, Angler ExploitKit.

Conclusion

Les attaques Drive-ByDownload est une méthode qui a connu son apogée en 2014.
Depuis des mesures ont été prises par les navigateurs WEB pour les limiter.
De plus, les régies publicitaires tentent aussi de limiter la portée des malvertising.

C'est aussi pour cela que début 2015, les pirates sont revenus à des campagnes de mails vérolés.
Pour connaître toutes les méthodes pour infecter les internautes, suivre cet article :

> *Les Virus et Trojan – comment les internautes se font infecter*

Pour aller plus loin dans la sécurité, vous pouvez lire les autres pages du site consacrées à la sécurité : Virus/Sécurité
Pour sécuriser Windows : Comment Sécuriser son Windows