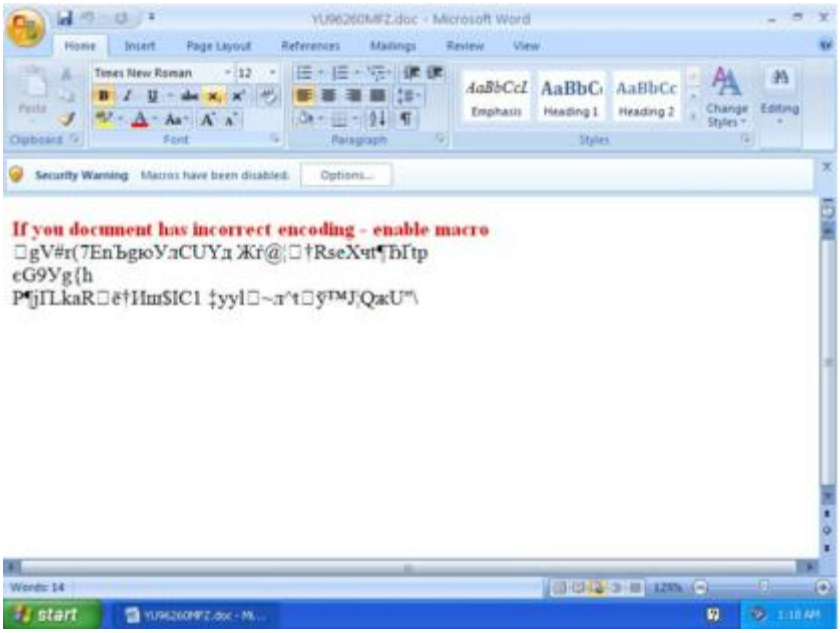
Lettre n°44 - novembre 2015 - disponible sur omc.ceis.eu

"Beginning Sunday, November 29, the government is prohibited from collecting telephone metadata records in bulk under Section 215, including of both U.S. and non-U.S. persons. And, while under the prior program NSA collected metadata in bulk and sought court approval for individual queries, the USA FREEDOM Act requires that the government must now base any application for telephone metadata records under FISA on a "specific selection term"—a term that specifically identifies a person, account, address, or personal device in a way that limits the scope of information sought to the greatest extent reasonably practicable" ***Déclaration de James R. Clapper, directeur du renseignement nationale des Etats Unis le 27 novembre 2015***

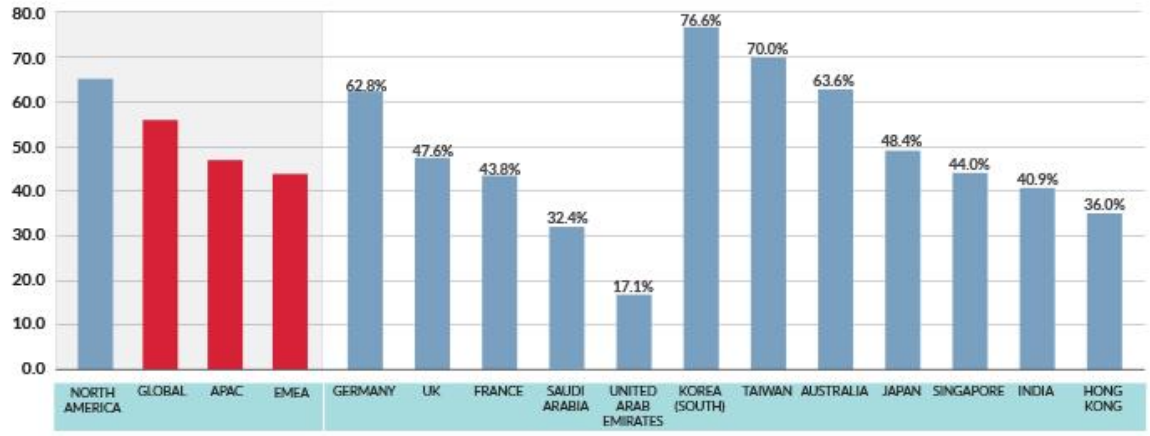
Table des matières

L'INSAISISSABLE TROJAN BANCAIRE DRIDEX



Capture d'écran d'un fichier Word contaminé - Source gdata.fr

En juillet 2014, la société de sécurité TrendMicro découvre un trojan bancaire, qu'ils nomment Dridex. C'est une évolution des malwares Cridex, Bugat, Geodo ou encore Feodo. Repéré dans au moins 26 pays, ce malware de type cheval de Troie s'installe sur les ordinateurs Windows à travers une pièce jointe piégée, un document Microsoft Office. Ce dernier contient des macros VBA malveillantes qui ont pour objectif d'infecter la victime avec Dridex, afin de récupérer les coordonnées bancaires à l'aide des différents outils présents dans le malware (logiciel espion, keylogger, etc.). Le document Office n'affiche aucun contenu lisible à part une invitation à activer les macros dans le document. Dridex utilise ainsi une méthode de propagation assez simple et ancienne qui fut populaire dans les années 90 : inclure des logiciels malveillants au sein de fichiers Word ou Excel.

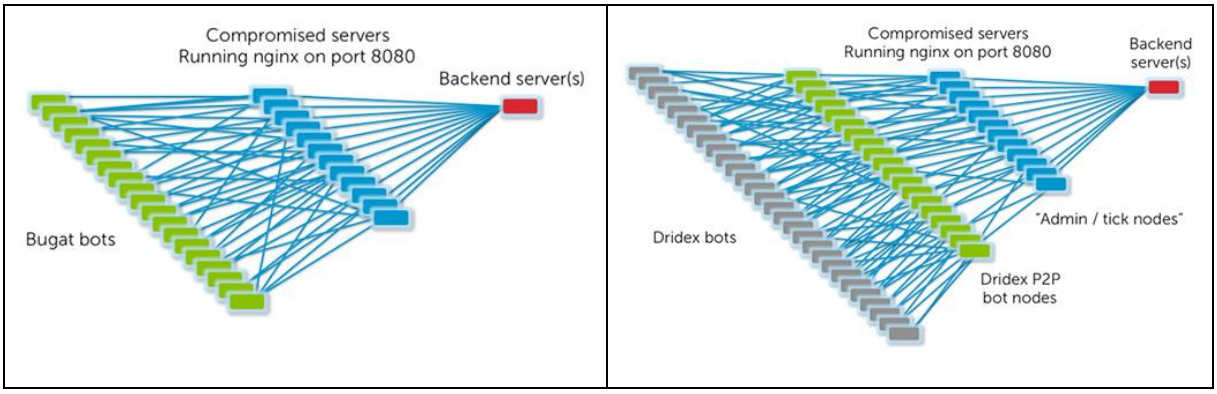


Taux d'expositions des différentes régions à Dridex.
Le taux est calculé par le nombre de clients de FireEye affectés par Dridex dans une région, divisé par le nombre de client dans la région – Source FireEye

Un malware assez innovant

Ce malware utilise des méthodes peu classiques, ce qui pourrait expliquer pourquoi il est autant virulent, et difficile à arrêter. Le CERT-FR a même réalisé plusieurs alertes sur Dridex[1] afin de sensibiliser les entreprises à la menace.

Tout d'abord, Dridex utilise une architecture P2P, héritée du célèbre réseau de zombies *Gameover Zeus*.



A gauche : architecture centralisée de Bugat ; A droite : architecture P2P de Dridex – Source : Secure Works

On peut voir à gauche ci-dessus, l'architecture de Bugat, un des prédécesseurs de Dridex, utilisant une architecture centralisée pour les communications avec le serveur de *Command and Control* (C&C). Les serveurs compromis de Bugat agissent en proxy vers les serveurs *back-end* (en rouge sur le schéma). Chaque malware Bugat comprend un ensemble de serveurs C&C, codées en dur.

Pour l'architecture P2P, présentée ci-dessus à droite, une couche supplémentaire apparait : les bots nœuds P2P (*P2P bot nodes*), en vert sur le schéma. Cette couche est construite par les machines infectées par Dridex qui peuvent se connecter directement sur un port Internet testé par le malware. Ces nœuds sont utilisés comme proxy HTTP entre les machines zombies (en gris sur le schéma) et le *front-end* du C&C (en bleu sur le schéma). Il semblerait que la fonction principale de cette nouvelle couche de nœuds augmente la difficulté de filtrer le trafic sortant pour les sociétés du fait des différentes adresses IP utilisées par le malware. Cette architecture offre ainsi une meilleure résistance aux actions des autorités qui visent à faire cesser ces réseaux de botnet.

Ensuite, Dridex utilise le site communautaire Pastbin.com (en majeure partie) pour charger le script Visual Basic du fichier Office corrompu. Ce site internet est un service gratuit dans lequel il est possible de stocker du texte pour une période définie et de partager ce dernier grâce à un lien vers ce site. Il est fréquemment utilisé par les développeurs pour partager des codes sources par exemple, ou pour stocker temporairement des informations. Ainsi, l'utilisation de ce site est tout à fait légitime au sein d'une organisation et il est peu probable que les solutions de sécurité l'inscrivent dans une liste noire.

[1] http://www.cert.ssi.gouv.fr/site/CERTFR-2015-ACT-024/CERTFR-2015-ACT-024.html

Enfin, Dridex fonctionne sur un modèle d'affiliation : le botnet est divisé en sous-réseaux de botnet. Il en existerait 13 selon Secure Works[2] mais les plus actifs seraient les botnets 120, 200 et 220. En avril 2015[3], le botnet Dridex-120 aurait 5850 bots, le botnet Dridex-200 750 bots et le botnet Dridex-220 9650 bots.

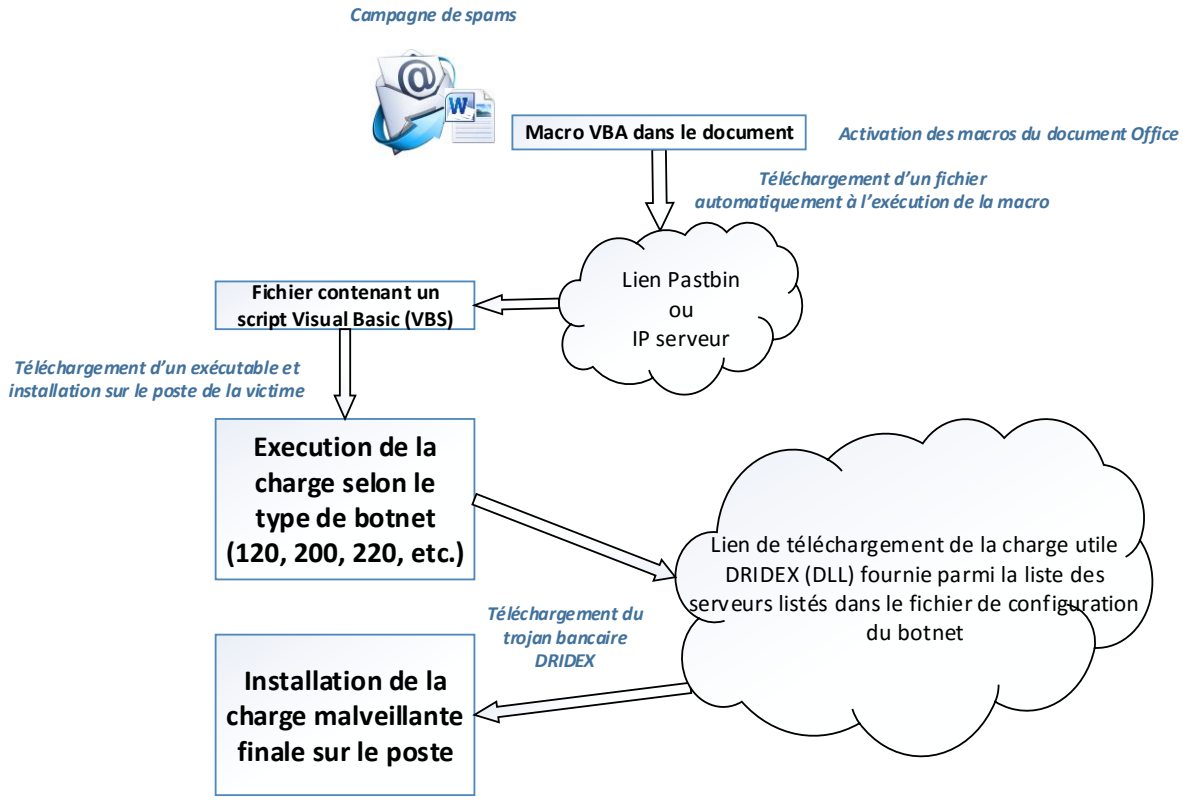


Schéma de fonctionnement de Dridex - Source: CEIS

Suite à son installation, le trojan bancaire Dridex offre plusieurs fonctionnalités sur le système de la victime :

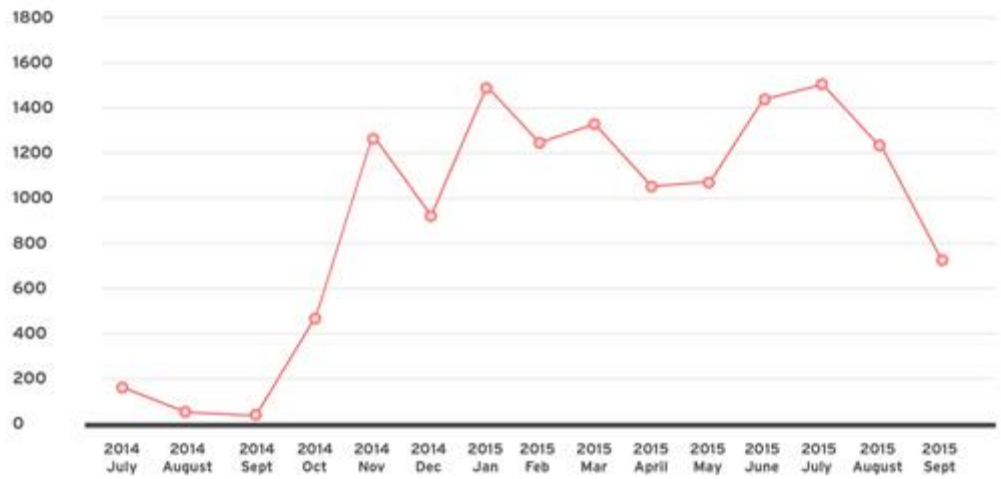
- Devenir un nouveau nœud P2P, afin d'agrandir l'architecture P2P de Dridex. Cette fonctionnalité dépendra de la possibilité au malware d'ouvrir des ports sur la machine ;

- Récupérer les données personnelles et bancaires de la victime puis effectuer des opérations frauduleuses. L'application cible explicitement des banques via des modules de contournement : à chaque clic sur le clavier virtuel de la banque, une capture d'écran est réalisée afin de pouvoir voler le mot de passe[4]. D'après le FBI[5], en octobre 2015, Dridex aurait permis de voler plus de 10 millions de dollars rien que sur les comptes bancaires américains : 999 000 dollars auraient été dérobés sur le compte d'une école municipale. L'entreprise Penneco Oil, quant à elle, a perdu plus de 3,5 millions de dollars, à la suite de trois transferts frauduleux. L'argent a été transféré vers des établissements bancaires situés en Ukraine, en Russie ou en Biélorussie.

[2] http://www.secureworks.com/cyber-threat-intelligence/threats/dridex-bugat-v5-botnet-takeover-operation/
[3] https://cdn2.hubspot.net/hubfs/507516/ANB_MIR_Dridex_PRv7_final.pdf
[4] https://www.lexsi.com/securityhub/comment-dridex-stocke-sa-configuration-en-registre/
[5] http://www.justice.gov/opa/pr/bugat-botnet-administrator-arrested-and-malware-disabled

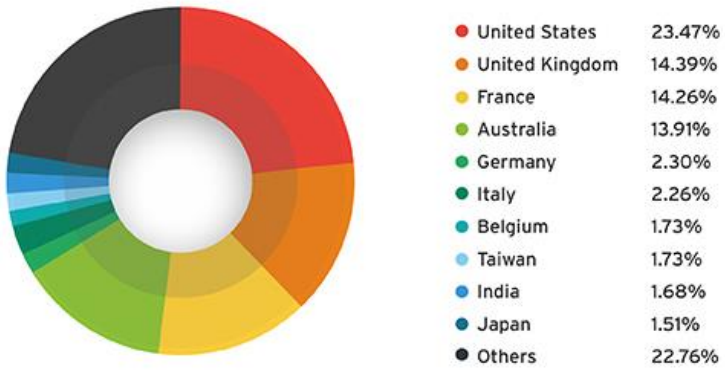
Dridex l'immortel ?

Le 28 aout 2015 en Chypre, une opération internationale coordonnée par le FBI et Europol (E3C) ont abouti à l'arrestation du moldave Andreï Ghinkul, dit « Smilex », principal administrateur de Dridex[6]. Avec l'aide de différentes sociétés de sécurité informatique, les autorités ont réussi à freiner les attaques du malware. Avec l'architecture de ce dernier, ses fichiers sont distribués de manière centralisée par les serveurs C&C. La saisie de ces serveurs principaux par les autorités a donc permis de réduire fortement les attaques de Dridex en redirigeant les flux des serveurs de commande de Dridex, identifiés pendant l'enquête (technique du *DNS sinkhole*). Les envois des spams ont été stoppés fortement le 2 septembre, quelques jours après l'arrestation du pirate, comme montré ci-dessous.



Détection de Dridex de juillet 2014 à septembre 2015 – Source : TrendMicro

Malheureusement, selon TrendMicro, Dridex semble être réapparu depuis novembre 2015, en visant plus particulièrement les Etats-Unis, le Royaume Uni, l'Australie et la France.



Répartition des victimes de Dridex du 13 octobre au 23 novembre 2015 – Source : TrendMicro

[6] https://www.fbi.gov/pittsburgh/press-releases/2015/bugat-botnet-administrator-arrested-and-malware-disabled

Les botnets sont en effet difficile à éradiquer : même si les réseaux utilisés par les cybercriminels sont mis hors ligne, de nouvelles infrastructures peuvent être reproduites ailleurs dans l'objectif de compromettre de nouveau les systèmes. De plus, Andreï Ghinkul appartiendrait, selon les chercheurs de Fox-IT[7], au groupe de pirates EvilCorp (connu pour le célèbre botnet *Gameover Zeus*). Il leur serait donc facile de répliquer le même type de cyberattaques.

Dridex est un bon exemple de la manière dont les menaces informatiques s'adaptent et évoluent. Malgré les revers subis par les pirates à la suite à des arrestations ou de difficultés opérationnelles, les cybercriminels, en particulier ceux qui disposent d'une certaine assise comme le groupe EvilCorp, continueront à être de véritables menaces. Même si certains membres clés du groupe de pirates administrant Dridex ont été arrêtés, l'organisation qu'ils laissent derrière eux reste viable. Il suffit alors à d'autres individus du groupe de s'associer et de redémarrer leur activité criminelle.

[7] http://www.forbes.com/sites/thomasbrewster/2015/10/13/dridex-botnet-takedown/

QUELS MOYENS DE PROTECTION CONTRE LES ATTAQUES DDOS ?

Le troisième trimestre de l'année 2015 fut marqué, selon un rapport[8] de Kaspersky Lab, par une attaque DDoS en continu d'une durée de 320 heures, c'est-à-dire deux semaines entières.

Les attaques par déni de service distribué (*Distributed Denial of Service ou DDoS*) sont l'un des types d'attaques les plus simples à mettre en œuvre et représentent donc une part croissante des types d'attaques détectées. Le terme désigne l'action d'un assaillant qui « tente d'épuiser les ressources disponibles d'un réseau, d'une application ou d'un service de manière à ce que les utilisateurs légitimes ne puissent y accéder »[9]. L'attaque vise littéralement la saturation afin de rendre un serveur, voir un système d'information inopérant.

Pour cela l'assaillant peut exploiter une vulnérabilité logicielle ou matérielle (dû le plus souvent aux faiblesses d'implémentation de certaines piles TCP/IP), mais aussi saturer la bande passante du réseau et ainsi infliger des pertes financières importantes, sans oublier l'impact en termes d'image et de marque pour l'organisation affectée[10].

Ce type d'attaques prend souvent la forme de séries d'assauts qui porte sur de grands volumes et qui s'accompagne d'attaques plus difficiles à détecter visant les applications et les infrastructures de sécurité que sont notamment les pare-feu et systèmes de prévention d'intrusion (IPS).[11]

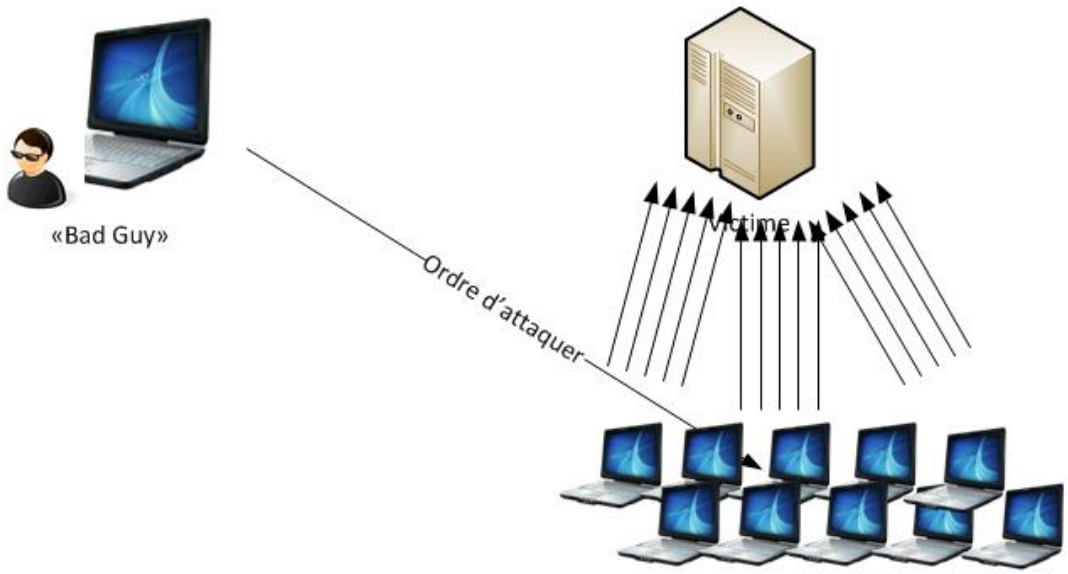
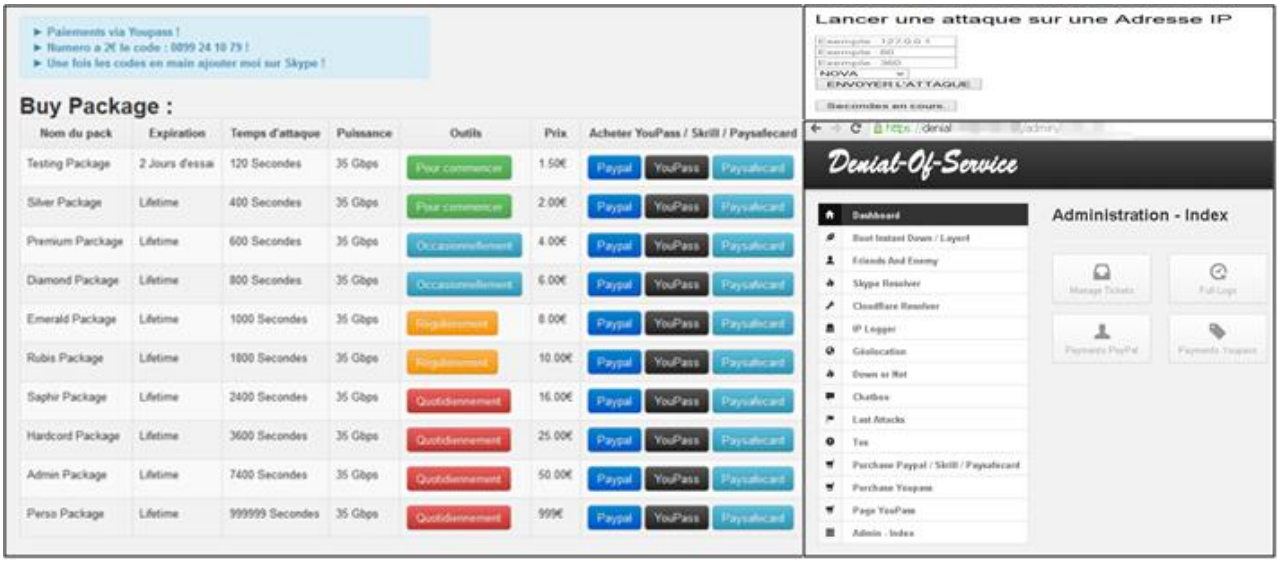


Schéma d'une attaque de type DDoS – Source : E-xpertsolutions

[8] http://www.viruslist.com/fr/analysis?pubid=200676402
[9] http://fr.arbornetworks.com/protection-ddos/
[10] « Comprendre et anticiper les attaques DDoS », rapport de l'ANSSI, consultable en ligne : http://www.ssi.gouv.fr/guide/comprendre-et-anticiper-les-attaques-ddos/
[11] Ibidem.

Alors que ces attaques sont en augmentation, les entreprises n'ont cependant pas toutes pris la mesure de la menace qu'elles représentent. Une étude de Kaspersky Lab et B2B Internationale démontrait que 20% des entreprises estimaient que c'était à leur prestataire informatique (en particulier son opérateur réseau) de protéger ses services en ligne contre les attaques de type DDoS, alors que la responsabilité relève bien des entreprises.[12]

Alors qu'aucune entreprise, aussi bien privée que publique, n'est à l'abri d'une attaque en déni de distribution de service, la question des moyens de protection à mettre en place est en effet délicate. Notamment parce que l'une des problématiques majeures des attaques DDoS est qu'il existe un véritable marché de location et d'achat de botnets, facile d'accès et proposant des prix très bas, permettant à tout un chacun d'acquérir pour une durée définie, une attaque par déni de service. En témoigne ces captures d'écrans :



Exemple de sites permettant d'acheter une attaque DDoS – Source CEIS

Des attaques DDoS multi-formes.

L'attaque DDoS est une variante de l'attaque DoS (*Denial of Service*), qui n'a, elle, qu'un seul point de départ, contrairement à une attaque DDoS qui provient d'une multitude de machines différentes (ordinateurs ou serveurs).[13] Ces attaques utilisent des botnets, ou réseaux de machines infectées (*machine zombie*) par un logiciel malveillant qui sont contrôlés à l'insu du propriétaire, utilisés souvent à des fins malveillantes[14]. Les botnets peuvent cependant fonctionner sur la base du volontariat. Ces « *voluntary botnet* »[15] désignent alors l'activation volontaire de machines infectées par leur propriétaire. Lors du conflit en Ukraine, des pirates russes ont ainsi encouragés les sympathisants à la cause russe à installer un malware sur leur machine afin de se connecter au botnet Kelihos[16]. Mais le plus souvent, le logiciel malveillant agit à l'insu du propriétaire de la machine.

[12] http://www.economiematin.fr/news-securite-informatiques-entreprises-attaques-ddos
[13] https://www.nbs-system.com/blog/ddos-dos.html
[14] Frédérick Douzet, « La géopolitique pour comprendre le cyberespace », Hérodote, 2014/1 n°152-153, p.9.
[15] https://www.nbs-system.com/blog/ddos-dos.html
[16] http://www.scmagazine.com/hackers-deliver-kelihos-to-users-sympathetic-to-russian-cause/article/368322/

Ces attaques prennent différentes formes, d'autant plus qu'il existe une multitude de vecteurs d'attaques, c'est-à-dire de moyens d'exécution, qui sont tous regroupés via une classification découpée en 3 grandes catégories[17].

- Les attaques DDoS réseau ou attaques volumétriques : elles s'attaquent à la bande passante en saturant la capacité réseau du serveur, le rendant ainsi injoignable.

- Les attaques sur les ressources provoquant un état d'épuisement TCP : elles s'attaquent aux ressources du système en les épuisant, empêchant ainsi la machine de répondre aux requêtes légitimes. Ces attaques asphyxient les tables d'état de connexion.

- Les attaques visant la couche applicative : elles ciblent une faille logicielle particulière afin de rendre une machine indisponible, ou d'en prendre le contrôle. Ces attaques sont les plus dangereuses puisqu'il suffit d'une seule machine d'assaut, même avec un débit lent pour causer d'importants dégâts. Cette catégorie d'attaque est la plus utilisée à l'heure actuelle, notamment via des attaques par débordement de la couche applicative (débordement HTTP GET, etc.).

L'une des pratiques les plus courantes est l'attaque DDoS par réflexion (DrDoS) ou rebond qui met en jeu trois types d'acteurs : un attaquant, une cible et des serveurs qui deviennent complices malgré eux. Ce type d'attaque utilise une technique d'usurpation d'adresse IP. Les attaques proviennent alors de machines dont l'adresse IP a été usurpée par l'assaillant. Pour exemple, le schéma ci-dessous présente l'envoi d'une requête ping à un grand nombre de serveurs sur Internet, en remplaçant son IP source par celle de la future victime, de sorte que ce soit la victime qui reçoive toutes les réponses.

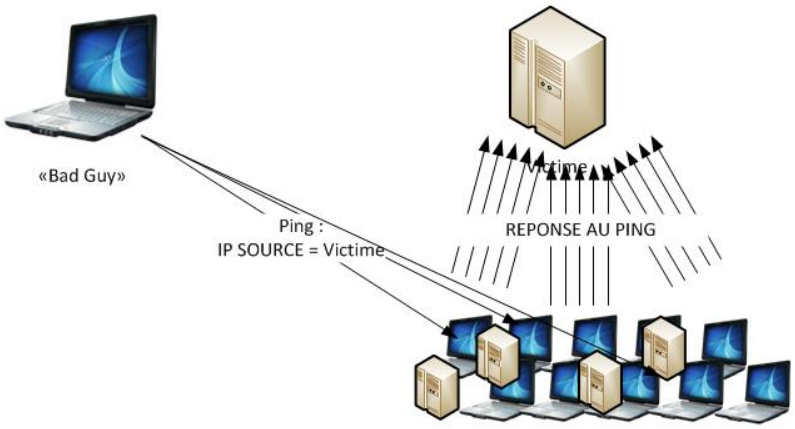


Schéma d'une attaque de type DrDoS à l'aide d'une requête ping – Source : E-xpertsolutions

En 2002, une attaque de type DrDoS était parvenue à paralyser 9 des 13 serveurs DNS racine, menaçant ainsi gravement le fonctionnement du réseau[18].

[17] https://www.ovh.com/fr/anti-ddos/principe-anti-ddos.xml
[18] http://www.tomshardware.fr/articles/attaque-dns-drdos,1-24672.html#peRfQL5OL3spDcfx.99

L'attaque DrDoS peut en outre être amplifiée. On parle alors *d'Amplified Distributed Reflective Denial of Service* (ADRDoS). Sur le même principe, cette technique utilise des protocoles dans lesquels la réponse transmise par les serveurs sur Internet est beaucoup plus volumineuse afin d'amplifier l'effet de l'attaque.

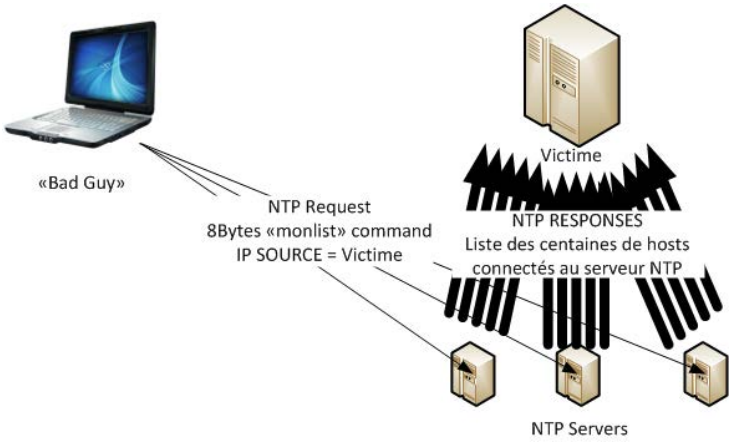


Schéma d'une attaque de type ADRDOS – Source : E-xpertsolutions

L'expansion des supports de diffusion de ces attaques est aussi à prendre en compte. En effet, l'utilisation de botnets pourrait prendre un nouveau tournant avec l'émergence massive d'objets connectés dans notre quotidien. Les *thingbots* ou « objets connectés zombies » pourraient devenir les nouveaux supports d'attaques privilégiées par les pirates.[19] La première attaque via l'utilisation d'un *thingbot* qui été détectée par Proofpoint avait permis l'envoi de plus de 750 000 courriels malveillants à partir de plus de 100 000 objets connectés détournés.[20] Ces thingbots pourraient à l'avenir être les vecteurs d'attaques par déni de service distribué.

[19] http://www.journaldunet.com/solutions/expert/62748/les-thingbots-arrivent.shtml
[20] http://cyberland.centerblog.net/42-un-monde-de-thingbots

Nom de l'attaque	Niveau OSI	Type d'attaque	Explications du principe de l'attaque
ICMP Echo Request Flood	L3	Ressources	Aussi appelé Ping Flood, envoi massif de paquets (ping) impliquant la réponse de la victime (pong) ayant le même contenu que le paquet d'origine.
IP Packet Fragment Attack	L3	Ressources	Envoi de paquets IP référençant volontairement d'autres paquets qui ne seront jamais envoyés, saturant ainsi la mémoire de la victime.
SMURF	L3	Bande Passante	Attaque ICMP en broadcast usurpant l'adresse source pour rediriger les multiples réponses vers la victime
IGMP Flood	L3	Ressources	Envoi massif de paquets IGMP (protocole de gestion du multicast)
Ping of Death	L3	Exploit	Envoi de paquets ICMP exploitant un bogue d'implémentation dans certains systèmes d'exploitation
TCP SYN Flood	L4	Ressources	Envoi massif de demandes de connexion TCP
TCP Spoofed SYN Flood	L4	Ressources	Envoi massif de demandes de connexion TCP en usurpant l'adresse source
TCP SYN ACK Reflection Flood	L4	Bande passante	Envoi massif de demandes de connexion TCP vers un grand nombre de machines, en usurpant l'adresse source par l'adresse de la victime. La bande passante de la victime sera saturée par les réponses à ces requêtes.
TCP ACK Flood	L4	Ressources	Envoi massif d'accusés de réception de segments TCP
TCP Fragmented Attack	L4	Ressources	Envoi de segments TCP référençant volontairement d'autres segments qui ne seront jamais envoyés, saturant ainsi la mémoire de la victime
UDP Flood	L4	Bande Passante	Envoi massif de paquets UDP (ne nécessitant pas d'établissement de connexion préalable)
UDP Fragment Flood	L4	Ressources	Envoi de datagrammes UDP référençant volontairement d'autres datagrammes qui ne seront jamais envoyés, saturant ainsi la mémoire de la victime
Distributed DNS Amplification Attack	L7	Bande Passante	Envoi massif de requêtes DNS usurpant l'adresse source de la victime, vers un grand nombre de serveurs DNS légitimes. La réponse étant plus volumineuse que la question, s'ensuit une amplification de l'attaque
DNS Flood	L7	Ressources	Attaque d'un serveur DNS par l'envoi massif de requêtes
HTTP(S) GET/POST Flood	L7	Ressources	Attaque d'un serveur web par l'envoi massif de requêtes
DDoS DNS	L7	Ressources	Attaque d'un serveur DNS par l'envoi massif de requêtes depuis un grand ensemble de machines contrôlées par l'attaquant

Exemples d'attaques DDoS – Source OVH :

Des motivations d'attaques diverses.

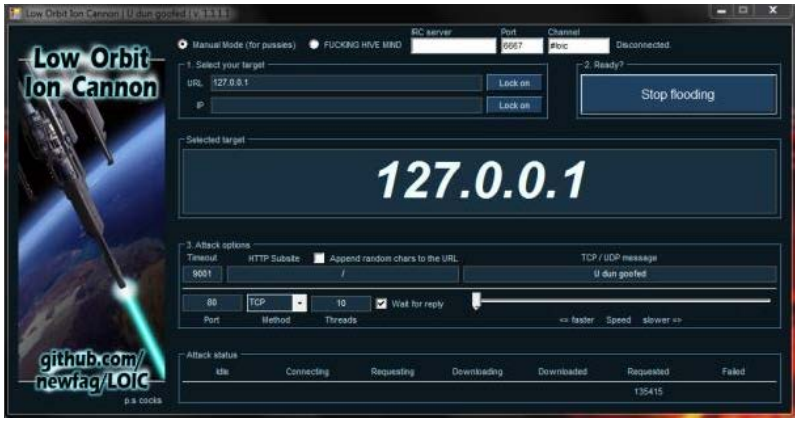
Les attaques DDoS sont devenues « une arme de concurrence déloyale, une méthode pour obtenir une rançon, un bâillon contre les journaux qui dérangeraient un hacker et globalement une méthode de nuisance en ligne quasi intraçable. »[21]. Selon NBS System, dans 99% des cas, l'origine d'une attaque DDoS n'est jamais identifiée et son auteur jamais poursuivi. Les motivations sont diverses au même titre que les cibles.

Si l'ensemble des secteurs d'activités peuvent être visés par ces attaques les secteurs du e-commerce, de la finance, du gouvernement et les structures d'hébergement informatique[22] sont les principales cibles de ce type d'attaque.

Les motivations de ces attaques sont d'abord idéologiques, comme en témoignent les actions de la nébuleuse Anonymous qui utilise les attaques de types DDoS pour paralyser régulièrement des sites internet. Il s'agit en réalité d'une nouvelle forme de manifestation virtuelle qui s'organise avec l'utilisation

[21] https://www.nbs-system.com/blog/ddos-dos.html
[22] http://www.ssi.gouv.fr/guide/comprendre-et-anticiper-les-attaques-ddos/

d'outils largement diffusés, telle l'application LOIC (*Low Orbit Ion Cannon*) proposée par les Anonymous afin de faire participer un maximum d'internautes à leurs opérations.



Low Orbit Ion Cannon, outil utilisé et proposé par Anonymous

Ces attaques ont cependant de plus en plus une motivation crapuleuse. Les banques sont ainsi une cible privilégiée, tout comme les entreprises, à qui sont réclamées des rançons contre l'arrêt des attaques.

Les attaques durent en majorité moins de 24 heures, mais la part des attaques qui dépassent 150 heures progresse de façon importante, ce qui peut avoir de graves conséquences sur les entreprises ciblées.

A l'inverse, les analyses montrent également que les attaques très courtes se développent aussi, le laps de temps entre l'attaque et la réponse de la victime étant trop court permettant aux pirates d'échapper aux solutions anti-DDoS présentes dans le cloud. L'étude de novembre 2015 de Corero Network Security montre en effet que la plupart des attaques subies par ses clients utilisent moins de 1Gbps, et que 95% des attaques ne durent pas plus de 30 minutes[23]. Ceci s'explique par la difficulté d'éviction de ces attaques, notamment dans les cas où la cible utilise des méthodes classiques de détection d'échantillons et des centres de nettoyage centralisés.

Un écran de fumée ?

Ces attaques qui ne provoquent pas de dégâts importants, mais perturbent le fonctionnement des réseaux, pose la question de leur objectif ultime. Pourraient-elles être des leurres visant à masquer d'autres formes d'attaques ?

Les attaques en déni de service distribué permettent en effet de plus en plus souvent aux pirates de masquer, grâce à un écran de fumée, des attaques de type APT grâce auxquelles ils vont s'infiltrer dans le réseau de la cible pour voler les informations clients et les données de la société ciblée[24]. L'étude de Kaspersky Lab et B2B international mettait en avant en octobre 2015 que 74% des attaques DDoS s'étaient accompagnées d'incidents de sécurité d'un autre type et que les attaques DDoS coïncidaient dans 45% des cas avec des incidents liés à des malwares, 32% des cas avec des intrusions dans le réseau de l'entreprise et 26% avec des fuites de données de métiers sensibles[25].

[23] http://www.globalsecuritymag.fr/Les-attaques-DDoS-utilisent,20151117,57595.html
[24] Ibidem.
[25] https://www.globalsecuritymag.fr/Enquete-Kaspersky-Lab-les-attaques,20151023,56914.html

Qu'elles soient ou non partie intégrante d'une stratégie de « distraction », les attaques DDoS posent de plus en plus de problèmes aux entreprises. Pour Evgeny Vigovsky, « même avec un vaste contingent de personnel informatique, il est quasi impossible pour les entreprises de faire face à une attaque DDoS d'envergure et de restaurer leurs services par elles-mêmes. En outre, si une autre activité malveillante se déroule simultanément, cela démultiplie les dégâts. Le plus dangereux réside dans le fait que les entreprises peuvent ne jamais apprendre qu'elles ont été victimes d'une attaque DDoS, [cette dernière] servant souvent d'écran de fumée » pour d'autres attaques[26]. Pourtant des moyens de protection existent bel et bien.

Des solutions de protection limitées ?

Aucune offre de sécurité ne peut promettre une sécurité sans faille, notamment du fait d'une évolution permanente des outils et vecteurs d'attaques. Cependant des méthodes et outils existent et permettent de limiter les dégâts[27] :

➡ En interne :

- Déployer des équipements de filtrage en bordure du réseau d'une entité : permet de se protéger contre les attaques qui ne saturent pas les liens réseau d'une entité.
  - Exemples : les pare-feu et répartiteurs de charge ; les équipements dédiés.

➡ En externe :

- Filtrer le trafic en amont en sollicitant l'opérateur de transit ou le fournisseur d'accès à Internet : se révèle nécessaire pour lutter contre une attaque qui sature les liens réseau d'une entité.
  - Exemples : protection via l'hébergeur ; filtrage au niveau du réseau via l'opérateur de transit ; filtrage dédié aux attaques DDoS via l'opérateur de transit ; utilisation d'un Content Delivery Network[28] (CDN). La société OVH[29] propose ce type de service.
- Solliciter un prestataire offrant une protection dédiée via le cloud mais hébergée par le prestataire lui-même sur son infrastructure.
  - Exemples : redirection via le protocole DNS ; déroutement du trafic par des annonces BGP.
- Utiliser une protection hybride associant l'utilisation d'équipements dédiés en bordure du réseau d'une entité à un filtrage effectué via le cloud afin de protéger l'entité des attaques volumétriques tout en lui donnant la capacité de lutter contre des attaques de débit plus faible. C'est notamment ce que propose la société CloudFlare[30].

---

[26] Ibidem.
[27] http://www.ssi.gouv.fr/guide/comprendre-et-anticiper-les-attaques-ddos/
[28] D'après l'ANSSI, un Content Delivery Network (CDN) « est une infrastructure de serveurs répartie dans plusieurs data centres, et dont l'objectif est de se substituer aux services d'une entité pour servir ses contenus au plus proche des utilisateurs. Les CDN ont ainsi une fonction de cache, et permettent notamment d'augmenter la disponibilité des ressources ou encore d'accroître la vitesse de mise à disposition des données, généralement des pages web ou des flux multimédia ». Définition consultable en ligne : http://www.ssi.gouv.fr/guide/comprendre-et-anticiper-les-attaques-ddos/
[29] https://www.ovh.com/fr/
[30] https://www.cloudflare.com/under-attack/

Il existe, d'autre part, des bonnes pratiques qui permettent d'obtenir un certain degré de protection en interne, que celles-ci soient le fait de l'entreprise elle-même ou de son opérateur de transit.

En interne, il s'agira par exemple de segmenter le réseau, ce qui permet l'isolement d'une partie du réseau en cas d'attaques. Ou encore d'instaurer un filtrage à la bordure du réseau de l'entité afin de contrôler les flux et de ne laisser passer que ceux nécessaires au fonctionnement de l'entité. Le transfert du risque à un prestataire SaaS constitue aussi une alternative intéressante. Dans ce cas, il est nécessaire de contrôler le niveau de sécurité de ce dernier et de mettre en place, par exemple, des SLA avec son prestataire de service.

Des mesures de sécurité peuvent permettre une détection plus rapide des attaques. Mais cela ne réduit pas les dégâts engendrés si l'on ne dispose pas de solution de « mitigation » : le trafic continuera de déverser le flot de requête constituant l'attaque.

La solution la plus adaptée semble alors être la combinaison d'outils de détection, qui pourront rapidement émettre une alerte en cas d'attaque, et d'un système de « mitigation » fourni par une entité externe.

Cette appellation désigne des moyens et des mesures mises en place pour atténuer les effets négatifs liés à un risque. Pour résister aux attaques DDoS, la mitigation consiste à filtrer le trafic non légitime pour ne laisser passer que les paquets légitimes.

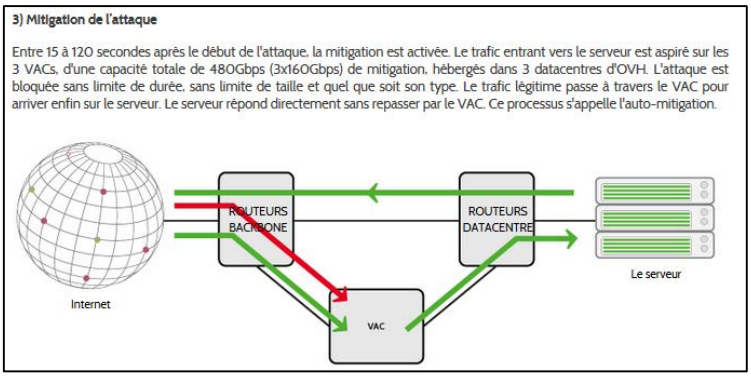
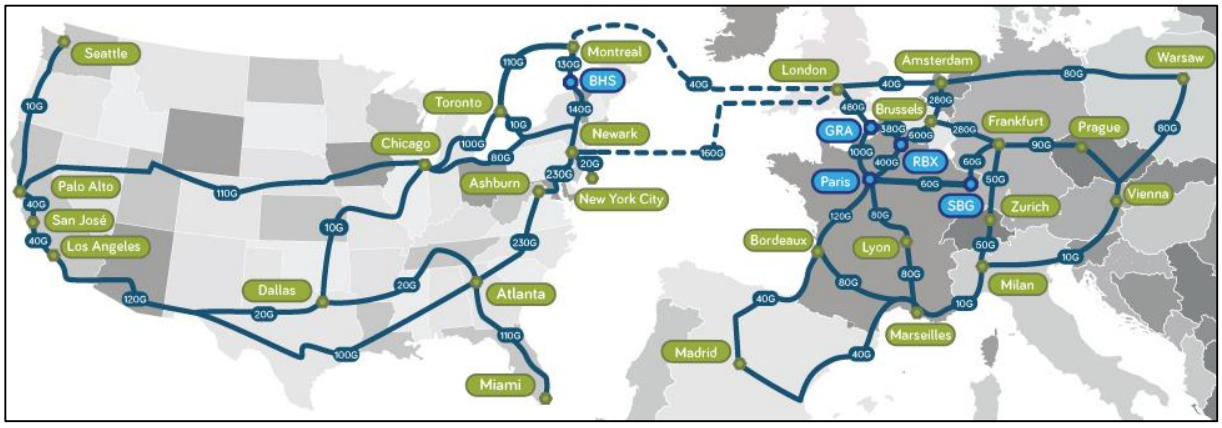


Schéma d'une Mitigation – Source : OVH.

La mitigation peut être renforcée par l'architecture du réseau de l'hébergeur, qui sera plus ou moins en mesure d'encaisser, d'aspirer et de « mitiger » de très nombreuses attaques. Lors d'une mitigation, répartie sur plusieurs datacenters, l'aspiration des attaques sera ainsi démultipliée. On parlera alors de « mitigation multipoints ».

OVH, mais aussi CloudFlare[31] proposent des solutions de ce type :



Exemple du réseau sur lequel OVH se base – Source : OVH

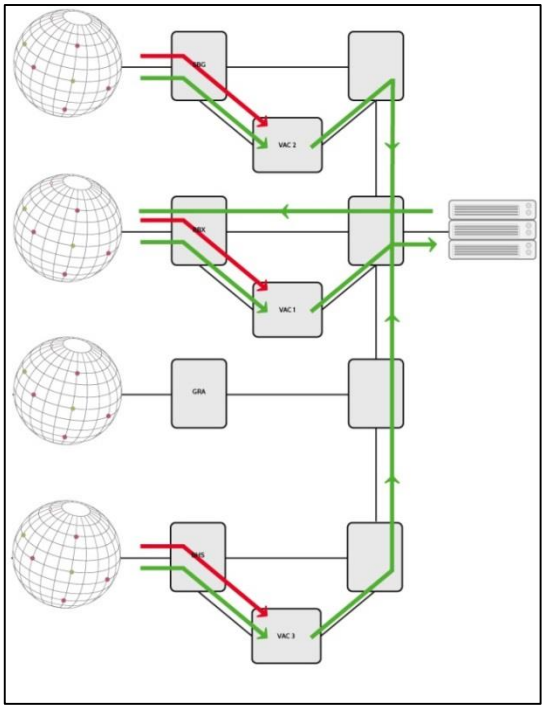


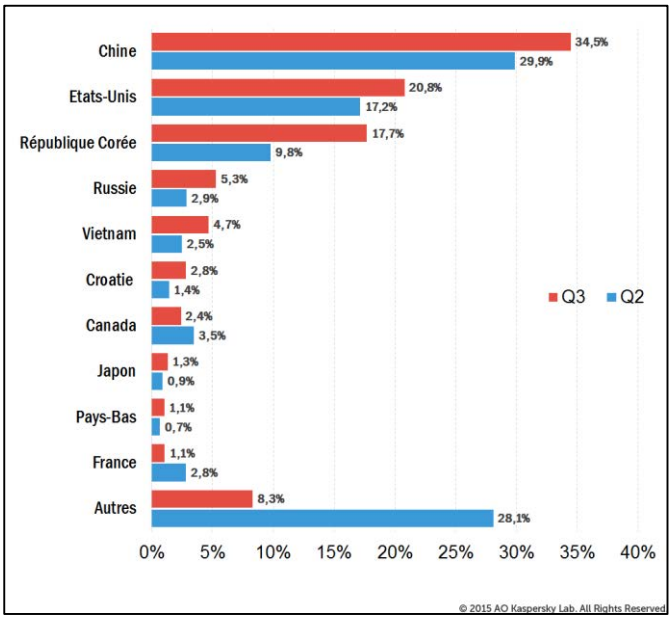
Schéma d'une « mitigation multipoints » - Source OVH

Lorsqu'une attaque est détectée, l'aspiration du trafic s'active afin de le filtrer et de ne laisser passer que des requêtes authentiques. Le principe développé par la société CloudFlare fonctionne sur le même modèle.

[31] Ibidem.

Quels Risques pour la France ?

Les attaques DDoS ne touchent pas aveuglément. Le rapport[32] de Kaspersky Lab sur l'évolution des attaques DDoS du troisième trimestre 2015 a souligné la diversité géographique des cibles, avec 79 pays touchés, et un trio de tête composé dans l'ordre décroissant de la Chine, des Etats-Unis et de la Corée du Sud. 91.6% des cibles se trouvent pourtant dans seulement 10 pays.



Répartition des cibles uniques d'attaques DDoS par pays Trimestre 2 et Trimestre 3 2015 – Source : Kaspersky Lab.

Si la proportion des attaques entre le trio de tête de ce classement et celle des attaques menées sur des cibles européennes est sans commune mesure, la France fait tout de même partie des pays européens les plus touchés avec l'Allemagne, la Croatie et les Pays-Bas.

Les Etats ont aujourd'hui pleinement conscience de la menace que représente ce type d'attaque, notamment depuis 2007, à la suite des attaques DDoS visant l'Estonie. Le cas estonien fut même un *wake up call* pour les Etats qui ont saisi les enjeux de protection liés à ce type d'attaques et mis en place des politiques visant à développer un arsenal défensif sans pour autant cibler spécifiquement les attaques de type DDoS.

Le constat est différent pour les entreprises : pour 75% des personnes sondés par Corero dans le cadre de son rapport « Tendances et Analyse des DDoS », ce sont les FAI qui doivent prendre en charge les mesures de sécurité contre ces attaques, dès lors que ces dernières entrent par le réseau fourni par ces mêmes FAI.[33]

Les entreprises se contentent donc généralement de l'offre traditionnelle de sécurité des infrastructures : pare-feu, systèmes de prévention d'intrusion et répartiteurs de charge, alors même que ce type d'équipement est reconnu comme notoirement insuffisant face aux attaques DDoS.[34]

---

[32] http://newsroom.kaspersky.eu/fr/news/detail/article/320-heures-dattaque-ddos-en-continu-kaspersky-lab-observe-levolution-des-attaques-par-deni/?no_cache=1&cHash=3409fb3853c4dde608dd08de48dbefcb
[33] http://www.globalsecuritymag.fr/Les-attaques-DDoS-utilisent,20151117,57595.html
[34] Ibidem.

L'un des obstacles à une meilleure prise en compte du risque par les entreprises est évidemment le coût d'une protection adéquate. L'étude de Corero précédemment citée soulignait d'ailleurs que près de la moitié des personnes interrogées ne souhaitaient pas ou n'étaient pas en mesure de s'offrir de tels services. Le décalage entre le coût des mesures de protection et l'accessibilité des outils d'attaque place de fait les entreprises dans une position très délicate. Nombreuses sont ainsi celles qui estiment que le coût de la protection est trop élevé par rapport à l'impact potentiel d'une attaque, celui-ci étant évalué par Neustar à entre 7 000 et 40 000 € par heure en moyenne[35].

L'impunité relative dont jouit cette forme de criminalité tient au fait qu'il est très difficile de parvenir à la source de l'attaque. Celles-ci sont en outre en pleine croissance et ne devraient pas diminuer au regard de l'expansion des supports et vecteurs. « Les pirates sondent sans relâche l'Internet pour découvrir de nouvelles ressources dont ils pourront tirer parti »[36], expliquait Stuart Scholly, directeur général d'Akamai, à propos des nouveaux vecteurs des attaques de type DrDoS. La lutte contre ces attaques doit donc être permanente et évolutive pour s'adapter aux innovations cybercriminelles.

[35] https://www.nbs-system.com/blog/ddos-dos.html
[36] http://www.datasecuritybreach.fr/trois-nouveaux-vecteurs-dattaques-ddos/#ixzz3sIwP7JtY

La **Direction Générale des Relations Internationales et de la Stratégie (DGRIS)** propose les analyses politiques et stratégiques contribuant à renforcer l'appréciation des situations et l'anticipation. Elle soutient la réflexion stratégique indépendante, en particulier celle menée par les instituts de recherche et organismes académiques français et étrangers. Elle contribue au maintien d'une expertise extérieure de qualité sur les questions internationales et de défense.

A ce titre, la **DGRIS** a confié à **CEIS** la réalisation de cet **Observatoire du Monde Cybernétique**, sous le numéro de marché 1502492543. Les opinions développées dans cette étude n'engagent que leur auteur et ne reflètent pas nécessairement la position du Ministère de la Défense.

Ministère de la Défense et des Anciens combattants
Direction Générale des Relations Internationales et de la Stratégie
14 rue Saint-Dominique - 75700 – Paris SP 07

CEIS
280 Boulevard Saint-Germain - 75007 - Paris
Téléphone : 01 45 55 00 20
E-mail : omc@ceis-strat.com