Cours d'expression et de communication, PPP, Mme Touba Keltoum

Rapport cyberattaque :
Attaque DDoS (Distributed Denial of Service)

Auteur :

Heu-Combe Nolan

Klughertz Jason

Corrêa do Carmo Jack-Alexander

BUT1 S1 R&T 2023/2024

Table des matières

Introduction

Dans un contexte de plus en plus préoccupant en matière de cybersécurité, cette analyse se penche sur l'attaque DDoS récente menée par le collectif d'hacktivistes pro-russes, UserSec, contre diverses institutions gouvernementales françaises, notamment le ministère de la Justice ce 29 Juin 2023. Cette attaque a mis en lumière la vulnérabilité croissante des infrastructures numériques françaises et soulève des questions essentielles sur la sécurité nationale. Ce rapport a pour objectif de détailler les événements liés à cette attaque, d'en évaluer les conséquences et d'explorer les mesures nécessaires pour renforcer la défense numérique de la France.

Problématique : Comment les attaques DDoS affectent-elles la cyber sécurité en France ?

Dans un premier temps nous expliquerons ce qu'est une attaque DDoS en exposant la chronologie des évènements et en définissant l'attaque. Nous traiterons du type d'attaque employées ainsi que de l'attribution de l'attaque du ministère de la justice.

Dans un second temps, nous exposerons les conséquences et l'impact que peuvent avoir ces cyberattaques sur la cybersécurité en France en expliquant quelles sanctions sont applicables aux coupables et en analysant la cybersécurité.

Enfin dans un dernier temps, nous traiterons des recommandations pouvant être faites pour se prémunir et réagir face à une attaque DDoS.

I/ Description de l'attaque DDoS

A) Chronologies des évènements

L'attaque DDoS a été menée de manière coordonnée par UserSec[1], un groupe hacktiviste qui avait déjà ciblé d'autres entités françaises par le passé. Elle a débuté avec une série d'attaques ciblées contre plusieurs sites de l'administration française, dont le ministère de la Justice, entraînant des interruptions de service significatives. Les hacktivistes ont exploité diverses méthodes de déni de service distribué (DDoS) pour surcharger les serveurs cibles, les rendant inaccessibles pour les utilisateurs légitimes. Cette attaque a duré plusieurs heures, perturbant le fonctionnement normal des sites touchés.

B) Définition de l'attaque

Techniquement, une attaque DDoS est une version distribuée d'une attaque par déni de service (DoS) dont le but est de perturber les opérations commerciales de la cible. Ce type d'attaque envoie un volume élevé de trafic pour surcharger le fonctionnement normal d'un service, d'un serveur ou d'une interconnexion de réseau, les rendant ainsi indisponibles. Les attaques DoS interrompent le service, tandis que les attaques distribuées (DDoS) sont menées à une échelle beaucoup plus grande, ce qui permet de mettre hors service des infrastructures entières et des services évolutifs (cloud).

C) Technique employée

Ici, nous avons affaire à une attaque DDoS dites « volumétrique ». C'est l'une des techniques les plus couramment utilisées et elle consiste à envoyer une grande quantité de petits paquets au botnet dont l'adresse IP a été usurpée (Un botnet est un groupe d'ordinateurs ou de dispositifs sous le contrôle d'un attaquant, utilisé pour mener des activités malveillantes contre une victime ciblée). Il répondra à son tour avec des paquets encore plus volumineux envoyés directement à la victime (c'est-à-dire à l'adresse IP usurpée). Les cibles de trafic flooding[2] (c'est simplement le fait d'inonder une machine ciblée dans le but de bloquer ou gêner son fonctionnement) ne sont généralement pas en mesure de répondre, car leurs connexions Internet sont

[1] Groupe d'hacktiviste
[2] Inondation d'information

totalement surchargées (elles atteignent les limites de leur bande passante). Cette technique est une attaque par réflexion et amplification.

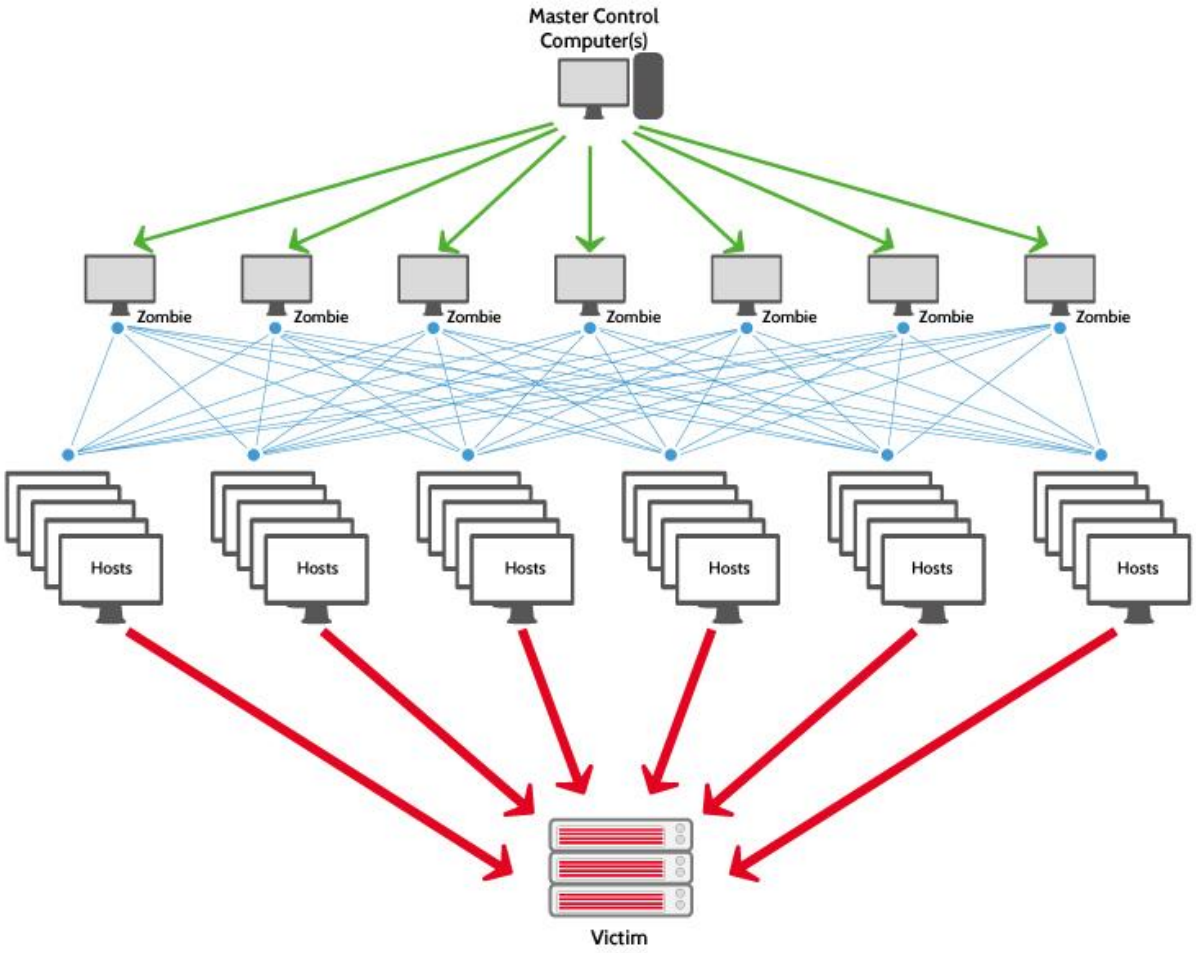

Figure 1: Méthode d'attaque DDoS Volumétrique

D) Attribution des attaques

L'attribution de cette attaque DDoS à UserSec est basée sur les revendications faites par le groupe sur la plateforme de messagerie Telegram[3]. Ils ont affirmé leur responsabilité et ont déclaré agir en tant qu'hacktivistes pro-russes, défendant les intérêts de la Russie. Les motivations précises derrière ces attaques restent un sujet de débat, mais il est clair que la géopolitique joue un rôle central dans leurs actions.

[3] Réseau de communication en ligne

II/ Conséquences et impacts

Les conséquences de cette attaque sont significatives, car elle a paralysé temporairement le ministère de la Justice, perturbant ainsi la fourniture de services essentiels. De plus, l'impact sur la sécurité numérique de la France est préoccupant, car cela soulève des préoccupations quant à la préparation et à la résilience des infrastructures gouvernementales face à de telles menaces. La réaction des autorités et l'attention médiatique ont également été des éléments clés de cette situation.

A) Les sanctions

Il est passible d'une peine de cinq ans d'emprisonnement et de 150 000 euros d'amende. Article 323-1 du Code pénal : « le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données » est passible de trois ans d'emprisonnement et de 100 000 euros d'amende.

B) Analyse de la cybersécurité

L'analyse de la cybersécurité révèle que de nombreuses cibles de cette attaque DDoS n'étaient pas préparées à faire face à une telle menace. Les mesures de protection en place étaient insuffisantes, laissant les serveurs vulnérables à l'assaut des hacktivistes. Cela souligne la nécessité pressante de renforcer la sécurité des infrastructures numériques gouvernementales en France. Les leçons tirées de cette attaque devraient servir de catalyseur pour améliorer la résilience numérique de notre pays.

III/ Recommandations

A) Sensibilisation

À la lumière de cette attaque DDoS et de ses répercussions, plusieurs recommandations s'imposent. Tout d'abord, il est impératif de renforcer les mesures de protection contre les attaques DDoS au sein des institutions gouvernementales. Cela devrait inclure la mise en place de solutions de détection précoce et de mitigation rapide. De plus, la France devrait travailler en étroite collaboration avec d'autres pays pour partager des informations sur les menaces et les tactiques utilisées par ces groupes hacktivistes. Enfin, il est crucial d'améliorer la sensibilisation à la cybersécurité au sein du gouvernement et du public pour mieux faire face à de telles menaces à l'avenir.

Pour se prémunir contre les attaques DDoS volumétriques, il est important de mettre en place une infrastructure réseau robuste et extensible. Cette technique anti-DDoS permet d'identifier le trafic malveillant et de le filtrer avant qu'il n'atteigne la cible.

Un réseau de distribution de contenu (CDN) est une solution de protection anti-DDoS très efficace. Les CDN sont conçus pour absorber et atténuer les attaques DDoS volumétriques en dispersant le trafic à travers un réseau mondial de serveurs. En dispersant le trafic, un CDN peut ainsi diluer une attaque DDoS et empêcher un unique point de faille d'être submergé.

B) Réaction

Un plan de réponse aux incidents est une étape cruciale dans la préparation à une attaque DDoS. Ce plan devrait inclure des détails sur qui contacter en cas d'attaque, comment isoler les systèmes affectés pour minimiser les dommages, et comment communiquer l'incident aux parties prenantes et aux clients.

Enfin, la sensibilisation des employés est une étape à ne pas négliger pour se prémunir contre les attaques DDoS. En effet, Les employés doivent comprendre les risques associés à ces attaques et savoir comment réagir en cas d'incident pour éviter d'accroître l'ampleur de l'attaque.

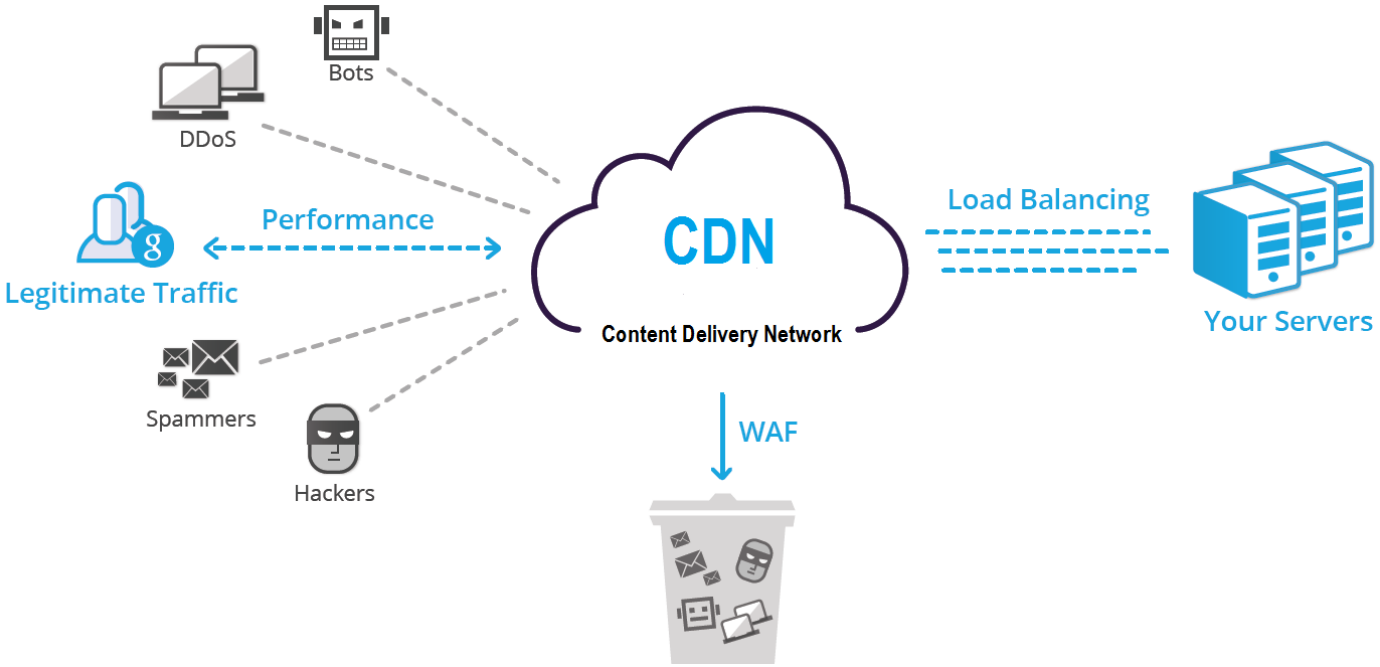

Figure 2: Méthode de protection anti-DDoS par CDN

Conclusion

En conclusion, l'attaque DDoS perpétrée par UserSec contre le ministère de la Justice et d'autres institutions gouvernementales françaises met en évidence la vulnérabilité de nos infrastructures numériques. Cette menace ne peut être ignorée, et des mesures immédiates sont nécessaires pour renforcer la sécurité et la résilience de notre pays face aux attaques cybernétiques. La collaboration nationale et internationale ainsi que l'amélioration de la préparation à de telles menaces doivent être des priorités pour garantir la stabilité numérique de la France.

Bibliographie

Gouvernement. (2019, Octobre 09). *Attaque DDoS, que faire?* Récupéré sur cybermalveillance.gouv: https://www.cybermalveillance.gouv.fr/tous-nos-contenus/fiches-reflexes/attaque-en-deni-de-service-ddos#loi-DDoS

Inconnu. (2023, Mai 05). *France : le Sénat victime d'une attaque DDoS russe.* Consulté le Septembre 2023, sur incyber: https://incyber.org/france-senat-victime-attaque-ddos-russe/

RFI. (2023, Mars 27). *France: le site internet de l'Assemblée victime d'une attaque de pirates pro-russes.* Consulté le Septembre 2023, sur rfi: https://www.rfi.fr/fr/france/20230327-france-le-site-internet-de-l-assembl%C3%A9e-victime-d-une-attaque-de-pirates-pro-russes

Thierry, G. (2023, Juin 30). *Après France-Visas, le ministère de la Justice visé par une attaque DDoS d'hacktivistes pro-russes.* Consulté le Septembre 2023, sur zdnet: https://www.zdnet.fr/actualites/apres-france-visas-le-ministere-de-la-justice-vise-par-une-attaque-ddos-d-hacktivistes-pro-russes-39960114.htm

vauxmoret, E. d. (2021, Mai 31). *Les CDN, ou comment diffuser plus efficacement le contenu d'un serveur web.* Récupéré sur uplix: https://www.uplix.fr/cdn/

Yoorshop. (s.d.). *Vous êtes sous attaque DDoS?* Consulté le Septembre 2023, sur yoorshop: https://support.yoorshop.hosting/knowledgebase/3077/Vous-etes-sous-attaque-Ddos.html

Index

Lexique

Ddos : Une attaque en déni de service ou en déni de service distribué (DDoS pour Distributed Denial of Service en anglais) vise à rendre inaccessible un serveur par l'envoi de multiples requêtes jusqu'à le saturer ou par l'exploitation d'une faille de sécurité afin de provoquer une panne ou un fonctionnement fortement dégradé.

Flooding : c'est le fait d'inonder une machine ciblée dans le but de bloquer ou gêner son fonctionnement.

CDN : Un réseau de diffusion de contenu est un réseau de serveurs interconnectés qui accélère le chargement des pages Web pour les applications à forte densité de données.

Hacktivistes : Les hacktivistes effectuent des cyberattaques en fonction de leurs opinions personnelles sur des actions spécifiques de gouvernements ou d'entreprises.

Botnet : Un botnet est un groupe d'ordinateurs ou de dispositifs sous le contrôle d'un attaquant, utilisé pour mener des activités malveillantes contre une victime ciblée.

Table des illustrations