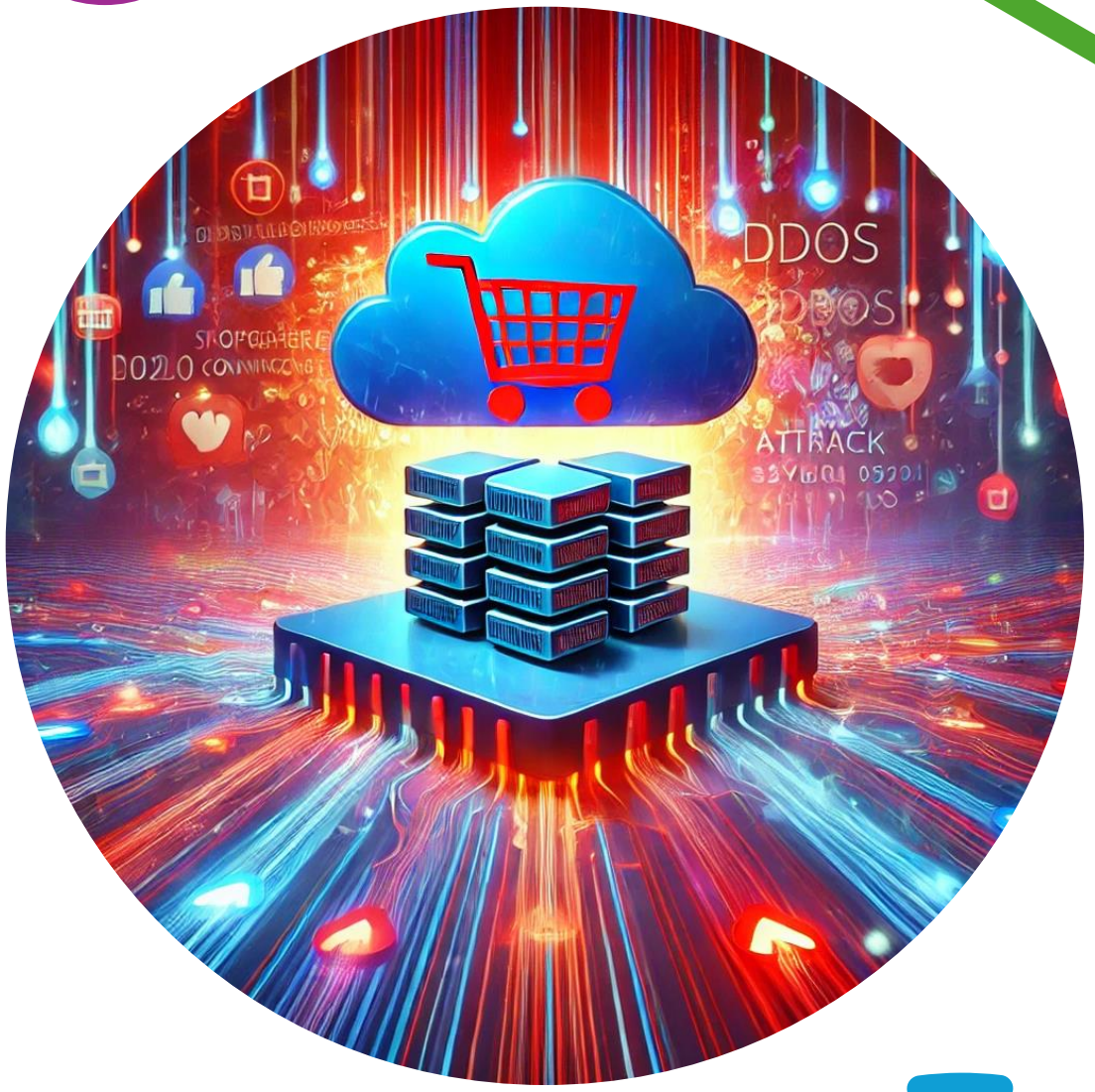

ECE
ÉCOLE D'INGÉNIEURS
ENGINEERING SCHOOL

Attaque DDoS sur une plateforme de e-commerce

SOMMAIRE

- Présentation Générale
- Analyse du context
- Description des attaques subies
- Analyse des vulnérabilités exploitées
- Solutions techniques pour corriger les failles
- Recommendations stratégiques conformes aux norms et réglementations
- Conclusion

ECE
ÉCOLE D'INGÉNIEURS
ENGINEERING SCHOOL

Présentation générale

ECE
ÉCOLE D'INGÉNIEURS
ENGINEERING SCHOOL

Ce rapport porte sur l'attaque DDoS massive subie par l'entreprise FastShop, un site de e-commerce, lors du Black Friday, une période de forte activité commerciale. Cette attaque a rendu le site inaccessible, entraînant des pertes financières importantes et une atteinte à sa réputation.Face à cet incident, l'ANSSI demande une analyse détaillée des événements afin d'identifier les failles exploitées et de proposer des solutions correctives pour éviter qu'une telle situation ne se reproduise. Ce rapport vise donc à comprendre l'attaque et à formuler des recommandations adaptées pour améliorer la cybersécurité de l'entreprise.

Analyse du contexte

FastShop est une entreprise de vente en ligne spécialisée dans le commerce électronique. Son activité repose sur la disponibilité et la performance de son site web, en particulier lors d'événements commerciaux majeurs comme le Black Friday, où le trafic client est extrêmement élevé.

C'est précisément à ce moment stratégique que l'entreprise a été ciblée par une attaque DDoS massive, visant à saturer ses serveurs et à rendre son site inaccessible.

Conséquences de l’attaque

- Site rendu inaccessible en quelques minutes → L’afflux artificiel de requêtes a rapidement dépassé la capacité des serveurs, empêchant les vrais clients d’accéder au site.

- Perte financière estimée à plusieurs millions d’euros → En raison de l’indisponibilité du site pendant une période de forte demande, FastShop a perdu un volume de ventes conséquent.

- Atteinte à la réputation et perte de confiance des clients → L’incapacité de l’entreprise à maintenir son service opérationnel a affecté son image, incitant certains clients à se tourner vers la concurrence.

Cette attaque met en lumière les risques majeurs liés à la cybersécurité dans le secteur du e-commerce, et souligne la nécessité de mettre en place des mesures de protection efficaces contre ce type de menace.

Description des attaques subies

1. Inondation de requêtes HTTP

- Envoi massif de requêtes HTTP pour surcharger les serveurs et empêcher l'accès aux clients.

2. Amplification DNS

- Exploitation de requêtes DNS malveillantes pour augmenter artificiellement le trafic dirigé vers FastShop.

3. Botnet IoT

- Utilisation d'appareils connectés piratés (caméras, routeurs...) pour générer un trafic énorme et difficile à bloquer.

Analyse des vulnérabilités exploitées

L’attaque DDoS contre FastShop a réussi en grande partie à cause de plusieurs failles de sécurité dans l’infrastructure et les mécanismes de protection du site. Ces vulnérabilités ont facilité la saturation du système et empêché une réaction rapide face à l’attaque.

1. Absence de protection anti-DDoS

- FastShop ne disposait d'aucun mécanisme spécifique pour limiter le trafic anormal.
- Les requêtes malveillantes ont pu inonder les serveurs sans restriction, entraînant leur saturation.
- Conséquence : L'entreprise n'avait aucun moyen de filtrer ou ralentir l'attaque, ce qui a permis aux assaillants de neutraliser le site en quelques minutes.

2. Manque de filtrage réseau

- L'infrastructure ne possédait pas de pare-feu avancé ni de système de filtrage des requêtes suspectes.
- Les paquets de données malveillants ont été acceptés sans vérification, permettant à l'attaque de se propager rapidement.
- Conséquence : Les requêtes envoyées par les attaquants ont été traitées comme des requêtes normales, empêchant toute différenciation entre le trafic légitime et le trafic malveillant

3. Infrastructure centralisée

- Les serveurs de FastShop étaient tous regroupés au même endroit, sans répartition de charge sur plusieurs data centers.
- Cette configuration a facilité la saturation rapide du système, car il n'existait aucune solution de secours pour absorber le surplus de trafic.

Conséquence : Une fois que les serveurs ont atteint leur limite, l'ensemble du site est tombé en panne, sans alternative pour garantir sa disponibilité

4. Absence de détection des comportements anormaux

- FastShop ne disposait d'aucun système de surveillance en temps réel pour analyser le trafic et détecter les attaques en cours.
- Aucun algorithme ou intelligence artificielle n'était en place pour repérer une augmentation soudaine et inhabituelle du nombre de requêtes.

Conséquence : L'attaque a pu se développer sans être détectée jusqu'à ce que l'infrastructure soit totalement saturée, empêchant toute réaction préventive

Solutions techniques pour corriger les failles

- Mettre en place une protection anti-DDoS
    - Utilisation de services spécialisés (Cloudflare, AWS Shield) pour bloquer les attaques en amont.
- Améliorer le filtrage réseau
    - Mise en place de pare-feux et de filtres DNS pour bloquer les requêtes suspectes.
- Répartir l'infrastructure
    - Utilisation de CDN (Content Delivery Network) pour distribuer la charge sur plusieurs serveurs.
    - Load Balancer pour éviter qu'un seul serveur ne soit surchargé.
- Détecter les comportements anormaux
    - Installation d'outils de SIEM (Security Information and Event Management).
    - Surveillance en temps réel du trafic pour repérer les anomalies.

Recommandations stratégiques conformes aux normes et réglementations

L’entreprise doit adopter une stratégie de cybersécurité robuste en accord avec les bonnes pratiques de l’ANSSI :

1. Plan de réponse aux incidents

- Mettre en place une équipe de réponse rapide en cas d’attaque.

2.Tests de résistance réguliers

- Simuler des attaques pour identifier les points faibles.

3.Sensibilisation et formation

- Former les équipes techniques aux menaces DDoS.

4.Conformité aux normes

- Respect des standards de cybersécurité (ISO 27001, RGPD).

ECE
ÉCOLE D'INGÉNIEURS
ENGINEERING SCHOOL

Conclusion

L’attaque DDoS contre FastShop a mis en évidence des failles critiques en cybersécurité, ayant entraîné des pertes financières et une atteinte à l’image de l’entreprise. Pour éviter de futurs incidents, il est essentiel de renforcer la protection avec une défense anti-DDoS, un meilleur filtrage réseau et une surveillance en temps réel. En appliquant ces mesures, FastShop pourra garantir la disponibilité de son site, protéger ses clients et sécuriser son chiffre d’affaires.

Présenté par :