Rapport du projet d'Internet Nouvelle Génération
dans le cadre du Master 2 Cybersécurité et e-Santé

Étude sur les incidents réseaux de Facebook (4 octobre) et de OVHcloud (13 octobre)

Année universitaire 2021 – 2022

Présenté par

GUARDIA Quentin
quentin.guardia@etu.u-paris.fr

HARMALI Anis
anis.harmali@etu.u-paris.fr

Sous la direction de MEHAOUA Ahmed

Table des matières

Introduction

Le lundi 4 octobre, dès 17H30, Facebook et ses filiales dont Whatsapp, Messenger et Instagram sont devenues inutilisables. Et ce pour une durée comprise entre six et sept heures. Après les réseaux sociaux, cela a été au tour d'OVHcloud de tomber en panne, le 13 octobre vers 9h30. En a résulté une mise hors service de nombreux sites web. Dans ce rapport, nous tenterons d'apporter une analyse technique aux faits précédemment annoncés.

Avant cela, nous allons rappeler quelques définitions.

Un Autonomus System (AS) est un ensemble de réseaux IP connecté à internet et qui gère son routage interne. Pour être identifié dans internet, chaque AS bénéficie d'un numéro. Un AS peut originer des préfixes (dire qu'il contrôle un groupe d'adresses IP), ainsi que des préfixes de transit (dire qu'il sait comment atteindre des groupes spécifiques d'adresses IP).

Le Border Gateway Protocol (BGP) est une protocole de routage externe. Il permet de connecter les AS entre eux, en indiquant aux paquets les chemins/routeurs à emprunter. Plus particulièrement, iBGP est utilisé pour le routage au sein d'un AS et eBGP pour router deux AS entre eux.

La Domain Name System, ou plus simplement DNS, est le service informatique qui associe un nom de domaine à une adresse IP sur internet.

L'adressage IP peut se faire en IPv4 ou en IPv6, bien que la dernière version soit plus recommandée.

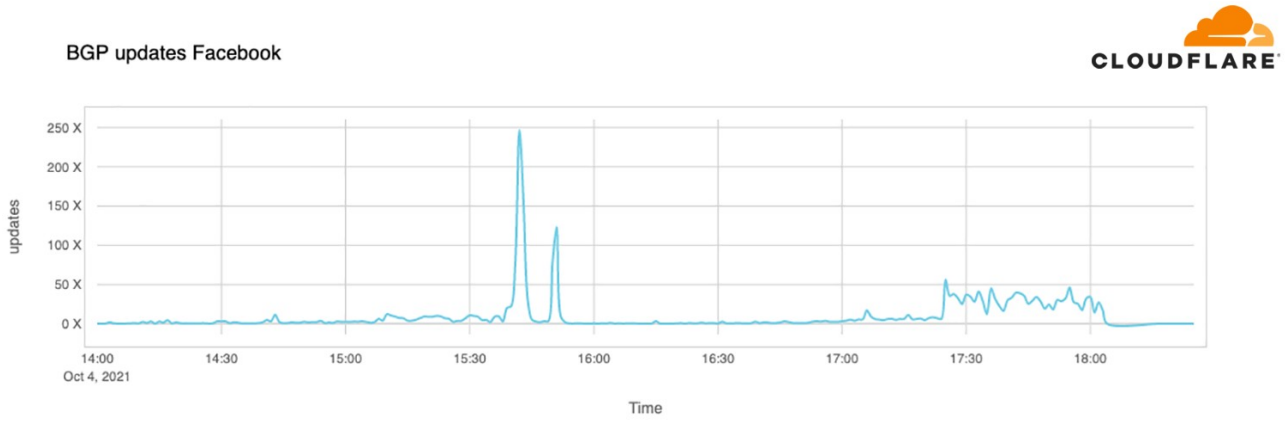
Étude des deux pannes

Facebook

Facebook est l'AS AS32934. Il est enregistré grâce à ARIN. Il héberge des centaines de milliers domaines et d'adresses IP.

Au moment de la panne, Facebook n'annonçait plus sa présence sur le protocole BGP et les FAI, les autres réseaux ne pouvaient pas trouver le réseau de Facebook. Celui-ci était donc indisponible. De nombreuses personnes, y compris dans le cadre de leur profession, ont été impactées, tandis que Facebook a vu ses actions chuter de 5 % le jour de la panne, et le PDG de Facebook Mark Zukerbeg a perdu plus de 6 milliards de dollars. Cela a créé une affluence soudaine vers d'autres réseaux sociaux.

Ce jour-là, vers 17h40 en France, CloudFlare a pu remarquer un pic du nombre de mises à jour des tables de routage BGP de Facebook (cf. ci-dessous).



Les mises à jour ont impliqué des retraits de préfixes d'adresse IP. Or certaines routes IP pointaient vers les serveurs DNS (Domain Name System) de Facebook. Ainsi, il est devenu impossible de résoudre les noms de domaines du groupe Facebook et leurs services à cause de routages BGP indisponibles. Les routes vers Facebook conservées en cache par les différents résolveurs publics ont été effacées vers 17h50.

Malheureusement, les ingénieurs sur place n'étaient pas habilités à corriger le problème, il fallait attendre que d'autres ingénieurs arrivent. Ainsi, vers 21h les tables BGP ont été mises à jour et les services Facebook étaient à nouveau disponibles.

Le lendemain, l'équipe d'ingénieurs de Facebook a expliqué que pendant la maintenance, une commande a été exécutée pour évaluer la capacité du réseau, et cette commande a accidentellement déconnecté tous les centres de données de Facebook. Bien que les

serveurs DNS de Facebook fonctionnent sur un réseau distinct, ils ont été conçus pour retirer leurs routes BGP s'ils ne pouvaient pas se connecter aux centres de données de Facebook, ce qui a rendu impossible la connexion du reste de l'Internet à Facebook.

OVHcloud

OVHcloud est un hébergeur français connu à l'internationale et qui a pour numéro d'AS le 16276.

Le 13 octobre de 9h à 10h30, une maintenance de routeurs était prévue chez OVH en vue de l'augmentation des attaques DDoS. Vers 9h30, OVH a été victime d'une panne, explique OVHcloud sur les réseaux sociaux. L'équipe est rapidement intervenue pour isoler l'équipement vers 10h15. Le retour à la normale s'est fait très progressivement. De simples blogs personnel jusqu'à des sites importants comme strasbourg.aeroport.fr et data.gouv.fr ont été indisponibles. Cela a également été problématique pour OVHcloud qui avait prévu son entrée en bourse sous peu. L'hébergeur est réputé pour être peu onéreux.

Il s'agit d'une erreur humaine. Au moment de la maintenance, le routage des adresses IP a été empêché par un mauvais paramétrage, bloquant l'accès à de nombreux sites web notamment.

Dans les faits, les connexions vers les machines adressées en IPv4 n'aboutissaient plus. En effet, l'erreur a été de couper une commande terminant par « ipv4 » un caractère trop tôt, isolant le 4. Ce qui a posé problème pour toutes les adresses IPv4, devenues indisponibles. Cela a été publié par un ingénieur travaillant chez OVHcloud. Concrètement, une boucle de convergence entre BGP et le protocole Open Shortest Path First (OSPF) a eu lieu, empêchant le routage IPv4. Donc le traitement correct du trafic IPv4 sur tous les sites web était impossible. Les adresses IPv6 ont elles été indisponibles quelques minutes, alors que c'était environ une heure pour les adresse IPv4.

Comparaison

Dans les deux cas, une information importante ressort. Il s'agit d'une simple erreur humaine, qui a été très dommageable du point de vue de la disponibilité des services et données. Cependant, le problème ne s'est pas déroulé de la même manière. Chez Facebook, la panne provenait du routage externe de l'AS tandis que chez OVHcloud, le problème se situait à l'intérieur du routage de l'AS.

Solutions proposées

L’erreur est humaine. La technologie ne crée pas de bug. Ces derniers sont nécessairement dûs à une maladresse humaine. Pour éviter ce genre de problème, on pourrait alors recourir à différentes aides.

Mais d’abord, notons qu’OVHcloud a commis une grosse erreur. OVHcloud a mis tous les serveurs DNS faisant autorité pour une zone dans le même AS. Diviser le réseau en plusieurs AS aurait diviser l’importance de la panne. En plus, on a constaté que les différents sites d’information d’OVHcloud n’ont pas d’IPv6.

Concernant Facebook, les serveurs sont involontairement hiérarchisés de sorte à créer un effet en cascade lors d’une panne, il faudrait entrevoir une architecture plus décentralisée.

Plus généralement, pour toute entreprise, on pourrait imaginer un système qui permettrait à chaque modification critique du réseau, une vérification par des pairs. C’est-à-dire que chaque modification, avant d’être effective, devrait passer par une étape de sécurité supplémentaire. Ainsi, les problèmes qui ont touché OVHcloud et Facebook auraient pu être évités.

Comme l’erreur est humaine, on pourrait aller au-delà et imaginer une intelligence artificielle qui, sur le modèle de tests unitaires, s’assure que chaque manipulation n’ait pas d’effet délétère, comme l’absence de routage vers une adresse IP. Cela éviterait avec certitude de nombreux bugs.

Enfin, il serait intéressant de migrer entièrement d’IPv4 vers IPv6, bien que cela prenne du temps. La version IPv6 est bien plus aboutie.

Conclusion

Facebook et OVHcloud ont récemment étaient victimes de panne, provoquant l'indisponibilité de leurs services, avec pour origine une erreur humaine. Cela a impacté de nombreux utilisateurs et provoqué de grosses pertes pour les deux entreprises.

On ne peut pas éternellement éviter les erreurs dans ce monde, y compris en informatique. Le problème pour les réseaux, c'est qu'un simple caractère erroné peut paralyser des millions voire des milliards d'utilisateurs. Or, certains services sont nécessaires au bon fonctionnement de la société.

Il faudrait donc concevoir des architectures de réseaux moins centralisées de manière à éviter les grosses pannes, sans trop complexifier chaque mise à jour pour autant. On pourrait également avoir recours à une intelligence artificielle qui vérifie la justesse de chaque commande écrite avant qu'elle ne soit effective.

Webographie

- « OVHcloud », https://fr.wikipedia.org/wiki/OVHcloud
- « OVHcloud », https://www.peeringdb.com/net/1264
- « OVH et la malheureuse erreur humaine de copier-coller qui a fait tomber des milliers de sites français », https://www.numerama.com/tech/747034-de-nombreux-sites-ne-fonctionnent-plus-ovh-semble-avoir-des-problemes.html
- « Understanding How Facebook Disappeared from the Internet », https://blog.cloudflare.com/october-2021-facebook-outage/
- « 2021 Facebook outage », https://en.wikipedia.org/wiki/2021_Facebook_outage
- « AS32934 », https://ipinfo.io/AS32934
- « Network incident, 13 October 2021 », https://corporate.ovhcloud.com/en-gb/newsroom/news/network-incident/
- « Update about the October 4th outage », https://engineering.fb.com/2021/10/04/networking-traffic/outage/